Demonstration of Positioning, Navigation, and Timing (PNT) Resilience Concepts to Reduce Development Risk

Elizabeth Dreifus

Civil GPS Service Interface Committee (CGSIC) 2024

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, DHS Science and Technology PNT Support
Control # 70RSAT20FR-062-18, Case 24-2410
The results presented in this report do not necessarily reflect official DHS opinion or policy

HSSEDI
Homeland Security Systems Engineering & Development Institute™

Bottom Line Up Front

- **Critical Infrastructure faces PNT threats such as jamming, spoofing**
- **PNT user equipment can withstand and recover from those threats by incorporating resilience concepts and architectures.**
- **Example resilient timing system demonstrates practicality, reduces risk to commercial development**

- **Key messages in this presentation:**
  1. **Layered Monitors**: Resilient PNT User Equipment requires layered monitors as defense against a variety of threats
  2. **Isolated Sources**: Isolating trusted core and "quarantining" sources keeps Position, Velocity, and Time (PVT) solution trusted
  3. **Visibility of States**: Developer must make internal states visible to the user for device evaluability and situational awareness.

PNT Threats are a Growing Problem for Critical Infrastructure

Inside GNSS

FCC Fines Operator of GPS Jammer That Affected Newark Airport GBAS

August 31, 2013 By Inside GNSS

Threats are out there, and regulations are difficult to enforce.

Spoofing Incident Report: An Illustration of Cascading Security Failure

October 9, 2017 By Inside GNSS

"This was by no means a sophisticated spoofing attack. It was an accident and there wasn't even an antenna on the spoofing source which would have extended range considerably."

What happens when a spoofer causes the following sectors to have degraded timing?

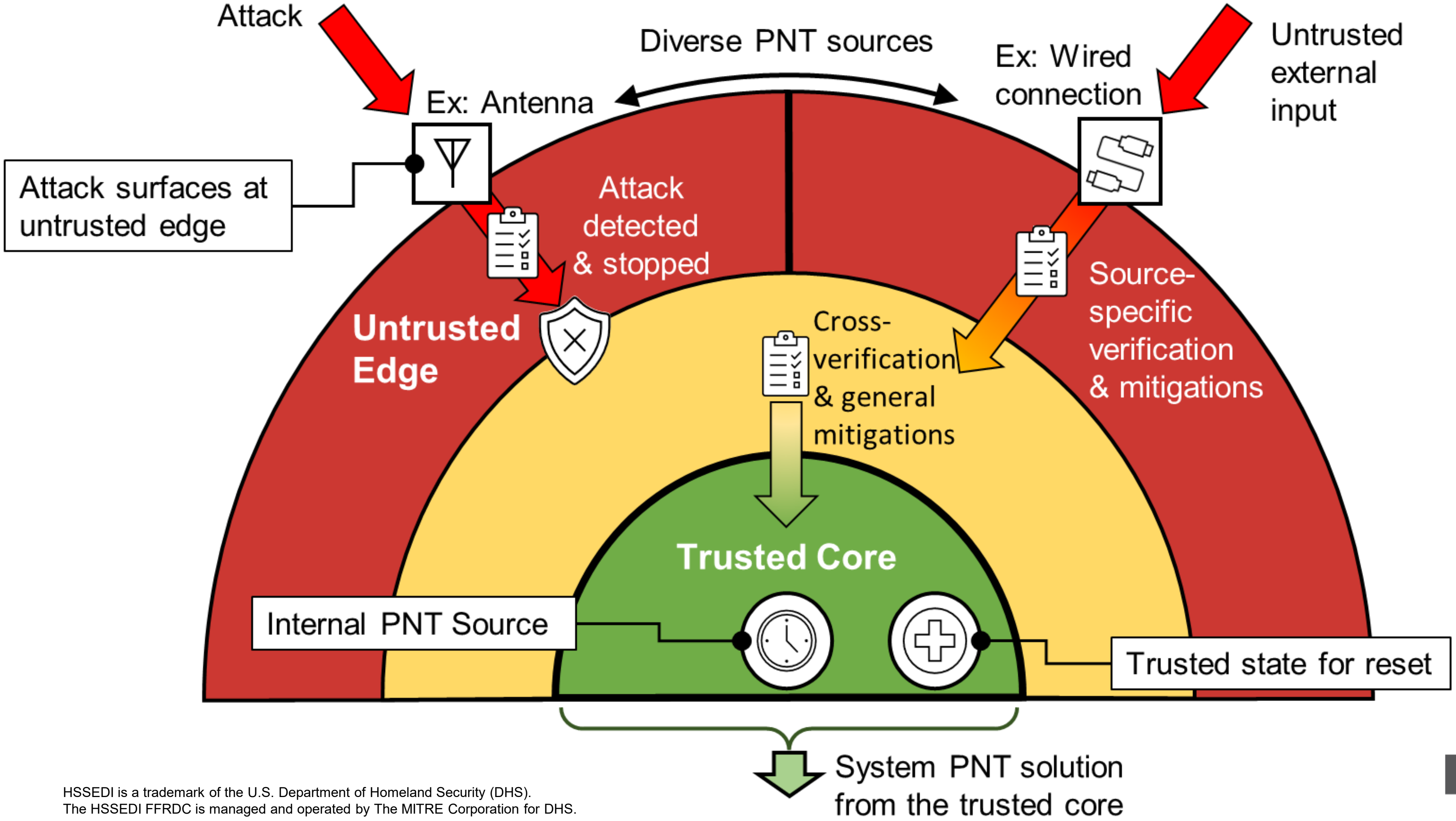
Financial Services:
Transactions compromised, monetary losses, out of compliance with regulations

Energy:
Takes **longer to fix problems** in the power grid

Communications:
Devices **may lose sync** with each other and be **unable to communicate**

FCC = Federal Communications Commission
GBAS = Ground Based Augmentation System
GNSS = Global Navigation Satellite System

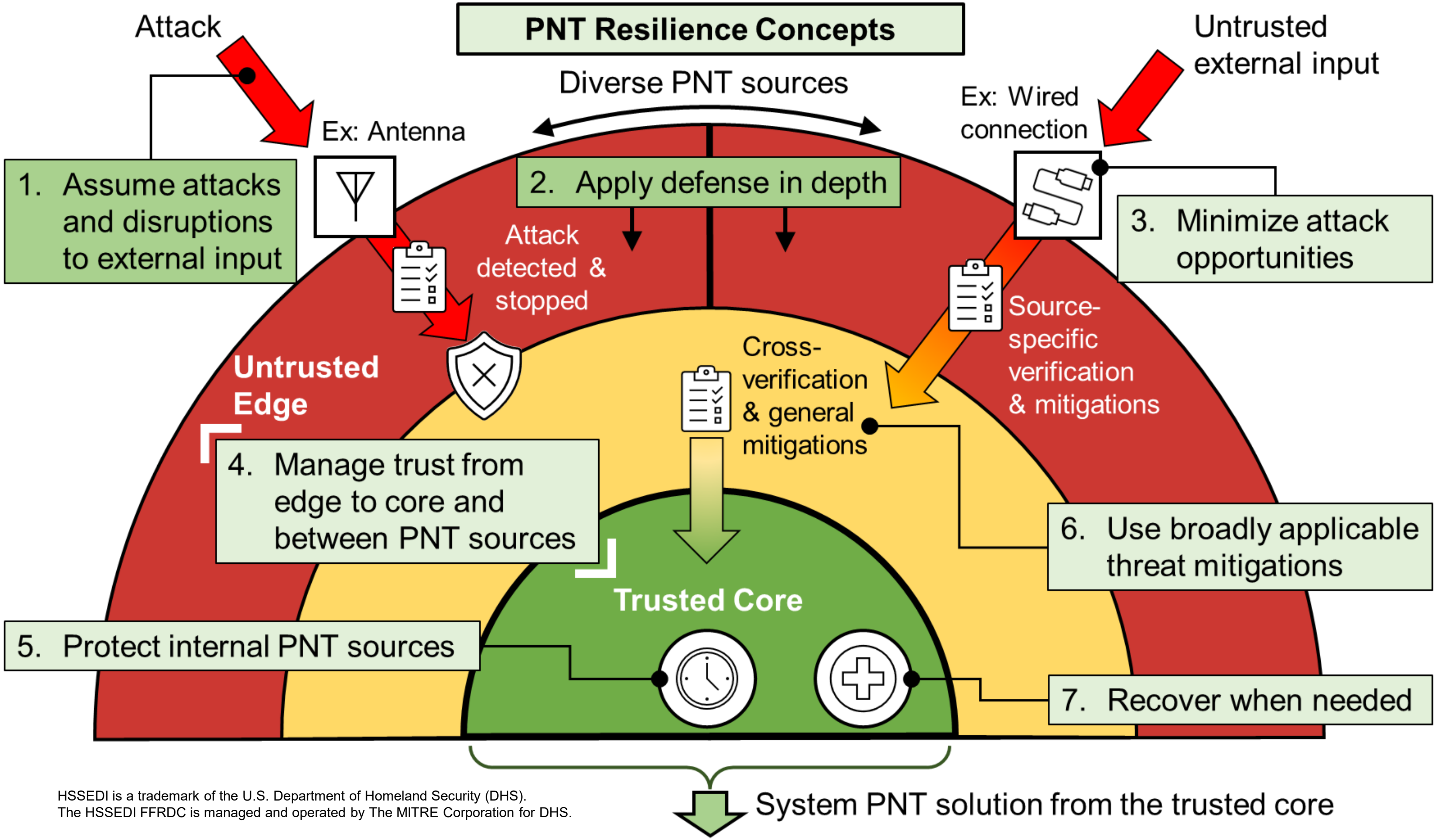
Resilience: From Concepts to Architecture to Implementation



Resilience: the ability to **withstand** and **recover** from a threat

Previous resilience work identified concepts to protect the trustworthiness of a PNT solution.

Resilience: From Concepts to Architecture to Implementation

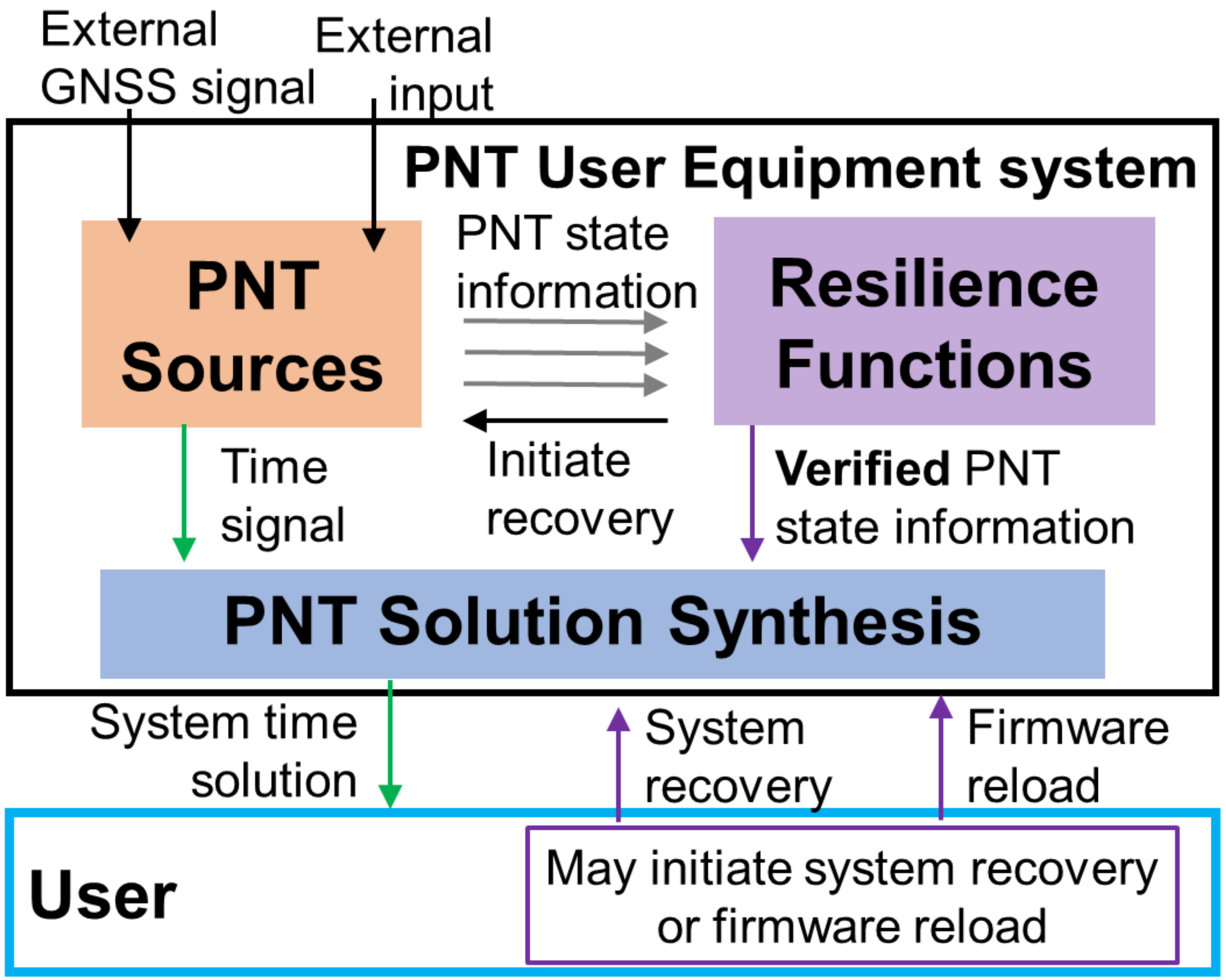


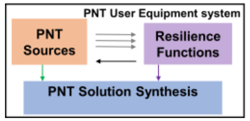
Resilience: the ability to **withstand** and **recover** from a threat

Previous resilience work identified concepts to protect the trustworthiness of a PNT solution.

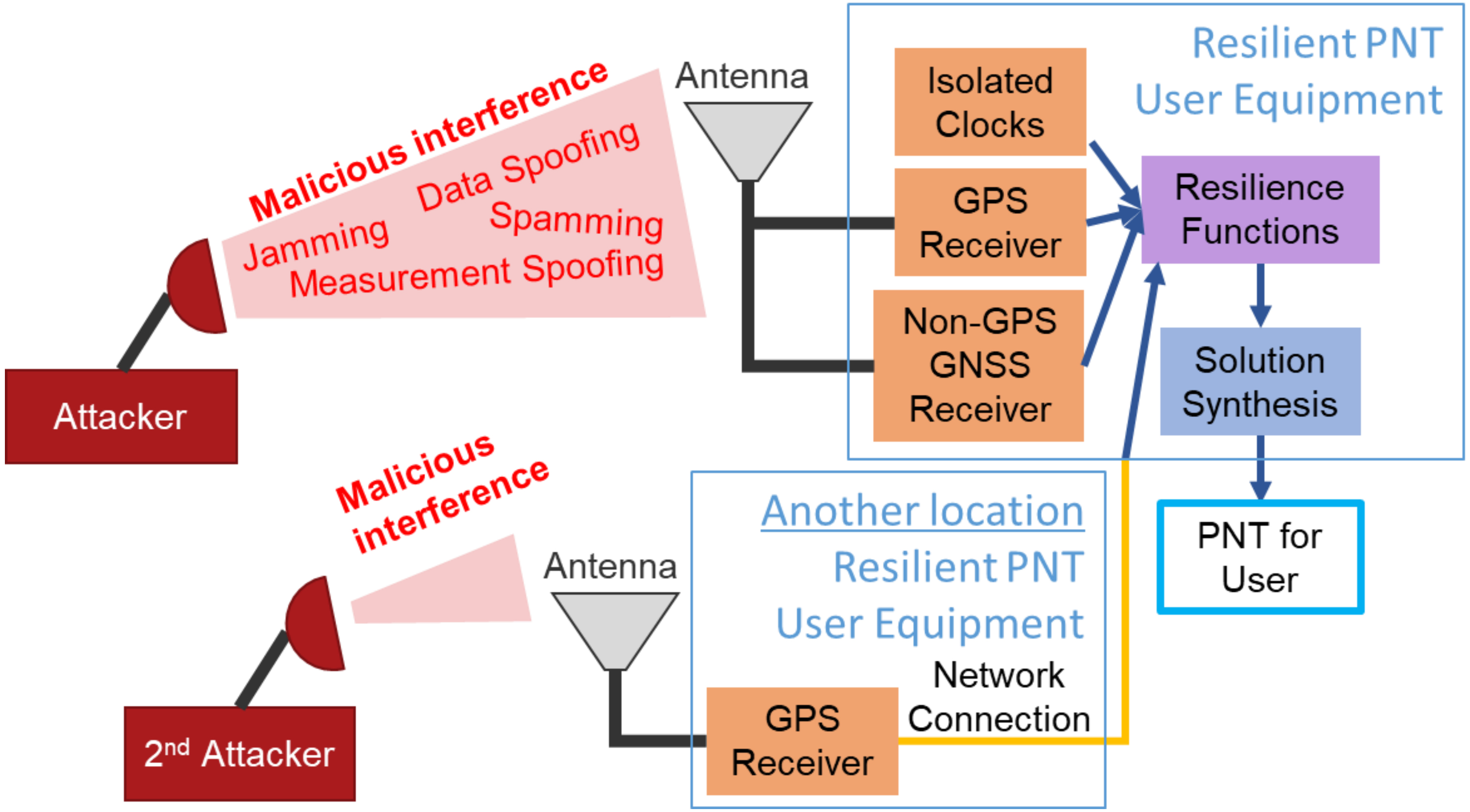
HSSEDI Homeland Security Systems Engineering & Development Institute™

Resilience: From Concepts to Architecture to Implementation





Resilience: From Concepts to Architecture to Implementation



- Proof-of-concept, demonstration
- Stationary timing application

We built an example resilient timing system to demonstrate practicality and reduce commercial development risk

GPS: Global Positioning System

There are many ways to implement the architecture

PNT Source Selections

- GPS Receiver
- Non-GPS GNSS Receiver
- Precise Time Protocol (PTP)
- Isolated Clocks:
  - Low-SWAP atomic clock
  - Oven-Controlled Crystal Oscillator (OCXO)
- **Many other options such as:**
  - Multi-GNSS Receiver
  - Software-Defined Receiver
  - Network Time Protocol
  - Two-way Satellite Time Transfer

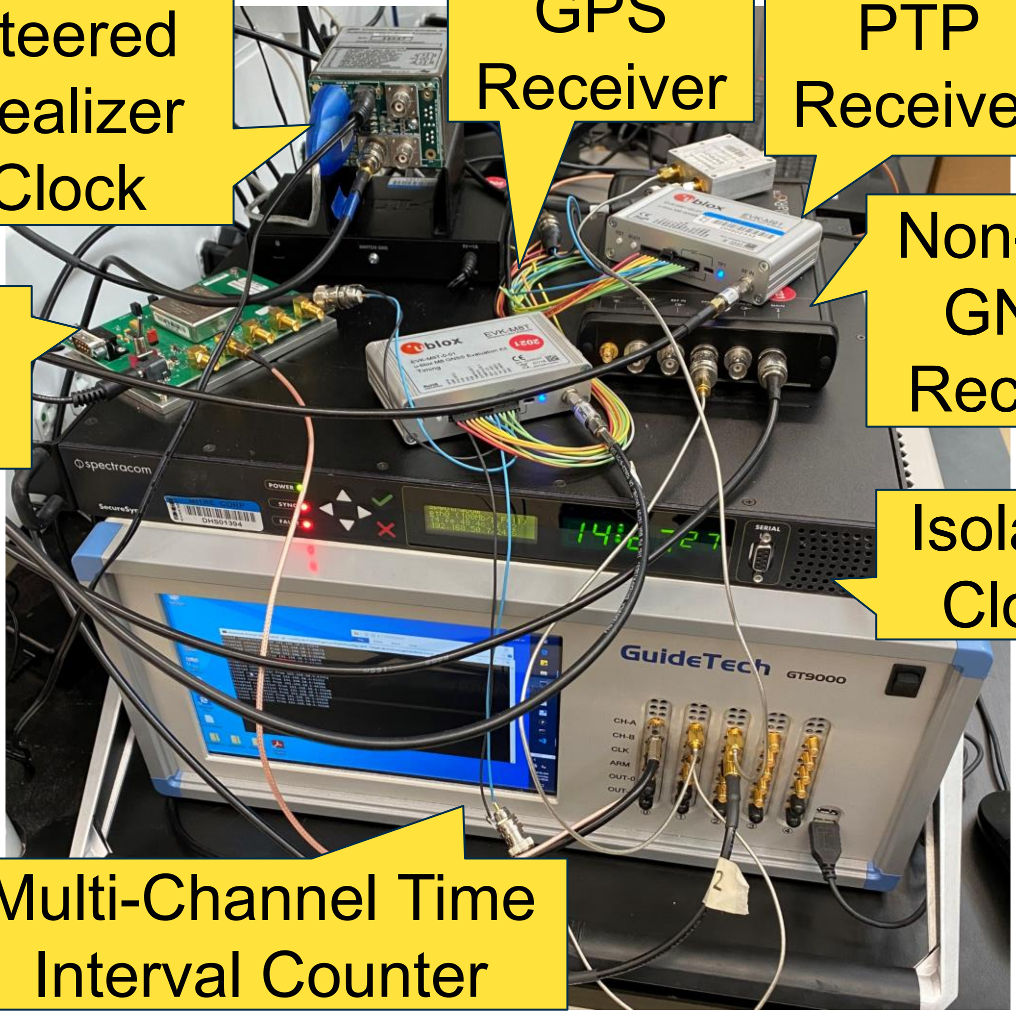
Threat Detection Monitor Selections

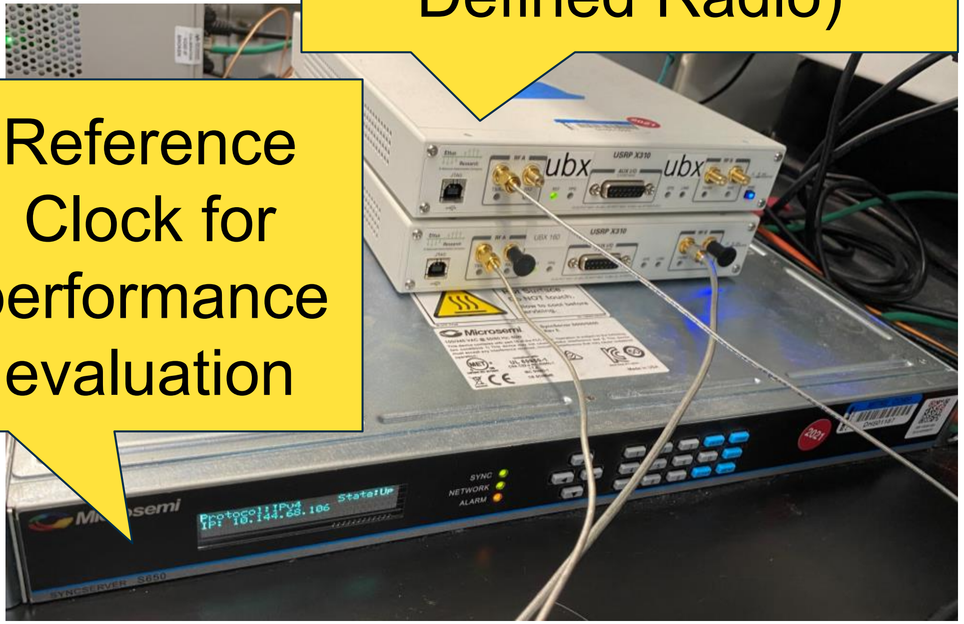
- Stationary Position & Velocity Monitors
- Clock Rate Monitor
- Wiener Process Disorder Detector (WPDD)
- Automatic Gain Control Jamming Monitor
- Commercial Receiver Built-in Jamming Monitor
- Cross-checks: Position, Velocity, 1 pulse per second (PPS) Measurements
- Monitor Fusion based on PNT Integrity Library
- **Many more options!**

Solution Synthesis Selections

- **Calculate the solution based on source trustworthiness**
  - Ensemble PNT sources
  - Switch between PNT sources, e.g., as a Primary-Alternate-Contingency-Emergency (PACE) plan would
- **Solution Realization:**
  - Steer independent output oscillator
  - Use output directly from a PNT source (for switching option)
  - Use auxiliary output generator

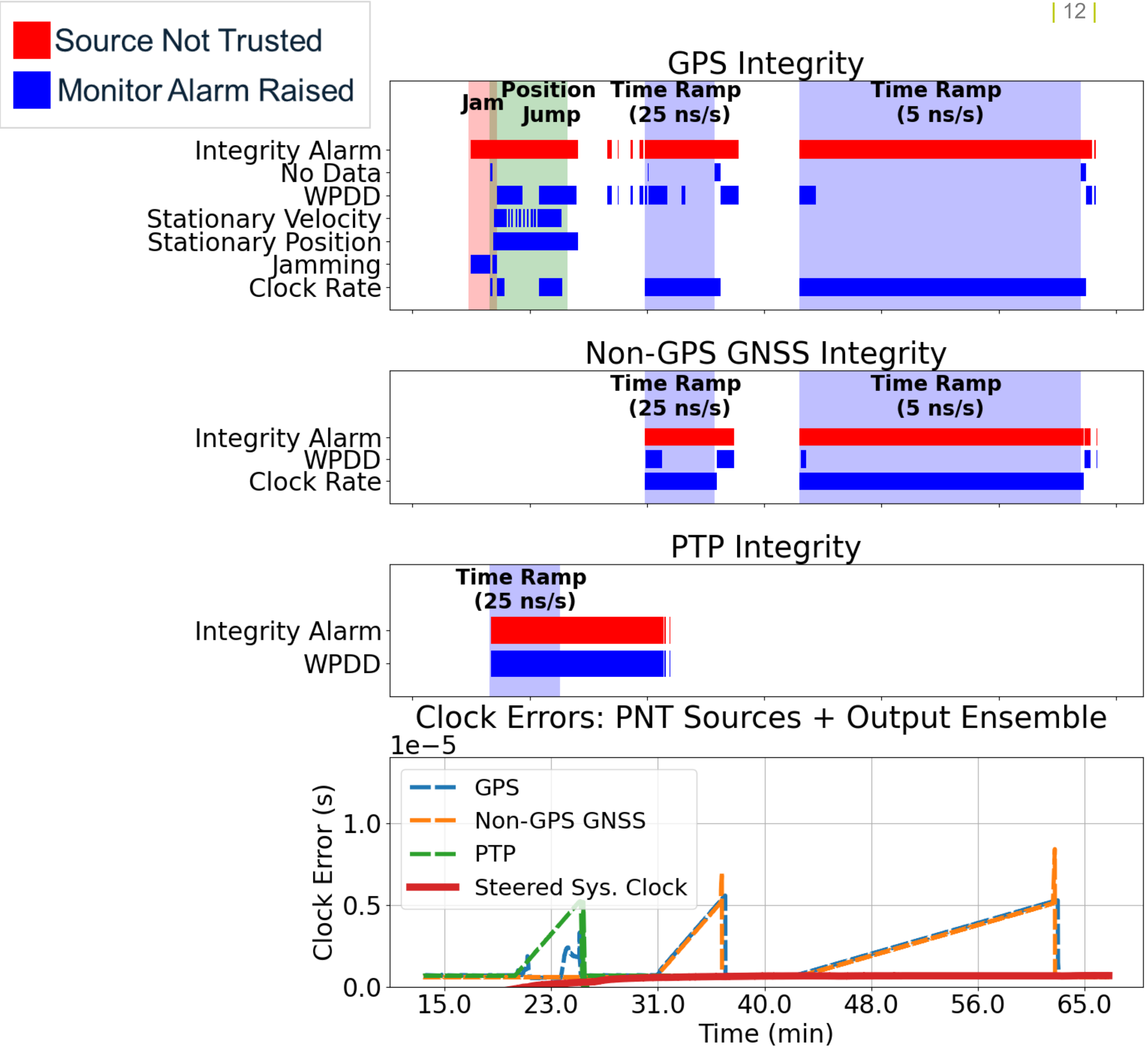
System Photo





Results and Evidence of PNT Resilience

How to read results



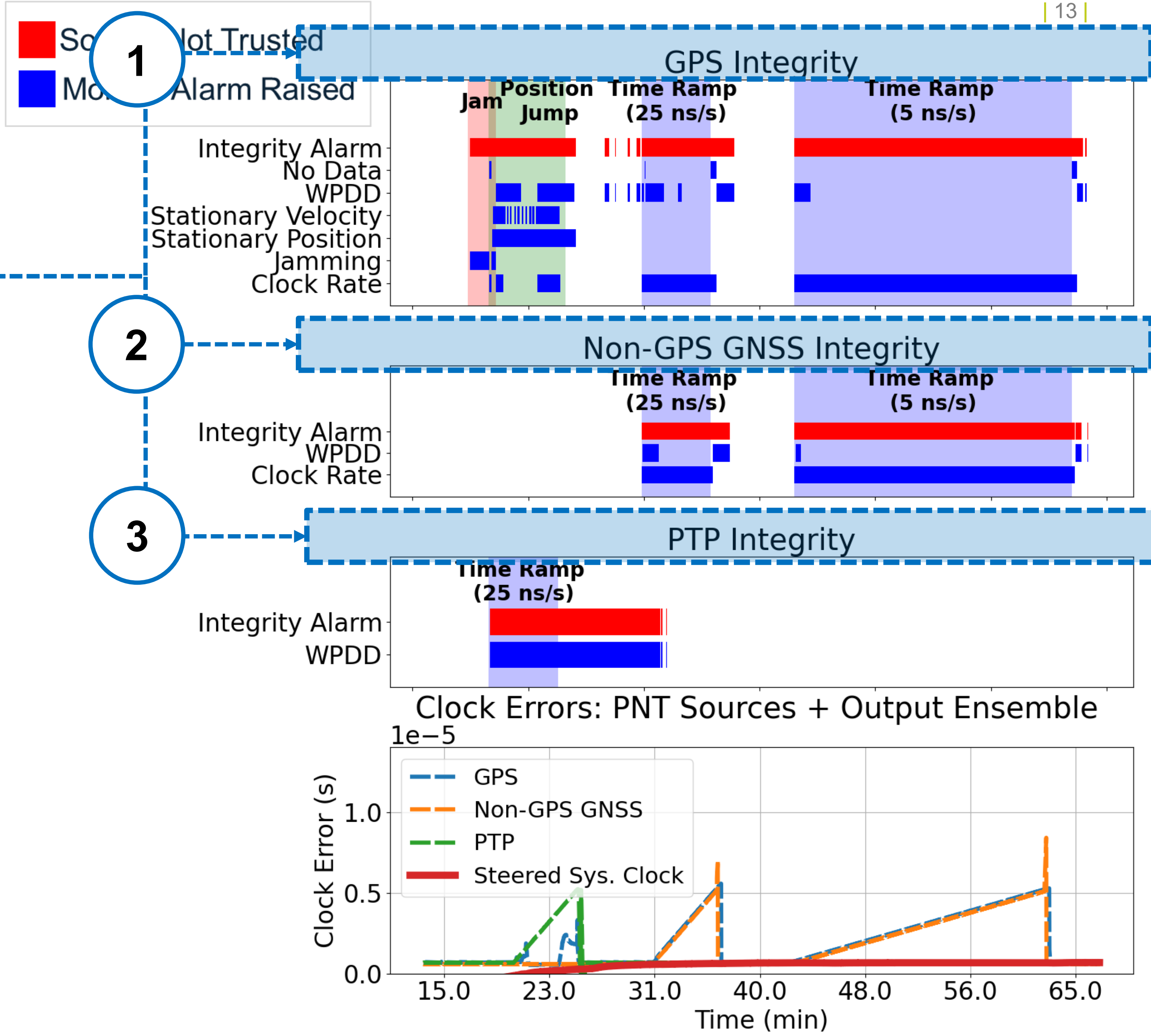
2. Apply defense in depth

6. Use broadly applicable threat mitigations

PTP: Precision Time Protocol
WPDD: Wiener Process Disorder Detector

How to read results

3 Sources



2. Apply defense in depth

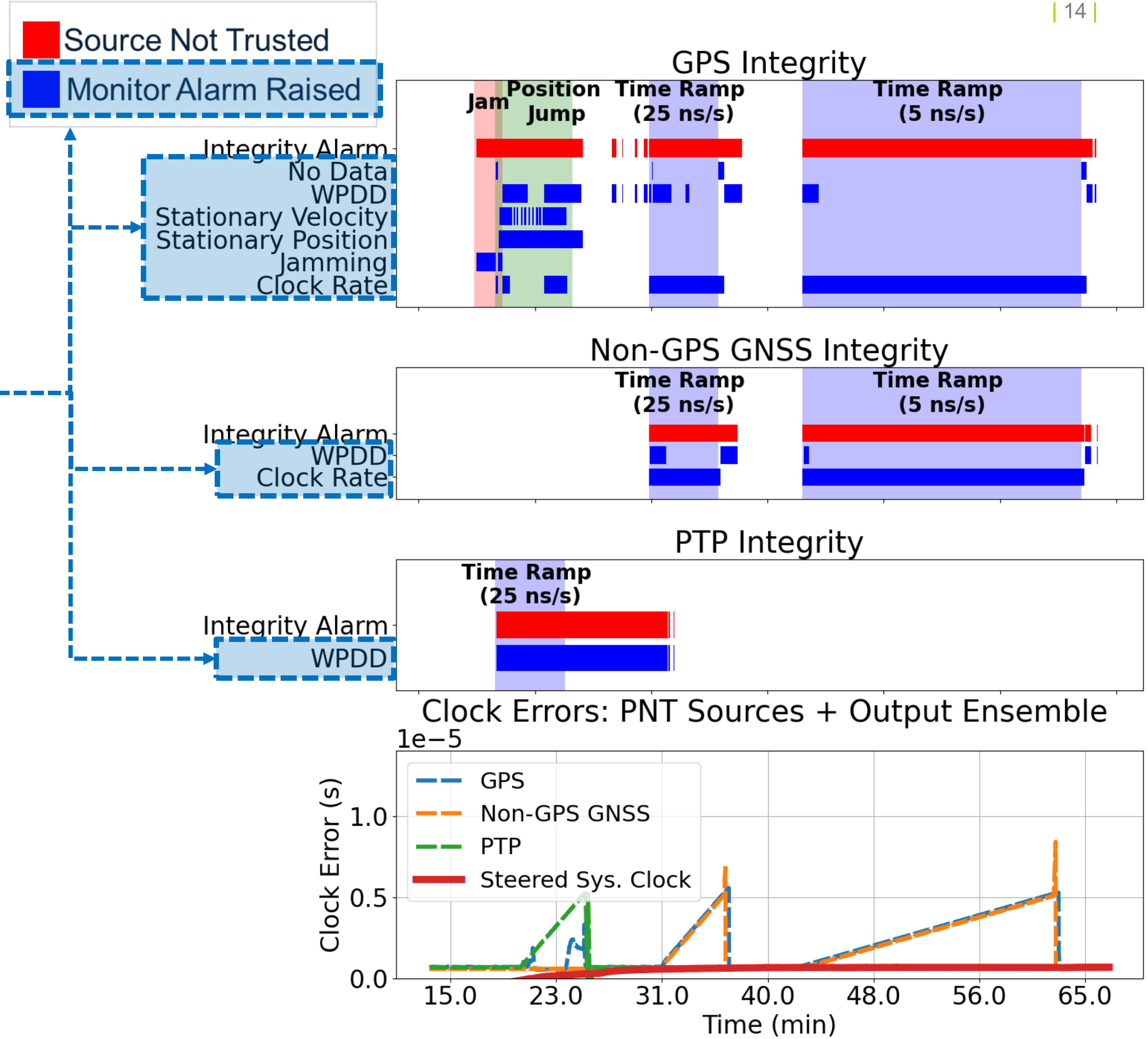
6. Use broadly applicable threat mitigations

PTP: Precision Time Protocol
WPDD: Wiener Process Disorder Detector

How to read results

3 Sources

Source Resilience Monitors
(Only monitors relevant to threats are shown)



2. Apply defense in depth

6. Use broadly applicable threat mitigations

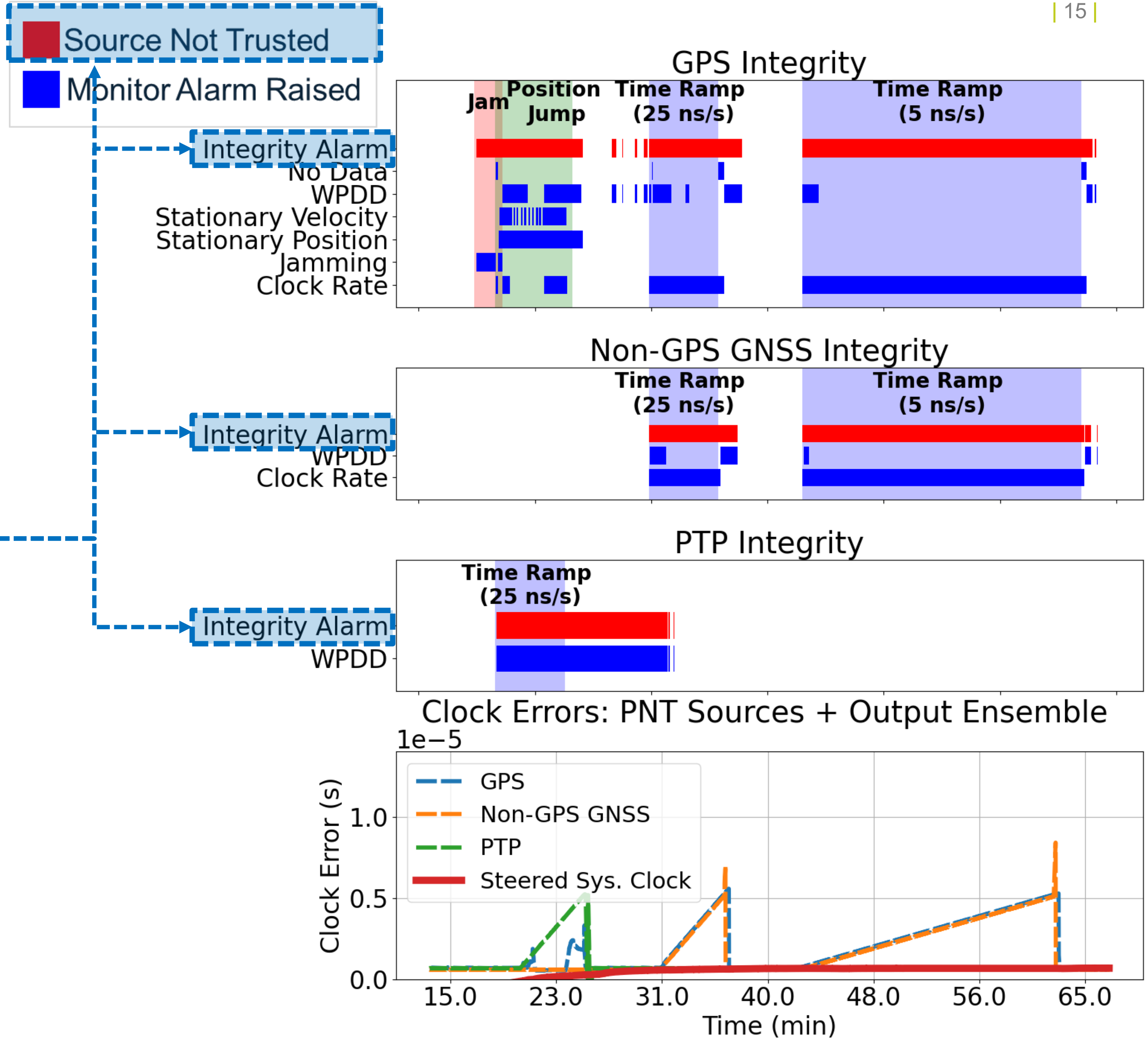
PTP: Precision Time Protocol
WPDD: Wiener Process Disorder Detector

How to read results

3 Sources

Source Resilience Monitors
(Only monitors relevant to threats are shown)

Source Integrity Alarm
(Source not trusted)



2. Apply defense in depth

6. Use broadly applicable threat mitigations

PTP: Precision Time Protocol
WPDD: Wiener Process Disorder Detector

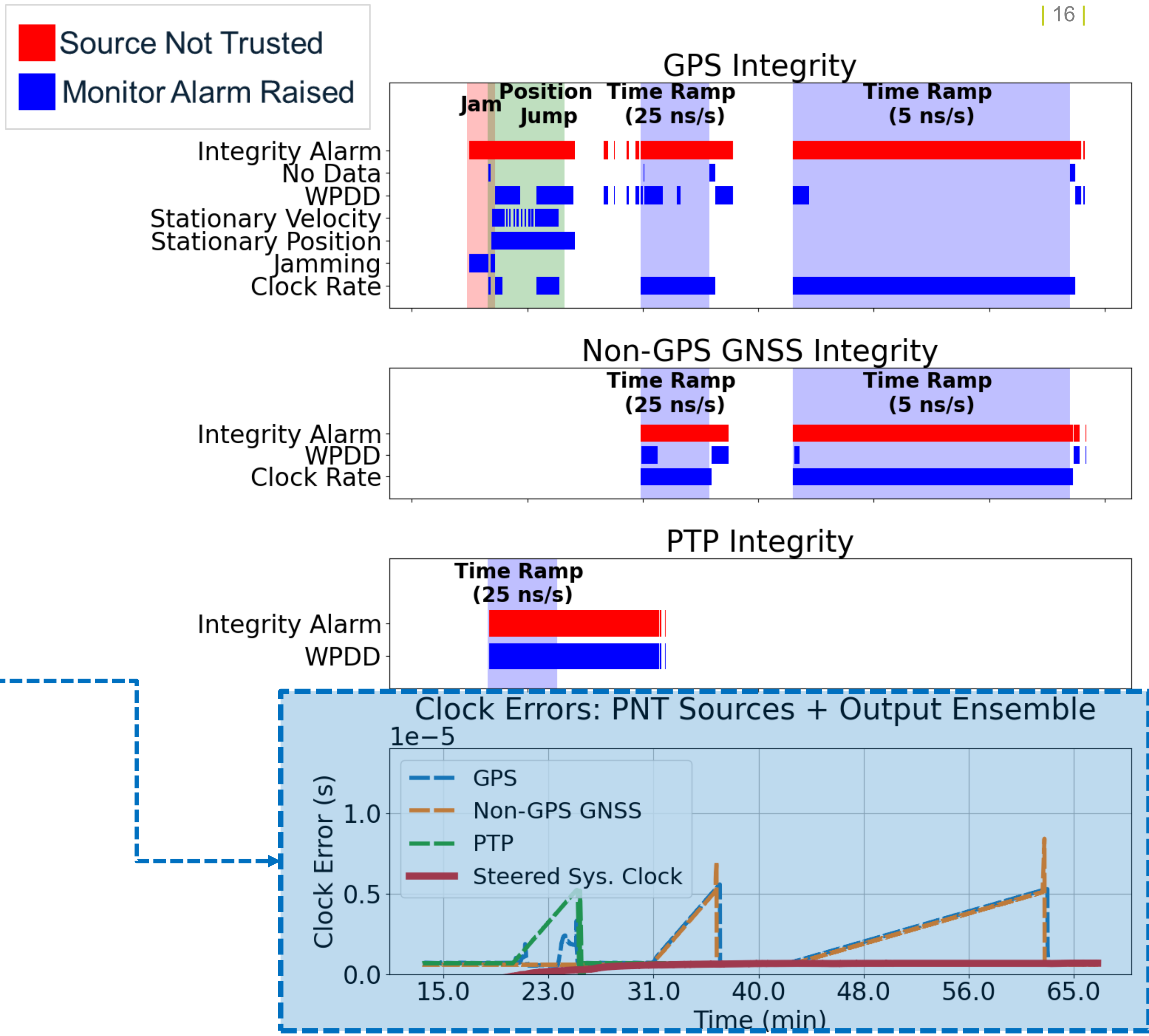
How to read results

3 Sources

Source Resilience Monitors
(Only monitors relevant to threats are shown)

Source Integrity Alarm
(Source not trusted)

Individual Source Clock Errors and Ensemble Result



2. Apply defense in depth

6. Use broadly applicable threat mitigations

PTP: Precision Time Protocol
WPDD: Wiener Process Disorder Detector

How to read results

3 Sources

Source Resilience Monitors
(Only monitors relevant to threats are shown)

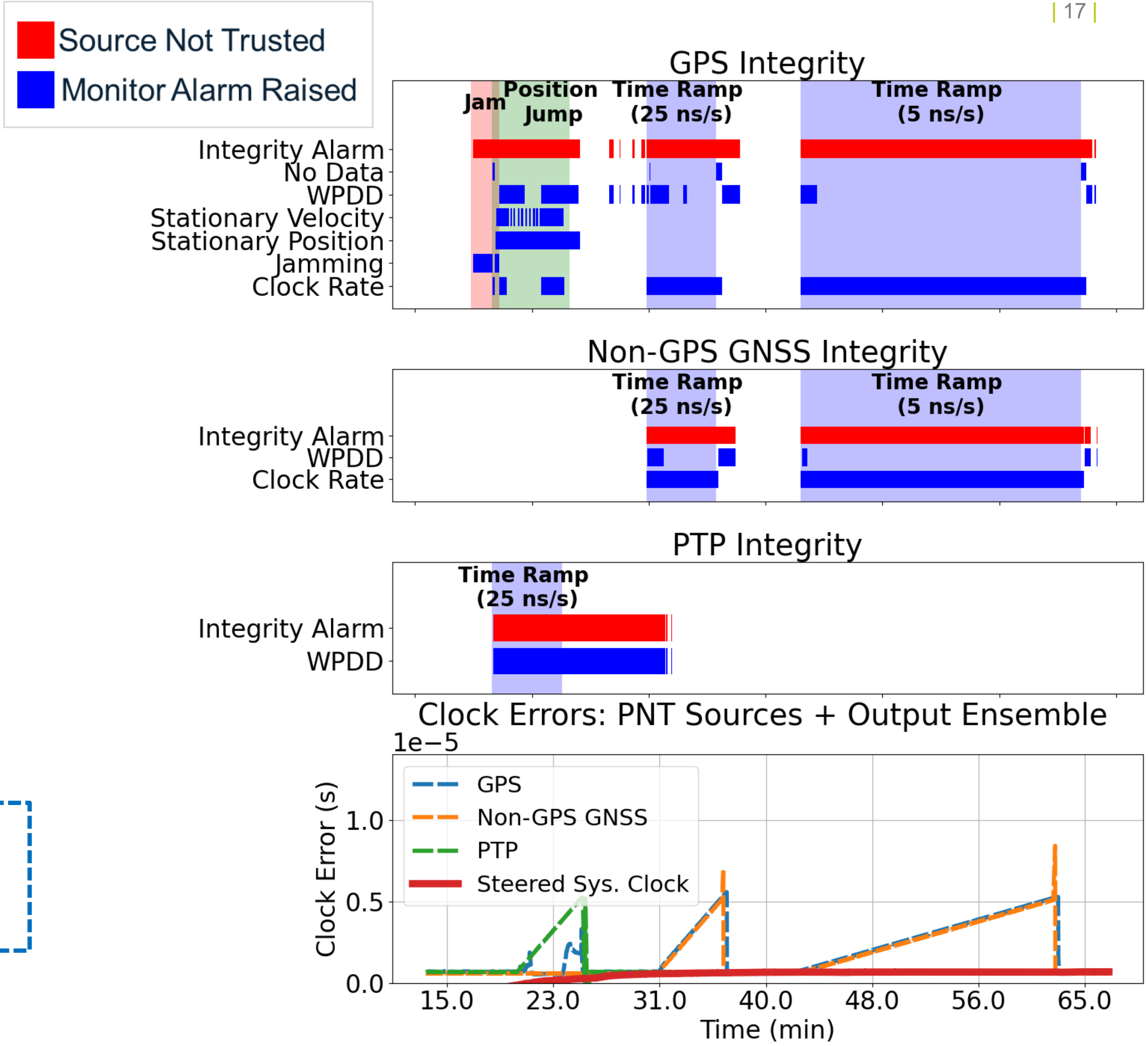
Source Integrity Alarm
(Source not trusted)

Individual Source Clock Errors and Ensemble Result

Resilience Concept(s) Demonstrated

2. Apply defense in depth

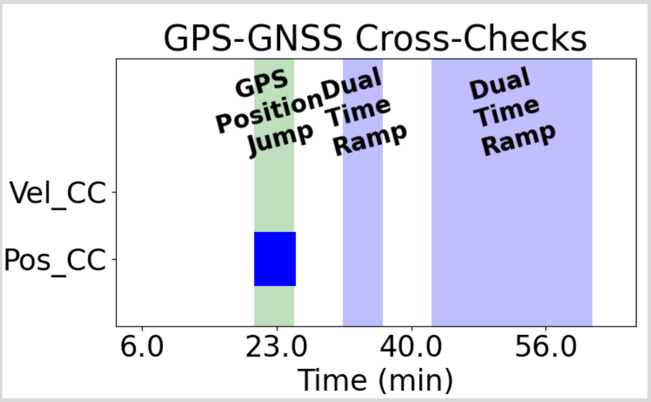
6. Use broadly applicable threat mitigations

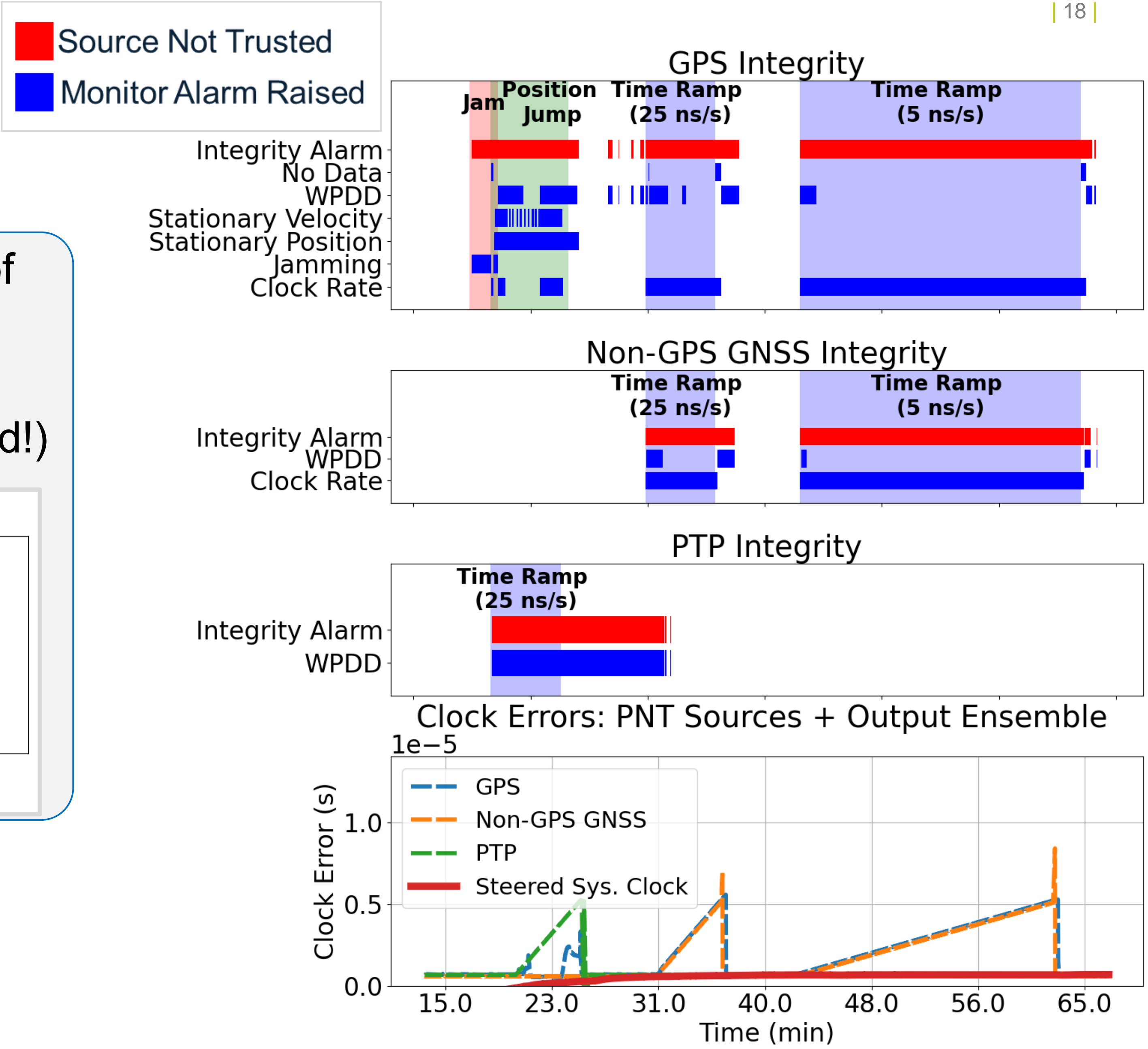


PTP: Precision Time Protocol
WPDD: Wiener Process Disorder Detector

Layered monitors defend against variety of threats

- Variety of **layered monitors** catch variety of threats
- **Defense in depth**: better threat coverage (obvious + subtle time ramp spoofs detected!)
- **Cross-checks**: position and time spoofs detected



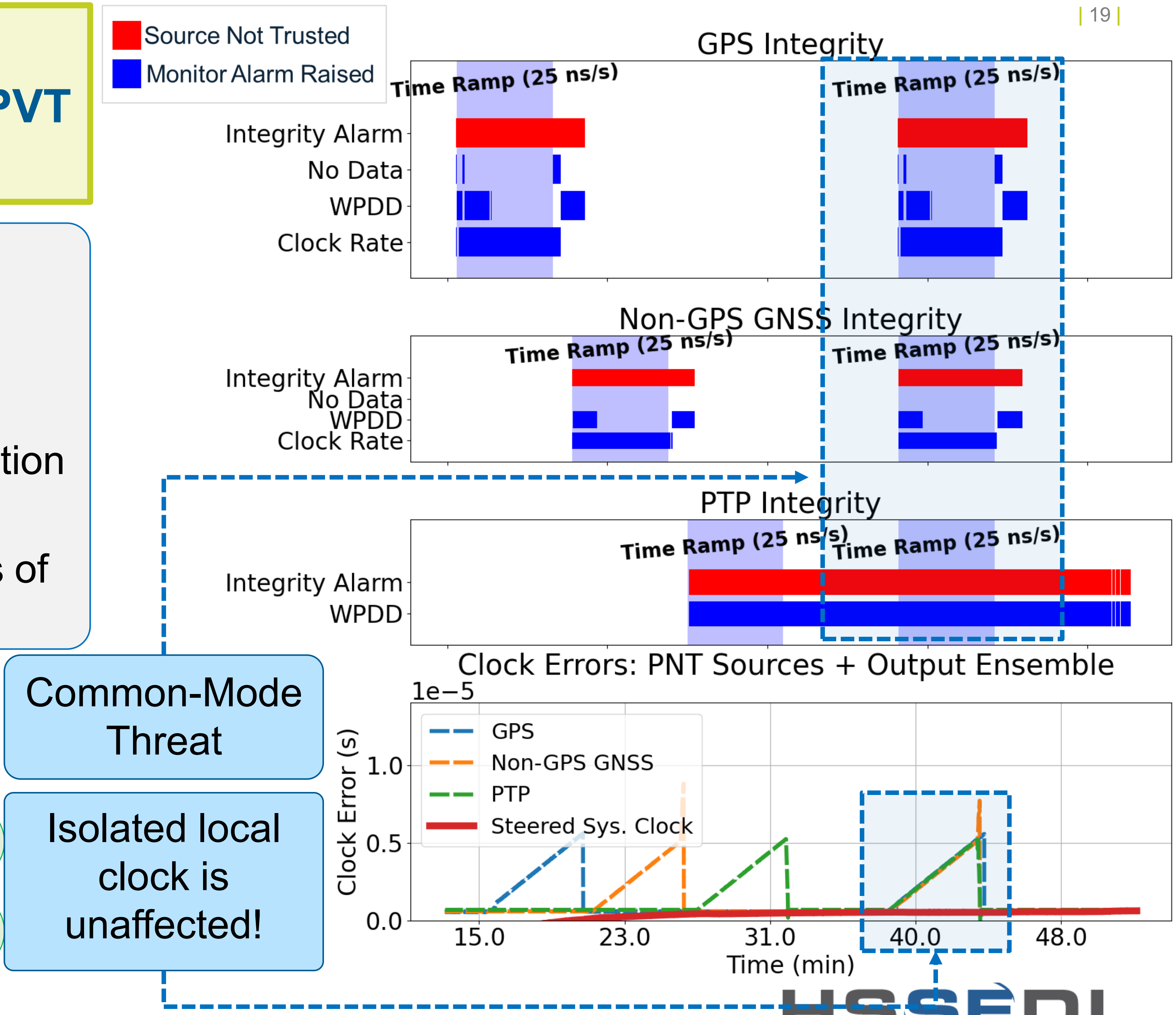


2. Apply defense in depth

6. Use broadly applicable threat mitigations

Isolating trusted core and "quarantining" sources keeps PVT solution trusted

- **Controlled information flow**: one source's output does not affect any other source
- **Managed trust**: source verification before adding incoming data to solution
- Keep **trusted core** protected: architecture design mitigates effects of common mode threats

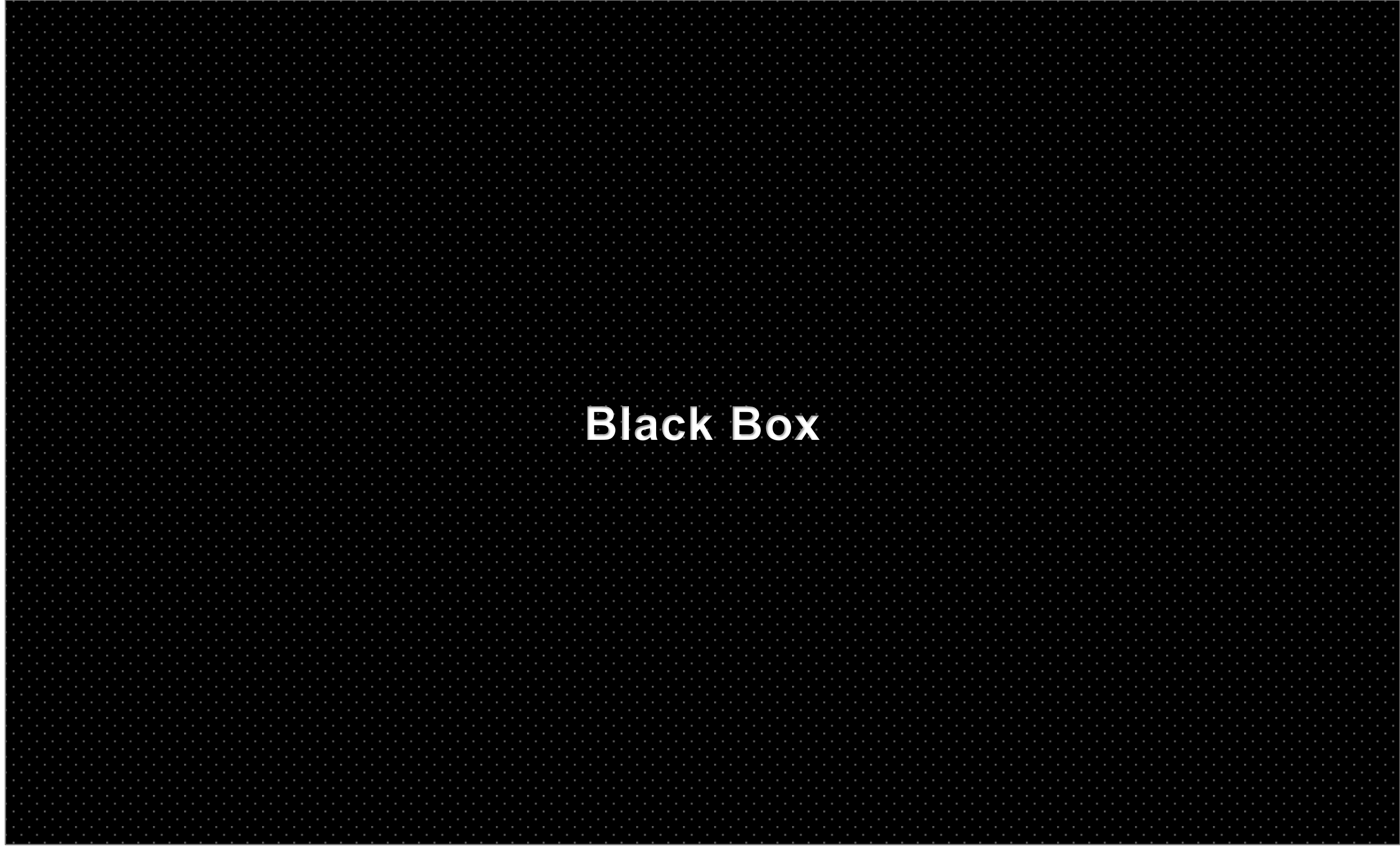


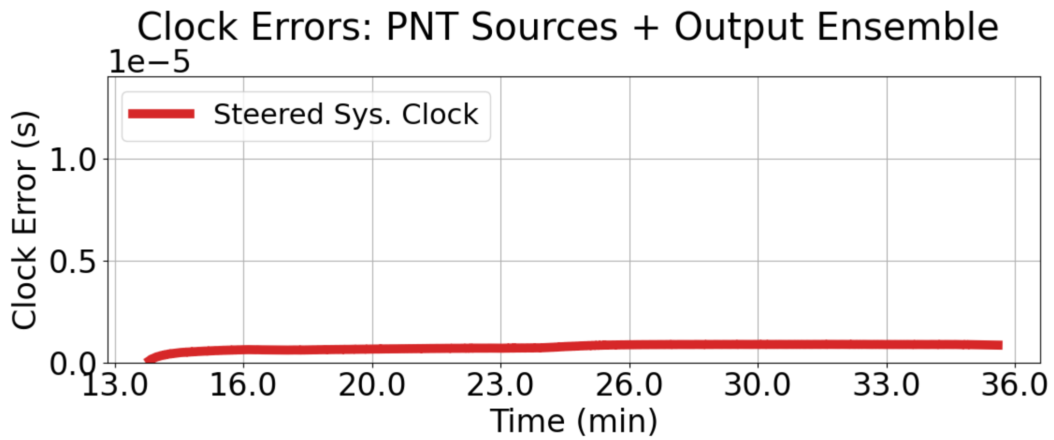
4. Managed trust from edge to core and between PNT sources

5. Protect internal PNT sources

Visible internal states for device evaluability and situational awareness

- **Transparency = key to integrity**
  - reporting needed for responsible use of PNT and user situational awareness
- **Recovery**
  - All integrity scores are "trusted" (especially cross-checks)
- **Motivation for evaluability**: IEEE standard conformity assessment





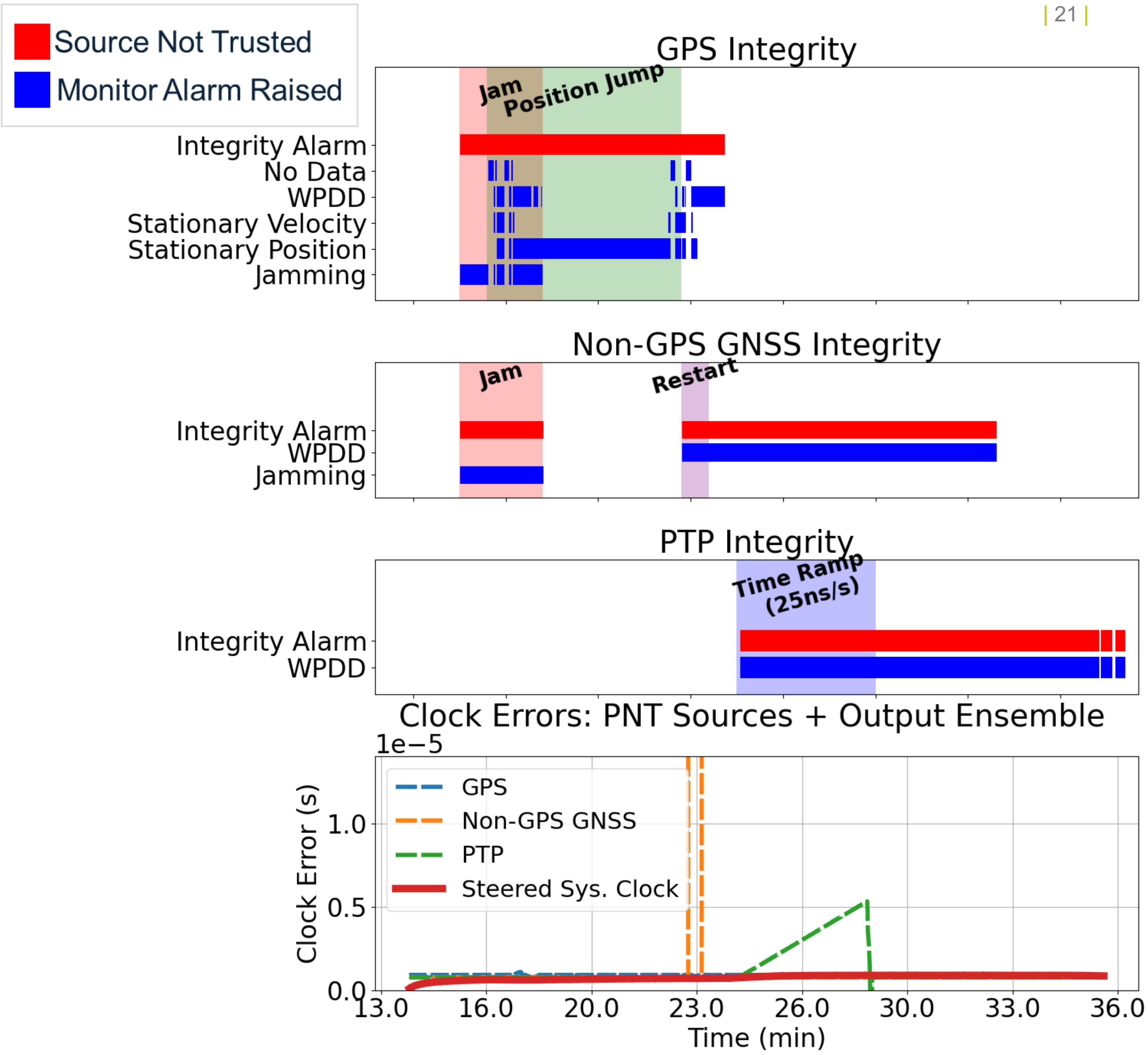
7. Recover when needed

HSSEDI
Homeland Security Systems Engineering & Development Institute™

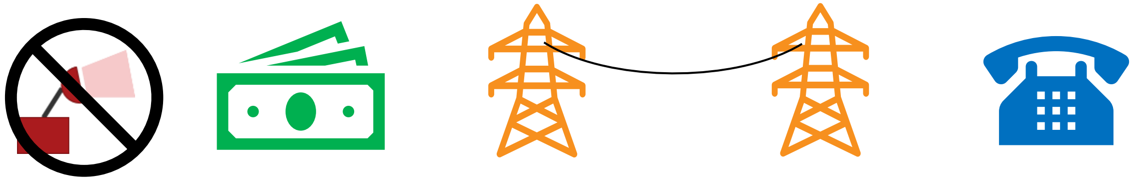
Visible internal states for device evaluability and situational awareness

- **Transparency = key to integrity**
  - reporting needed for responsible use of PNT and user situational awareness
- **Recovery**
  - All integrity scores are “trusted” (especially cross-checks)
- **Motivation for evaluability**: IEEE standard conformity assessment

7. Recover when needed



Concluding Thoughts



- **Assess PNT system conformity to upcoming standard**
  - "Will this device meet my PNT resilience needs?"
  - Ex. "I need a PNT source with Level 4 resilience to time ramp threats of 100ns/s or more"
- **Incorporate these concepts into new and existing PNT systems**
  - New: design from architecture
  - Existing: can do with commercially-available PNT sources

PNT Resilience Concepts

1. Assume attacks and disruptions to internal input
2. ☆ Apply defense in depth
3. Minimize attack opportunities
4. ☆ Manage trust from edge to core and between PNT sources
5. ☆ Protect internal PNT sources
6. ☆ Use broadly applicable threat mitigations
7. ☆ Recover when needed

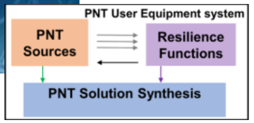
☆ Concepts highlighted in this brief

Highlighted References

Resilient Positioning, Navigation, and Timing (PNT) Conformance Framework

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

Resilient Positioning, Navigation, and Timing (PNT) Reference Architecture



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

- **DHS CISA Epsilon Algorithm Suite: https://www.cisa.gov/resources-tools/resources/epsilon-algorithm-suite**
- **DHS CISA PNT Integrity Library: https://www.cisa.gov/resources-tools/resources/pnt-integrity-library**
- **PNT Threats:**
  - Inside GNSS. FCC Fines Operator of GPS Jammer That Affected Newark Airport GBAS. https://insidegnss.com/fcc-fines-operator-of-gps-jammer-that-affected-newark-airport-gbas (2013)
  - Logan Scott / Inside GNSS. Spoofing Incident Report: An Illustration of Cascading Security Failure. https://insidegnss.com/spoofing-incident-report-an-illustration-of-cascading-security-failure/ (2017)

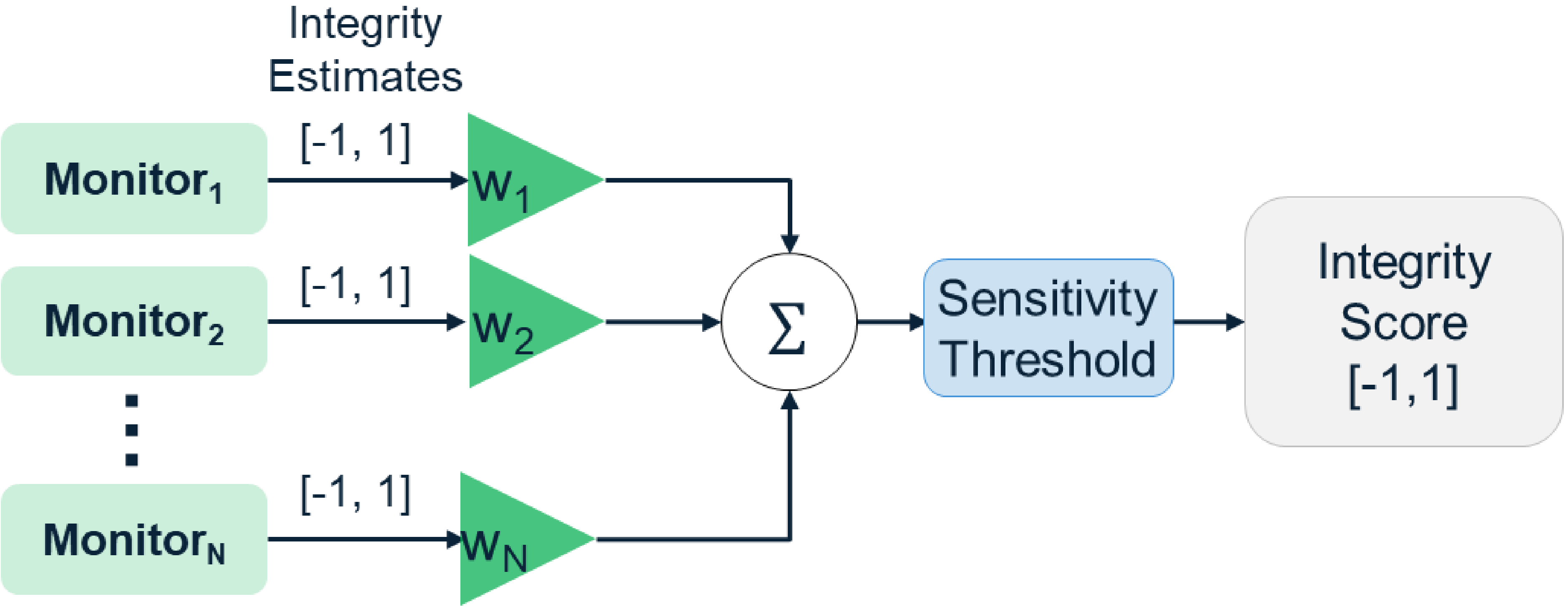
Further References

- PNNL. Energy Sector Position, Navigation, and Time Profile. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-30780.pdf
- Michael A. Lombardi / NIST. An Evaluation of Dependencies of Critical Infrastructure Timing Systems on the Global Positioning System (GPS). https://doi.org/10.6028/NIST.TN.2189 (2021)
- DHS. Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure. https://www.cisa.gov/sites/default/files/documents/Improving_the_Operation_and_Development_of_Global_Positioning_System_%28GPS%29_Equipment_Used_by_Critical_Infrastructure_S508C.pdf
- IEEE SA. Standard for Resilient Positioning, Navigation and Timing (PNT) User Equipment. https://sagroups.ieee.org/p1952/
- RAND. Analyzing a More Resilient National Positioning, Navigation, and Timing Capability https://www.rand.org/pubs/research_reports/RR2970.html (2021)
- Safran. 10 Reasons Why Time is Critical for Trading Systems. https://safran-navigation-timing.com/10-reasons-why-time-is-critical-for-trading-systems/
- Inside GNSS. FCC Fines Operator of GPS Jammer That Affected Newark Airport GBAS. https://insidegnss.com/fcc-fines-operator-of-gps-jammer-that-affected-newark-airport-gbas (2013)
- Logan Scott / Inside GNSS. Spoofing Incident Report: An Illustration of Cascading Security Failure. https://insidegnss.com/spoofing-incident-report-an-illustration-of-cascading-security-failure/ (2017)
- Jeff Dagle / PNNL. Electric Power Applications Enabled by Wide-Area Synchronized Time. https://www.gps.gov/cgsic/meetings/2023/dagle.pdf. (2023)
- Humphreys, Todd. GPS Spoofing and the Financial Sector. http://hdl.handle.net/2152/63513 (2011)
- John A. Volpe National Transportation Systems Center (U.S.). Vulnerability assessment of the transportation infrastructure relying on global positioning system. https://rosap.ntl.bts.gov/view/dot/8435 (2001)
- John W. Betz, Brady W. O'Hanlon, Bradley A. Moran. Canonical Use Cases for Critical Infrastructure. https://www.gps.gov/governance/advisory/meetings/2023-12/betz.pdf (2023)
- Patricia Larkoski / HSSEDI. Resilient PNT Reference Architecture for Timing Applications https://www.gps.gov/cgsic/meetings/2021/larkoski.pdf (2021)
- Ernest Wong / DHS S&T. A Cybersecurity Perspective to Addressing PNT Vulnerabilities. https://www.gps.gov/cgsic/meetings/2022/wong.pdf (2022)
- Brad Moran, Patricia Larkoski. Resilience Evaluation for Timing Systems. https://wsts.atis.org/presentation/resilience-evaluation-for-timing-systems/ (2023)

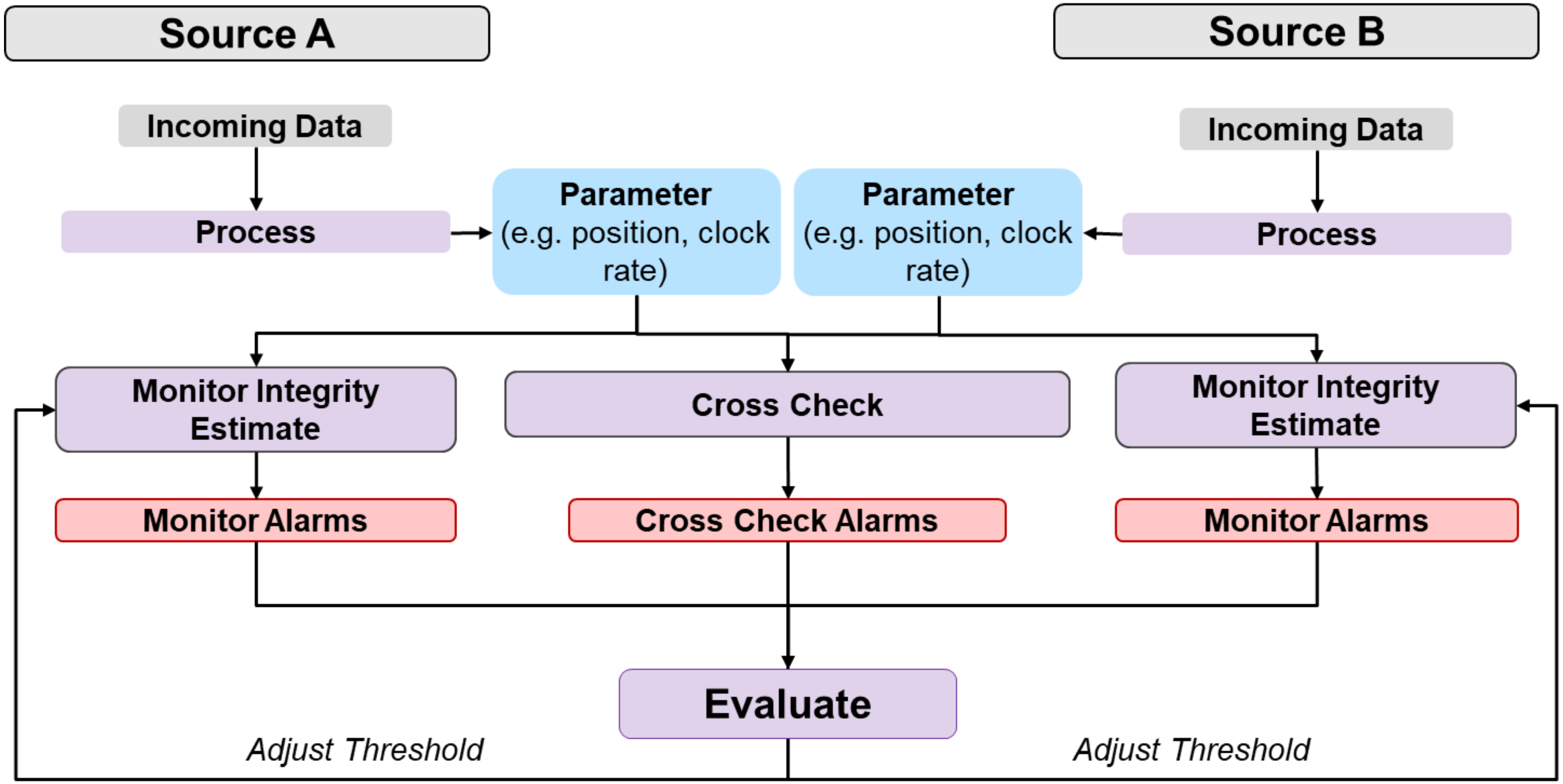
Backup

Monitor Fusion

- **Based on PNT Integrity Library monitor fusion:**
- **The implementation has since expanded to include monitor cross-checks**

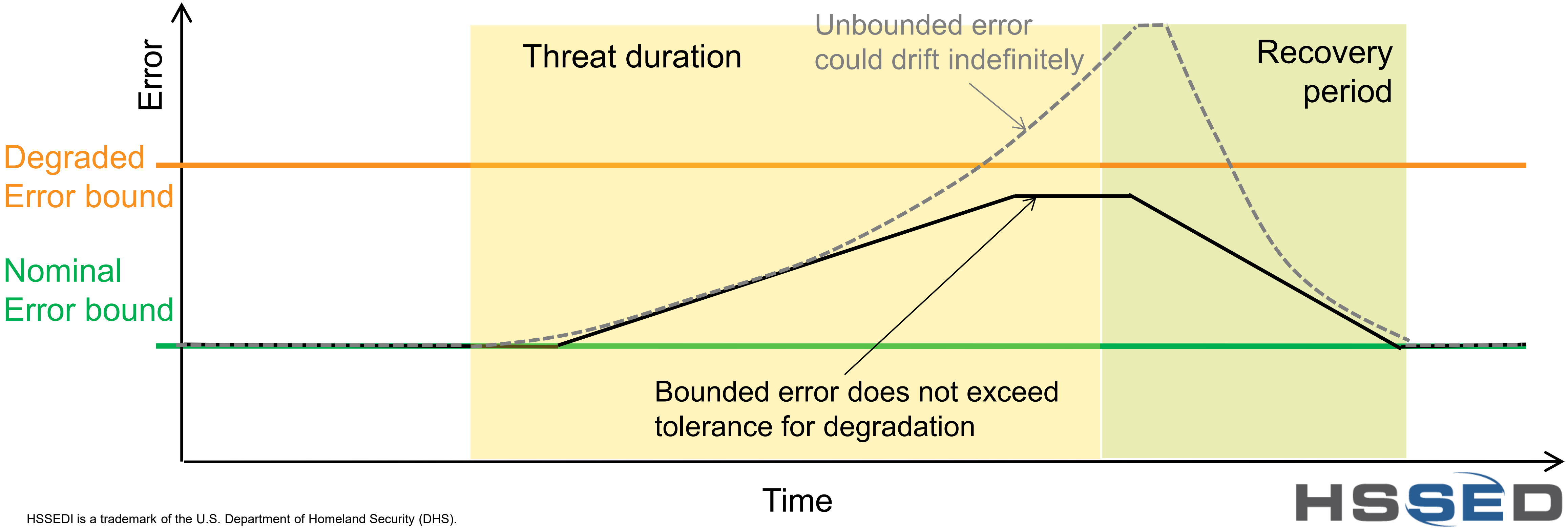


Monitor Cross-Checks



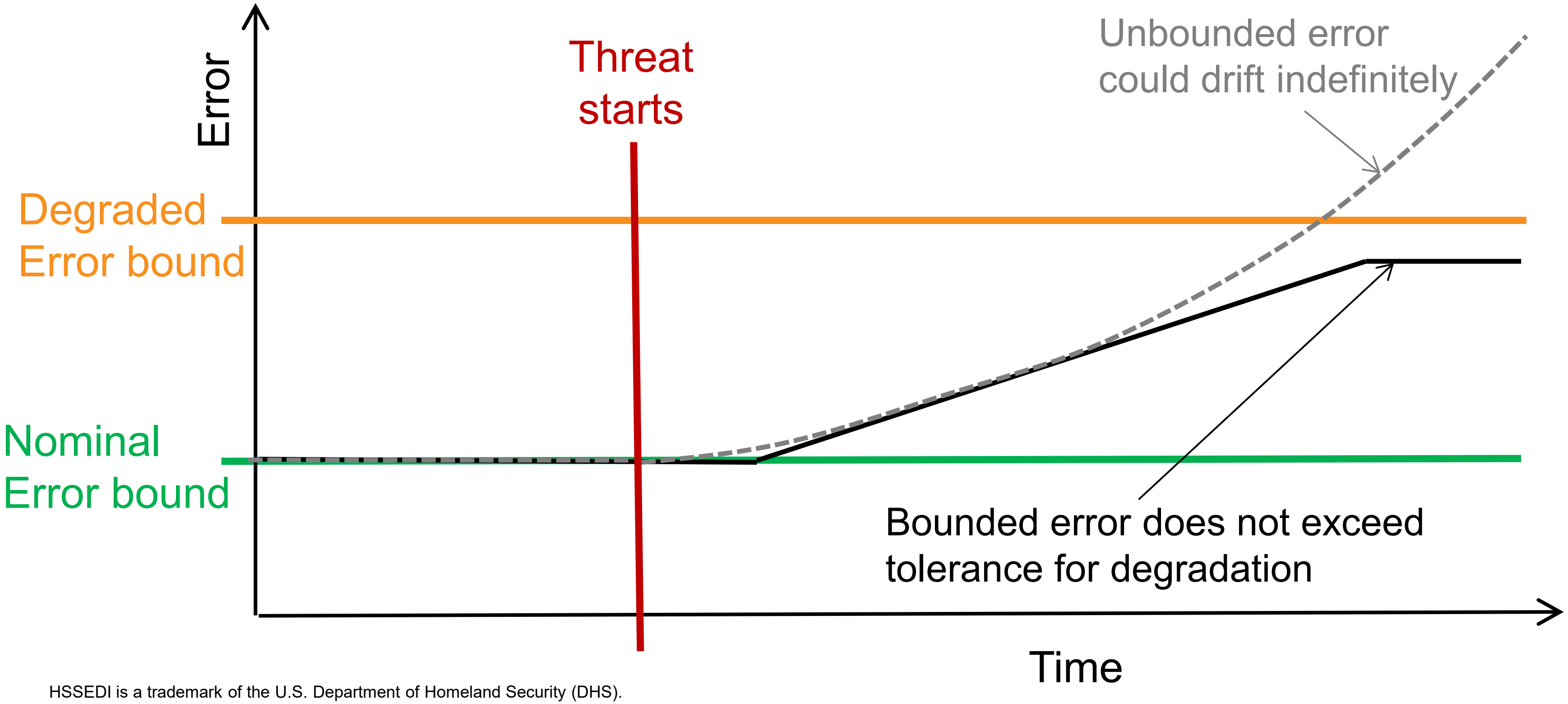
Bounded/Unbounded Error

- **From the DHS S&T Conformance Framework:**
  - "Bounded degradation means that the performance may be reduced compared to nominal operation within well-characterized tolerance limits throughout the degraded period."
  - See: https://www.dhs.gov/publication/st-resilient-pnt-conformance-framework



Bounded/Unbounded Error

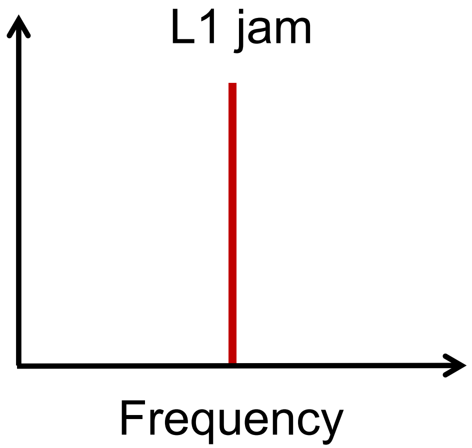
- **From the DHS S&T Conformance Framework:**
  - "Bounded degradation means that the performance may be reduced compared to nominal operation within well-characterized tolerance limits throughout the degraded period."
  - See: https://www.dhs.gov/publication/st-resilient-pnt-conformance-framework



- A free running clock can have unbounded error due to drift
- Degraded bounded error may result from disciplining a clock with a different source of external input after a threat is detected for the primary source of external input.

Jamming and Spoofing in Demonstration

Jam

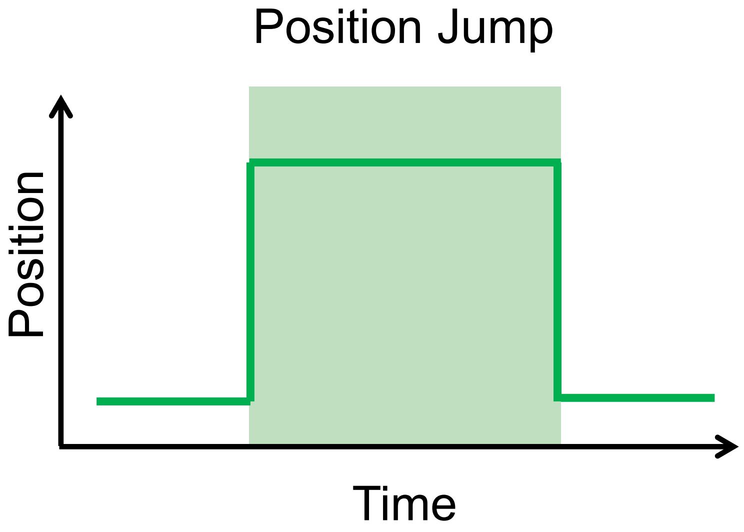


Band: GPS L1

Waveform: Tone

Duration: 3 min

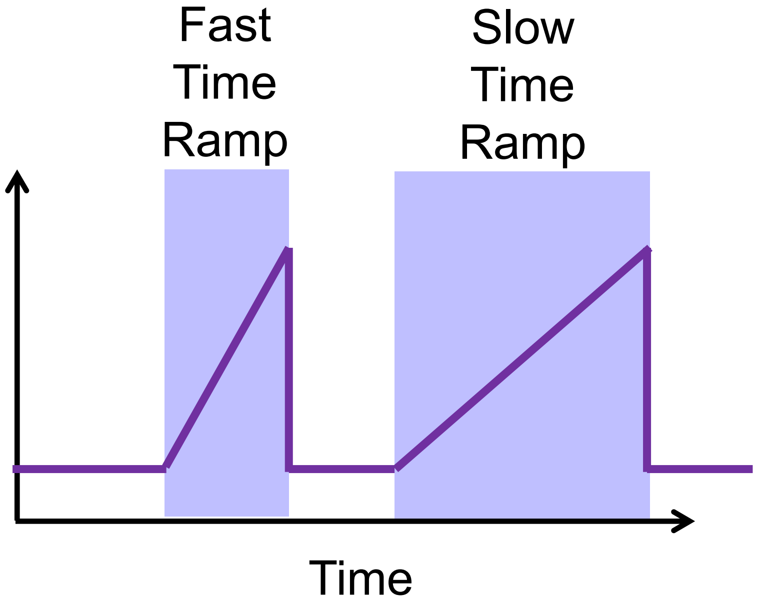
Jump



Jump distance: 500 m

Duration: 5 min

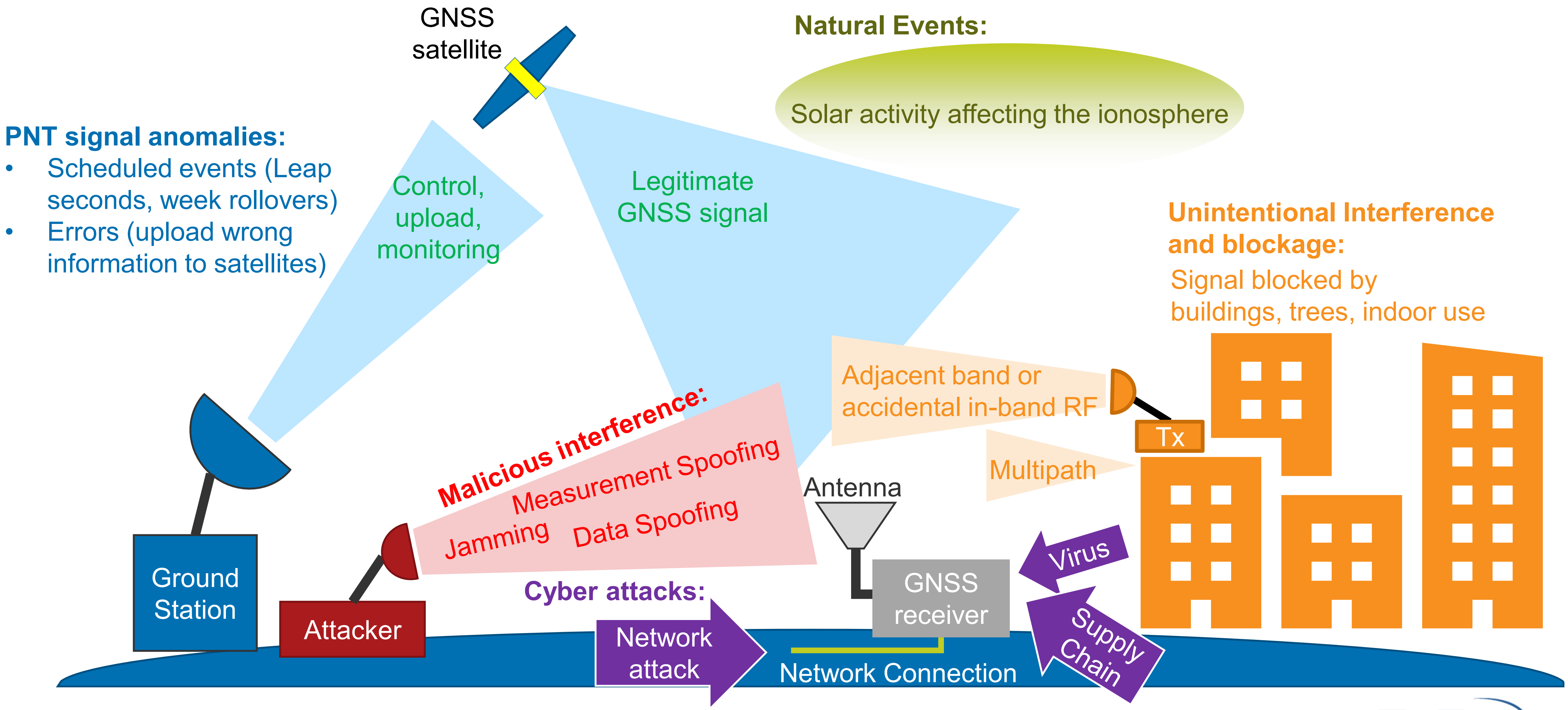
Ramp



Ramp Speed: 25 ns/s (fast); 5 ns/s (slow)

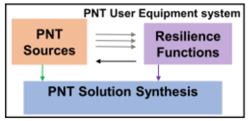
Duration: 4 min (fast); 20 min (slow)

Threat Types

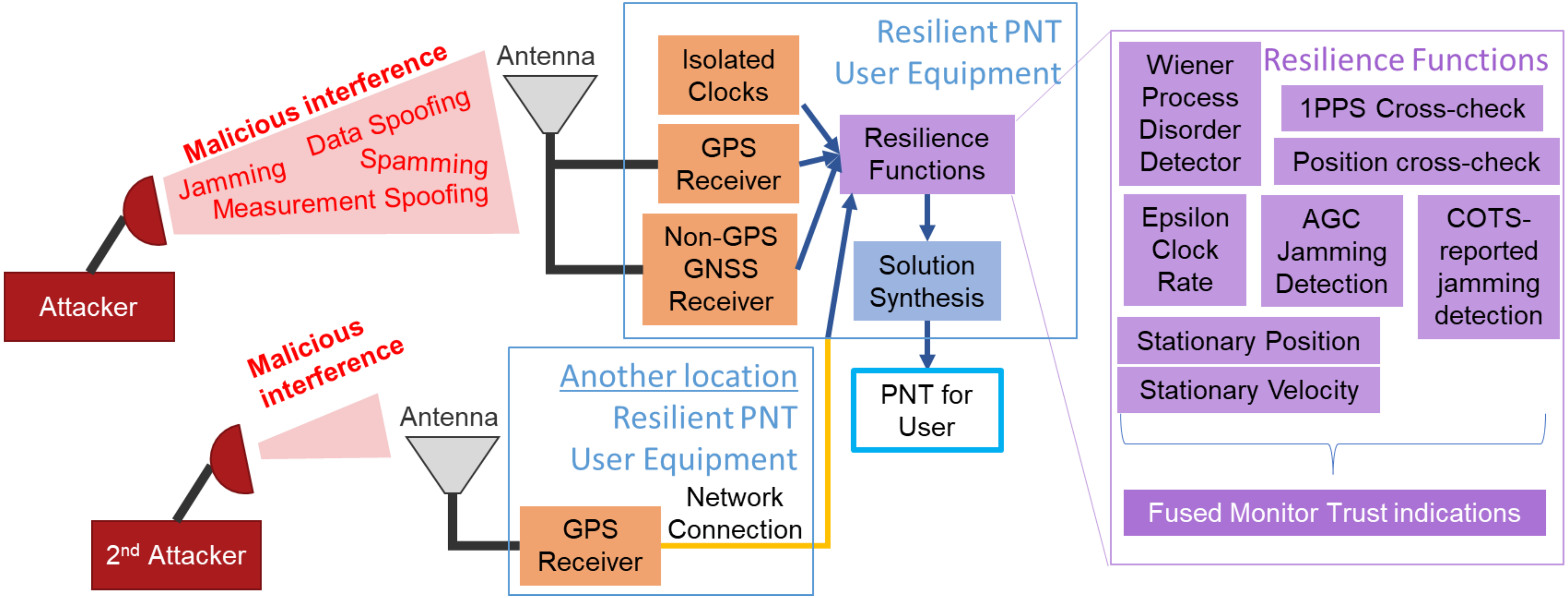


Proposed Use Cases (1 of 3)

Use Case	PNT Func.(s)	Meas. Accuracy	Service Region	Operating Conditions	CSWaP	Ref.
Cellular Base Station: Intercell Interference	T	± 1 µs	Entire U.S.	All Terrestrial	Mod.	1
Cellular Base Station: Carrier Aggregation	T	± 0.13 µs	Entire U.S.	All Terrestrial	Mod.	2
Phasor Measurement Unit	T	± 1 µs	Entire U.S.	All Terrestrial	Mod.	3
Financial Trading	T	± 50 µs	Urban Areas	All Terrestrial	High	3
Positive Train Control	P	2D 1 m (2DRMS)	Entire U.S.	All Terrestrial	High	3
Precision Agriculture, Other Commercial	P, N	±1 cm H, ±1.5 cm V	Entire U.S.	All Terrestrial	Mod.	–

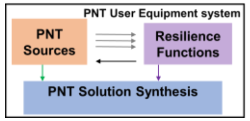


Resilience: From Concepts to Architecture to Implementation

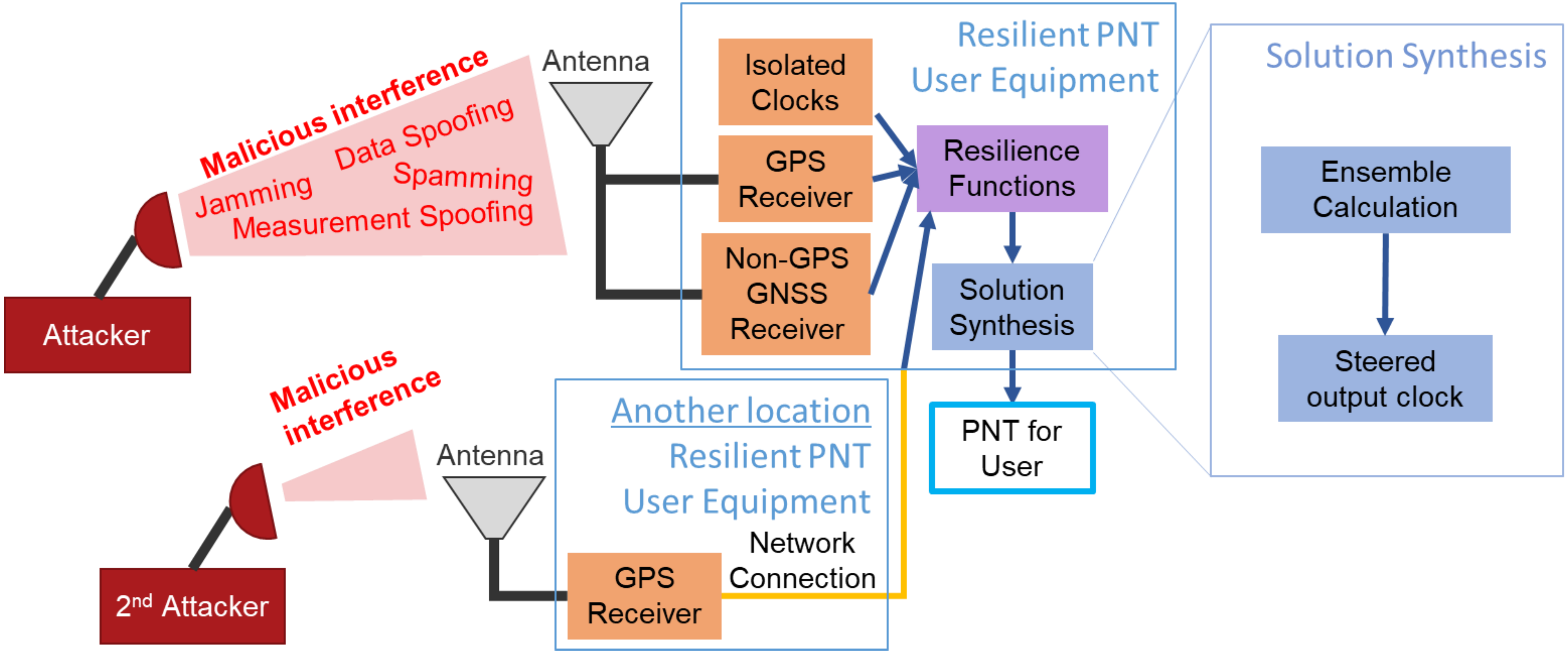


We built an example resilient timing system to demonstrate practicality and reduce commercial development risk

HSSEDI
Homeland Security Systems Engineering & Development Institute™



Resilience: From Concepts to Architecture to Implementation



We built an example resilient timing system to demonstrate practicality and reduce commercial development risk

There are many ways to implement the architecture

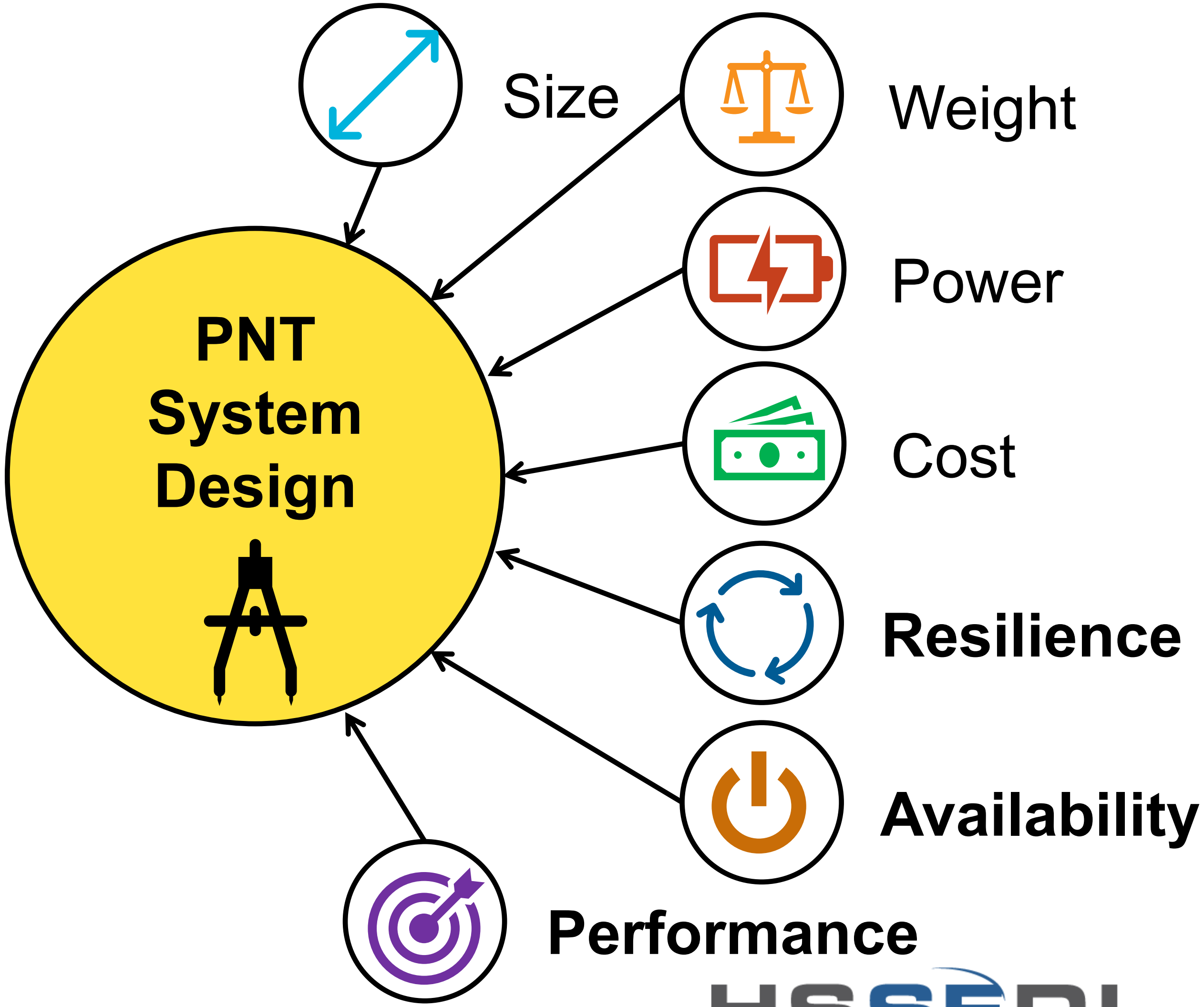
PNT Source Selections
- GPS Receiver
- Non-GPS GNSS Receiver
- Precise Time Protocol (PTP)
- Isolated sources:
  - Low-SWAP atomic clock
  - Oven-Controlled Crystal Oscillator (OCXO)
- **Many other options such as:**
  - Multi-GNSS Receiver
  - Software-Defined Receiver
  - Network Time Protocol
  - Two-way Satellite Time Transfer
  - Lab-grade reference
  - TCXO, MEMS

Threat Detection Monitor Selections
- Stationary Position & Velocity Monitors
- Clock Rate Monitor
- Wiener Process Disorder Detector (WPDD)
- Automatic Gain Control Jamming Monitor
- Commercial Receiver Built-in Jamming Monitor
- Cross-checks: Position, Velocity, 1-pulse-per-second (PPS) Measurements
- Monitor Fusion based on PNT Integrity Library
- **Many more options such as:**
  - Cumulative Innovations Monitor
  - Clock Consistency Divergence Monitor
  - Cryptographic Authentication (like GALILEO NMA)
  - Signal Angle of Arrival Monitor
  - GNSS message data cross-checks
  - CAF peak monitors, Carrier-to-noise monitor, Signal angle of arrival monitor
  - Pos/vel monitors that assume specific dynamics)

Solution Synthesis Selections
- **Calculate the solution based on source trustworthiness**
  - Ensemble PNT sources
  - Switch between PNT sources, e.g., as a Primary-Alternate-Contingency-Emergency (PACE) plan would
- **Solution Realization:**
  - Steer independent output oscillator
  - Use output directly from a PNT source (for switching option)
  - Use auxiliary output generator

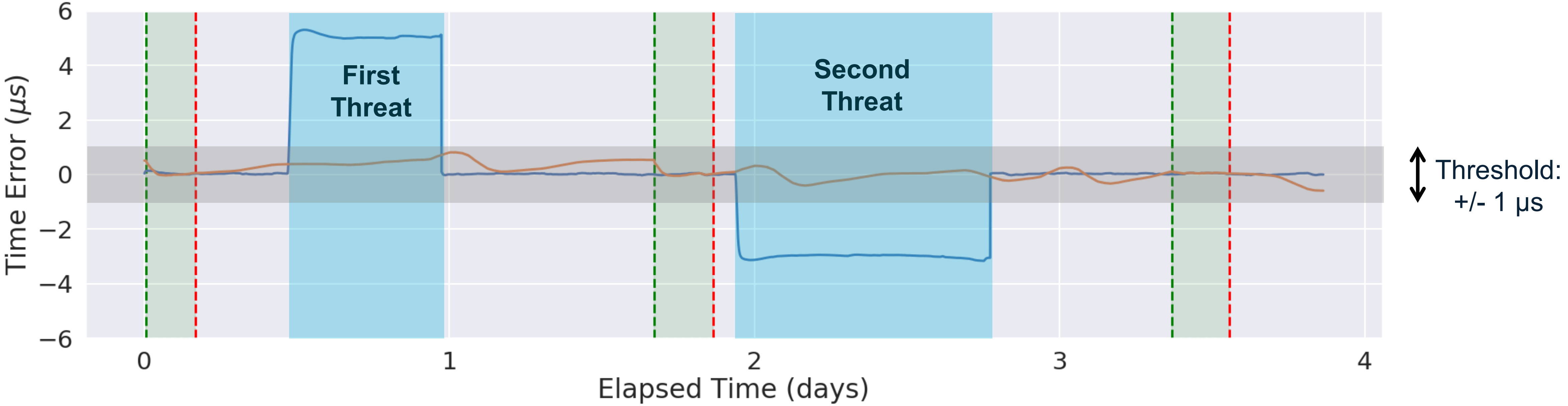
Trade-Space: Size, Weight, Power, Cost, and *Resilience*

- **SWaP-CR:**
  Resilience is another dimension to the usual SWaP-C trade-space considerations.
- **Resilient PNT UE will withstand and recover from disruptions. Without resilience, UE optimized only for SWaP-C may not perform when needed.**
- **Availability and Performance of system output is another trade-off**



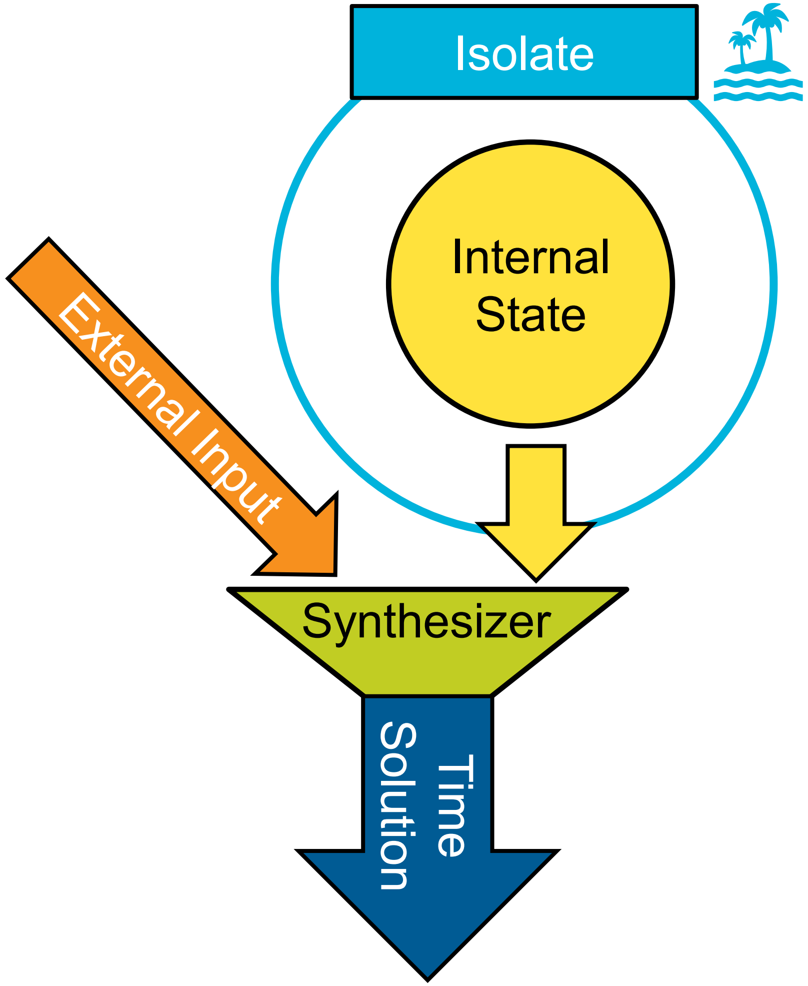
Resiliency versus Accuracy

- **Optimize PNT Systems for resilient behavior rather than a typical metric, such as accuracy**
  - **Clock 1**: Not resilient to threats, better accuracy
  - **Clock 2**: Resilient to threats, accuracy is still within the application threshold



Applying Resilience to Timing Control – Long Term

- **Maintain a protected internal state**
  - Ex: a local clock/oscillator
- **The more isolated the internal state is from the rest of the system, the more protected it is from corrupted external input**
  - **Isolate the internal state all the time** for the most secure resilience
    - Resilient timing control algorithms apply corrections to the internal state using a synthesizer
    - More control over system output (Ex: facilitates rollback to a good state)
    - Isolate external inputs as well

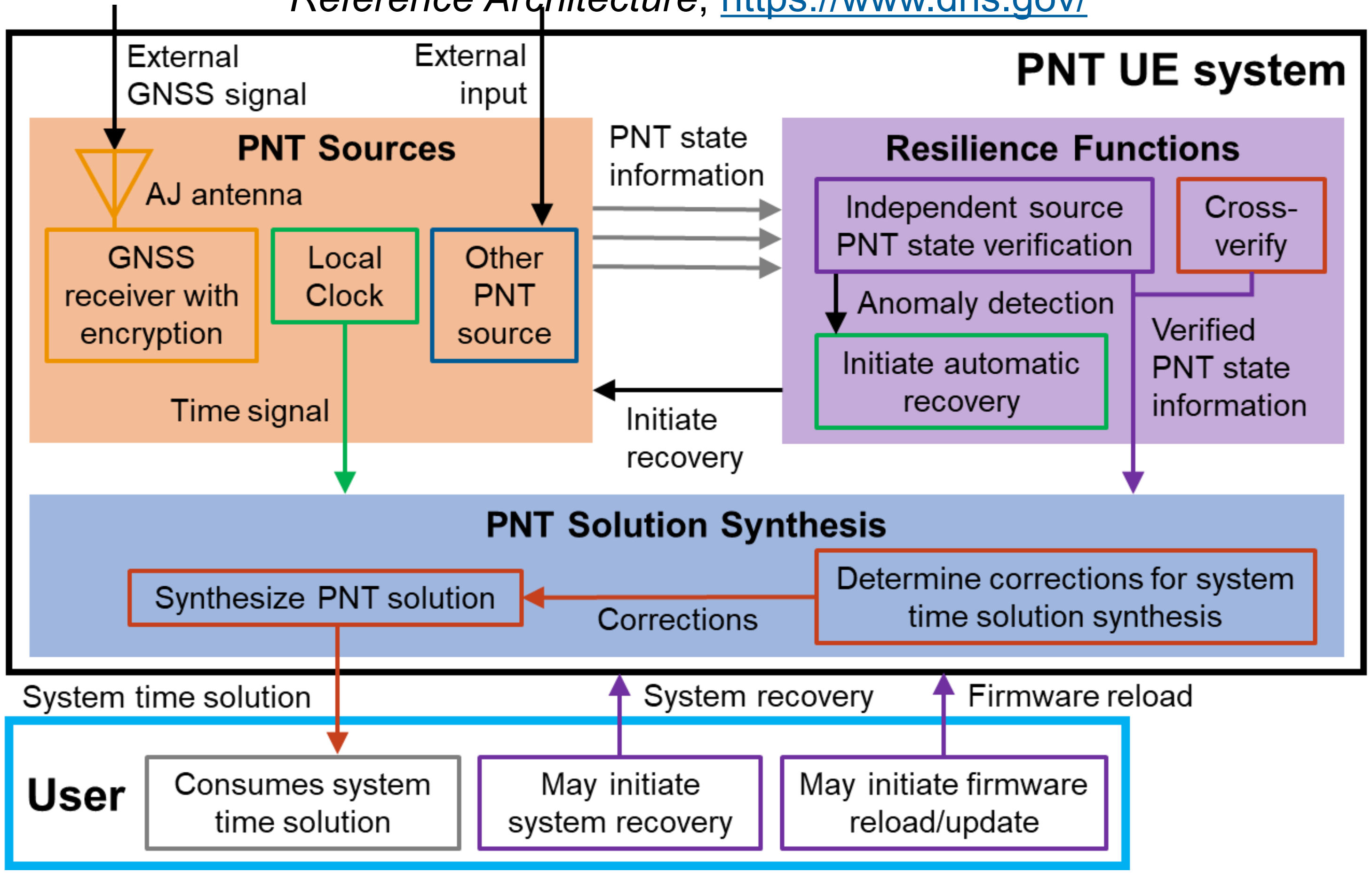


Resilient PNT Reference Architecture

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

Many opportunities for UE to provide evidence of resilient behavior

Types of components in a resilient PNT system, from *Resilient PNT Reference Architecture*, https://www.dhs.gov/



Notional conformity assessment table

Statement implies specific threat against which the system is resilient

Example resilience statement:

The system {name}, when subjected to {threat info}, can provide timing at Resilience Level {#} with {performance}.

Resilience Level numbers here indicate higher=better resilience. In future, levels in a table like this will correspond to the P1952 standard. The performance level must also be specified.

A CI owner/operator with knowledge of desired resilience level and relevant threats can select the system that meets their needs.

Threat → System ↓	GPS Time jump ≥100ns for ≤10min	MGNSS Time jump ≥100ns	GPS position walk-off ≥1m/s	MGNSS position walk-off ≥1m/s	GPS data spoof: unexpected week number rollover
Critical Infrastructure Need	5	4	3	2	4
Candidate System A	3	1	4	2	5
Candidate System B	2	1	3	1	1
Candidate System C	5	4	5	3	2

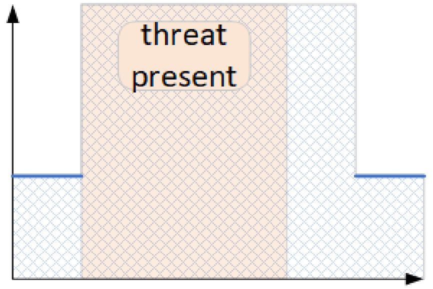
H
T

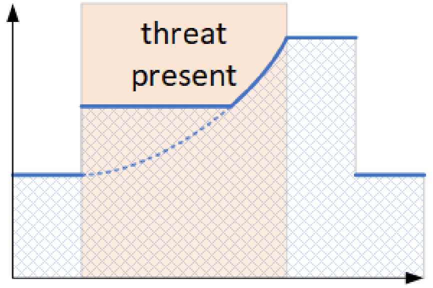
Introduction to Resilience Levels

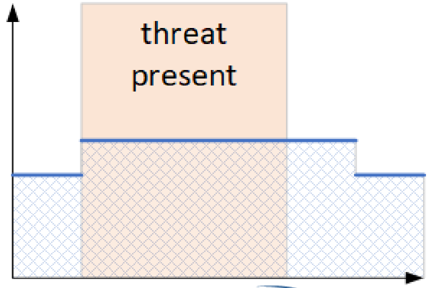
Level*	Behavior
Level 1	**Ensures recoverability after removal of the threat.** [RS] 1. Must support robust system recovery, making all memory clearable or resettable, enabling return to a trusted configuration, and returning to the defined performance after removal of the threat. [RS, RC] 2. Must validate that stored data from external sources adheres to values and formats of established standards. [P] 3. Must include the ability to securely reload or update firmware. [RC]
Level 2	**Continues providing a solution (possibly with degradation) during threat.** [RS] Includes capabilities enumerated in Level 1 plus: 4. Must isolate compromised sources without causing additional errors to the system PVT Solution. [P, RS] 5. Must support automatic recovery of individual PNT Sources, without disrupting system PVT output. [RS, RC]
Level 3	**Continues providing a solution (with bounded degradation) during threat.** [RS] Includes capabilities enumerated in Levels 1 and 2 plus: 6. Must ensure that corrupted data from one source cannot corrupt data from another source. [P] 7. Must cross-validate between PVT Solutions from all sources. [P] 8. Must isolate compromised PNT Sources from the system PVT Solution. [RS, RC]
Level 4	**Continues providing a solution without degradation during threat.** [P, RS] Includes capabilities enumerated in Levels 1, 2 and 3 plus: 9. Must have PNT Source diversity. [P, RS, RC]
Notes	P = Prevent; RS = Respond; RC = Recover ***Level 0** indicates source or system that does not meet the criteria in Level 1, thus is considered a Non-resilient System or Source.

Resilience Concepts in Conformance Framework

Level	Minimum Requirements (Cumulative)
1	**Ensures recoverability after removal of the threat.** • Must verify that stored data from external inputs adheres to values and formats of established standards. • 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. • Must include the ability to securely reload or update firmware.
2	**Provides a solution (possibly with unbounded degradation) during threat. Includes capabilities enumerated above plus**: • Must identify compromised PNT sources and prevent them from contributing to erroneous PNT solutions. • Must support automatic recovery of individual PNT sources and system.
3	**Provides a solution (with bounded degradation) during threat. Includes capabilities enumerated above plus**: • Must ensure that corrupted data from one PNT source cannot corrupt data from another PNT source. • Must cross-verify between PNT solutions from all PNT sources.







Conformance Framework: Resilience Levels Summary

- **Foundation of resilience**
  - ***Protect an internal state***
  - Better resilience withstands a threat with minimal to no degradation to performance
  - If the system can't **withstand** a threat, it must have **recovery** capability

Decreasing degradation to the system PVT solution performance

Increasing number of sources and source type diversity

Level	Behavior
Level 1	Focuses on Recovery after the threat has passed, the last resort of resilience
Level 2	Responds to error detection by isolating compromised sources and correcting the system PVT Solution
Level 3	Always prevents sources from corrupting each other and protects the system PVT Solution
Level 4	Required source type diversity protects internal state from losing validated external input in the presence of one threat

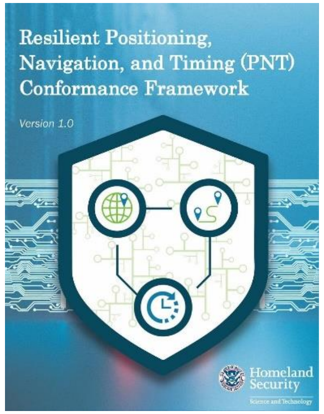
Requirements from each level build on each other

Architecture Interpretation of Conformance Framework PNT Resilience Levels

- **One interpretation of the PNT Resilience Levels from the Conformance Framework, as they relate to the architecture of the PNT UE system**

Level	Interpretation
Level 1	Focuses on recovery after the disruption is removed, setting the foundation for all resilience levels. Also includes basic verification steps to confirm external inputs adhere to established standards.
Level 2	Implies needing a local, physical PNT source for holdover. Responds to threat detection by temporarily isolating compromised PNT sources and initiating their automatic recovery.
Level 3	May need to implement additional hardware to permanently isolate PNT sources from each other. Implies three or more PNT sources to implement cross-verification.
Level 4	Required source type diversity prevents local source from losing validated external input when a single PNT source is disrupted.

Resilient PNT User Equipment Conformance Milestones



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

V2.0 published in May 2022 expands evaluation guidance

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

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/

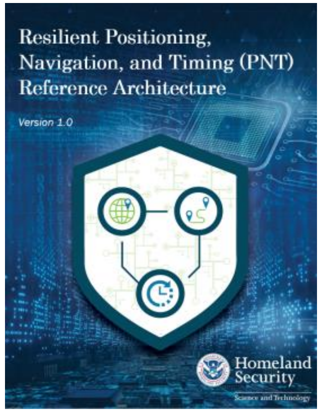
June 2022

DHS S&T publishes 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



April 2024

Kickoff meeting for

IEEE PNT Conformity Assessment Steering Committee (PNT-CASC) for the Conformity Assessment Program (ICAP)

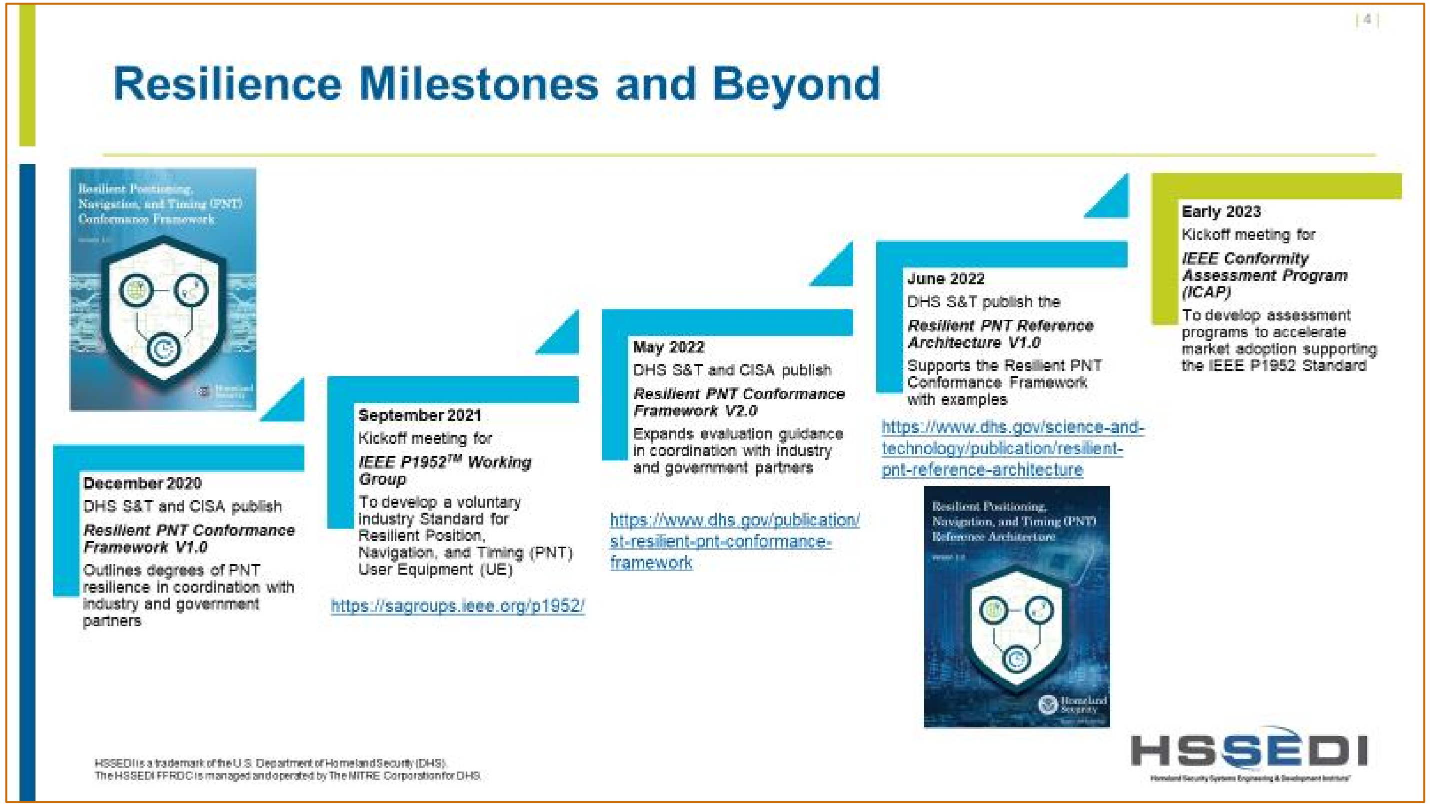
To develop assessment programs to accelerate market adoption supporting the IEEE P1952 Standard

https://standards.ieee.org/products-programs/icap/programs/pnt-user-equipment/

HSSEDI
Homeland Security Systems Engineering & Development Institute™

Context for Reference Implementation

- **Conformance Framework sets preliminary definitions and abstract concepts**
- **Reference Architecture shows logical groupings of resilience functions and connectivity**
- **IEEE Standard formalizes CF point of departure**
- **Reference Implementation provides experimental foundation for transition from definitions to practice (ICAP)**



IEEE P1952 Standard

- **The IEEE P1952 Working Group is developing an industry standard for resilient PNT User Equipment (UE).**
  - The multidisciplinary group has members representing diverse stakeholders, including PNT UE users, PNT UE manufacturers, test equipment manufacturers, test labs, and government agencies.
- **The P1952 Project Authorization Request (PAR) describes the scope and purpose of the standard (see: https://development.standards.ieee.org/myproject-web/public/view.html#pardetail/9060):**
  - *"Based on technical requirements, the standard defines different levels of resilience to enable users to select a level that is appropriate based on their risk tolerance, budget, and application criticality."*
  - *"The standard allows stakeholders to define and communicate resilient PNT UE needs and evaluate proposed resilience solutions in a consistent, uniform manner."*
- **Stakeholders representing Critical Infrastructure sectors, including Energy, Telecommunications, Financial services, and Transportation, are providing use cases for the standard development**
- **A draft of the full standard will begin the editing and balloting process soon**

Resilience Levels and Stakeholder Communication

- **P1952 will define Resilience in terms of a UE box's behavior under disruption**
- **Resilience is not described in terms of the usual performance metrics (1-m of accuracy, 1 ms/month of drift, etc.), so P1952 will not make such requirements**
- **Standard will allow statements like this:**

Use case and PNT technology section

For application {X}, subject to adversity {Y}, using technology {Z}, …

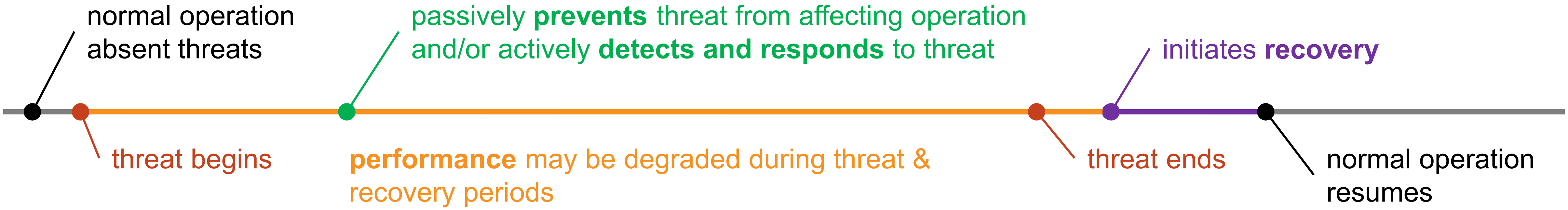
Performance bounds section

… the PNT user equipment's output interface will provide an accuracy of {X.X meters or seconds …} and an availability of {XX.X}% …

… at a resilience of Resilience Level C.

Resilience level C: e.g., verify inputs, manual reset, etc. (defining this content is subject of P1952)

Resilient PNT 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:** what kinds of threats can the UE detect?
  - **Response:** if the threat affects the UE, how does it respond?
  - **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

HSSEDI
Homeland Security Systems Engineering & Development Institute™