Resilient PNT Reference Architecture for Timing Applications

Dr. Patricia Larkoski

Department of Homeland Security (DHS)
Homeland Security Systems Engineering and Development Institute (HSSEDI)
Federally Funded Research and Development Center (FFRDC), operated by The MITRE Corporation

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 HSHQDC-14-D-00006.

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:

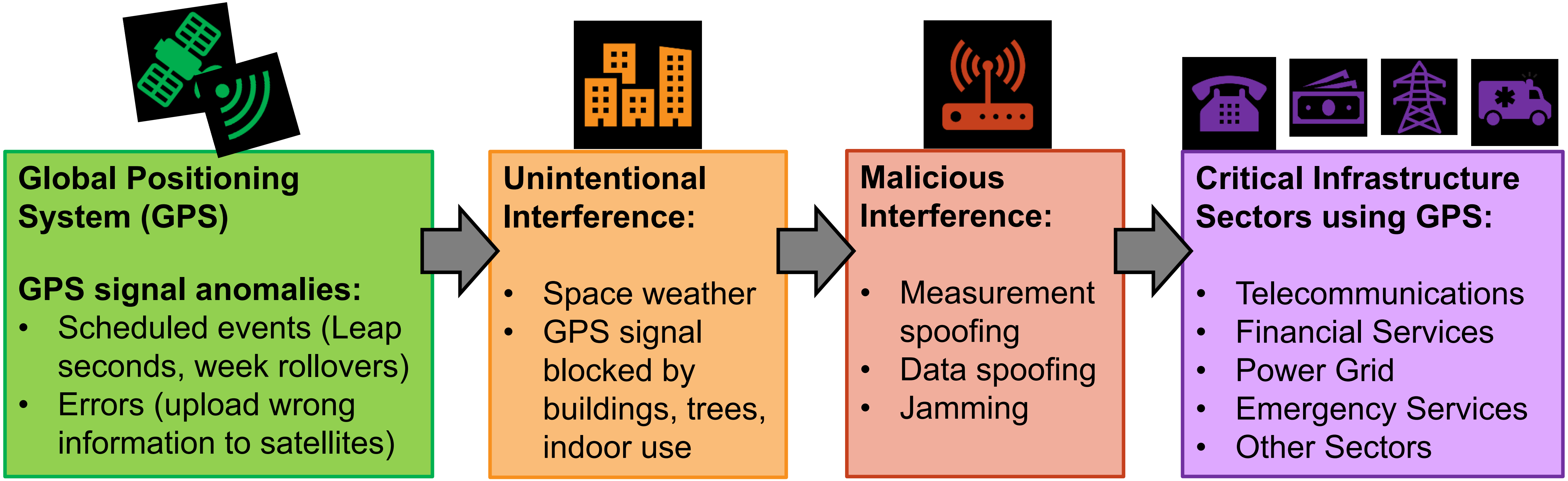
70RSAT20FR0000062
Science and Technology Directorate (S&T), Next Gen Resilient Position, Navigation, and Timing (PNT)
Develop and maintain the Nation's technical expertise, frameworks and artifacts necessary to guide PNT users, product integrators and supply chain manufacturers on government resiliency expectations related PNT system integrations and effectiveness of product solutions

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

Approved for Public Release; Distribution Unlimited.
Case Number 21-2597 / DHS reference number 70RSAT20FR-62-02

Critical Infrastructure Relies on GPS

- The Global Positioning System (GPS) is used by timing applications in many critical infrastructure sectors.
- GPS (and GNSS) receivers are attack surfaces and common points of failure for downstream applications.
- Non-resilient GPS receivers are essentially radios with open ports, unequipped to respond to interference.*



Global Positioning System (GPS)

GPS signal anomalies:
- Scheduled events (Leap seconds, week rollovers)
- Errors (upload wrong information to satellites)

Unintentional Interference:
- Space weather
- GPS signal blocked by buildings, trees, indoor use

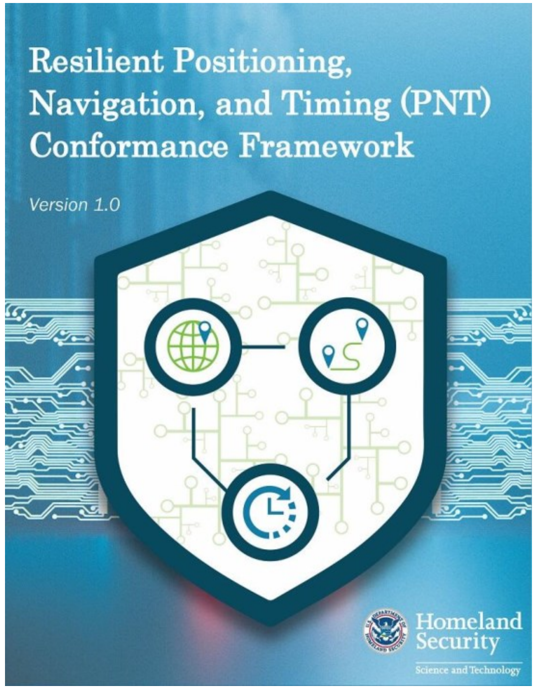
Malicious Interference:
- Measurement spoofing
- Data spoofing
- Jamming

Critical Infrastructure Sectors using GPS:
- Telecommunications
- Financial Services
- Power Grid
- Emergency Services
- Other Sectors

*See https://us-cert.cisa.gov/sites/default/files/documents/Technical-Level_Resilient_Timing_Overview-CISA_Fact_Sheet_508C.pdf

Background – Resilient PNT Conformance Framework

- **“The term "resilience" means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions.”**
  - From: Presidential Policy Directive – Critical Infrastructure Security and Resilience/PPD-21
  - There are other definitions of resilience used within the community
- **Resilient PNT Conformance Framework**
  - Published December 2020: https://www.dhs.gov/publication/st-resilient-pnt-conformance-framework
  - DHS S&T and CISA product developed in coordination with industry and government partners, which defines 4 levels of PNT resilience
- **Transitioning to IEEE P1952™ - Standard for Resilient Positioning, Navigation and Timing (PNT) User Equipment**
  - Working group kickoff held 15 September 2021 (website: https://sagroups.ieee.org/p1952/)



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

Version 1.0

Homeland Security

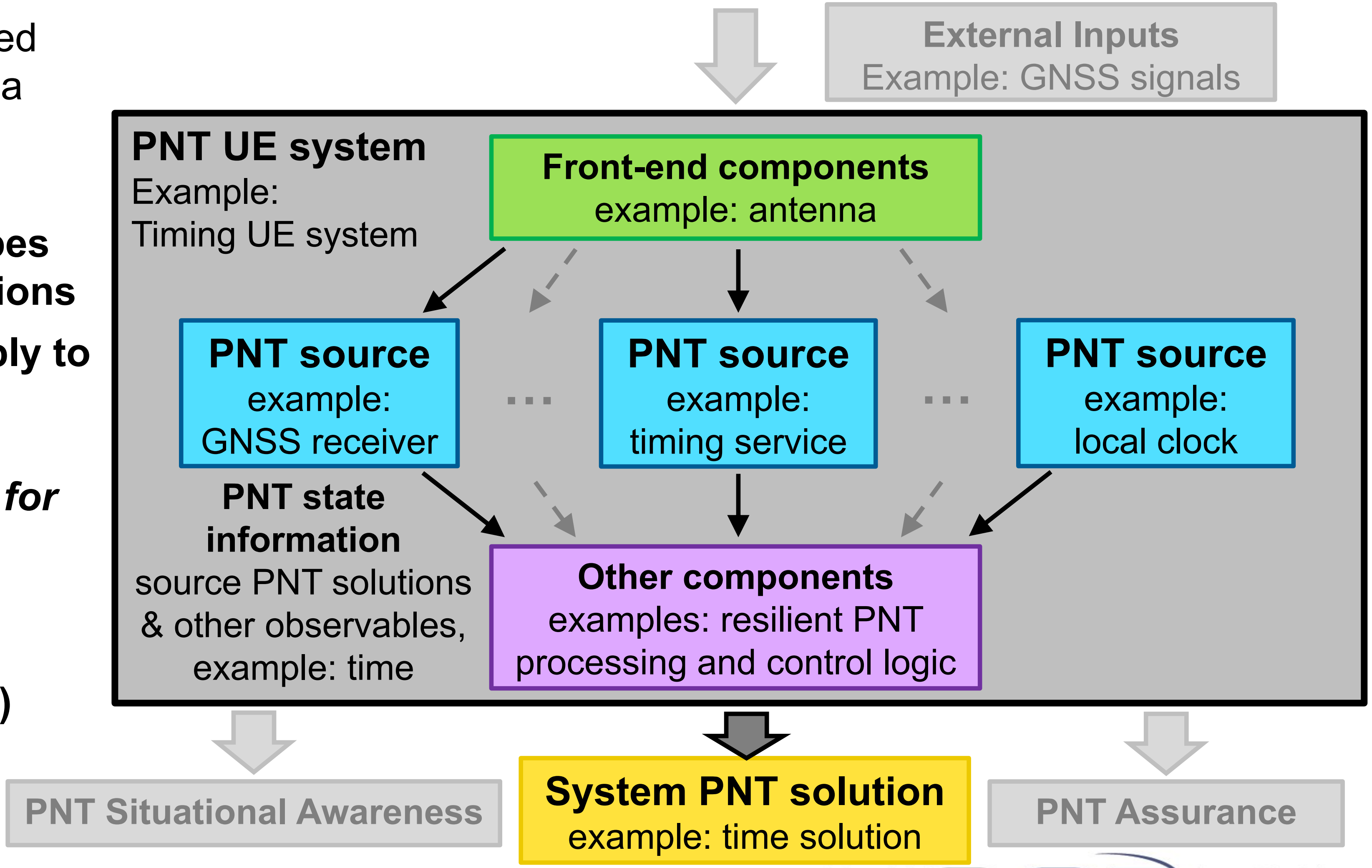
Science and Technology

Reference Architecture Document

- **The *Resilient PNT Reference Architecture* (RA) document supports the *Resilient PNT Conformance Framework* with specific architecture examples**
  - Describes architecture examples that show how specific techniques are combined to create PNT user equipment (UE) system resilience
  - The example architectures are meant to clarify high level descriptions from the Conformance Framework. They are not meant to be prescriptive, canonical standards that restrict innovation.
  - Provides conceptual framework to organize examples of different resilient techniques that have been developed and documented elsewhere
  - Intended for a public audience, to develop civilian user equipment
  - Projected publication in December 2021
- **There are many other resources for PNT resilience, assurance, and situational awareness. There is a rich history and active innovation in this area.**

Resilient PNT Reference Architecture Definitions

- **Reference Architecture:** a structured document describing how to design a system to meet defined principles
- **Terms defined to describe User Equipment (UE), including the types of components and their connections**
- **The RA document is meant to apply to any UE that provides Position, Navigation, and/or Time services.** ***This brief will focus on resilience for timing UE only.***
- **Assurance (assessing trust) and situational awareness (detection, characterization, and geolocation) intersect with resilience, but are not discussed directly here**



External Inputs
Example: GNSS signals

PNT UE system
Example:
Timing UE system

Front-end components
example: antenna

PNT source
example:
GNSS receiver

…

PNT source
example:
timing service

…

PNT source
example:
local clock

PNT state information
source PNT solutions & other observables,
example: time

Other components
examples: resilient PNT processing and control logic

PNT Situational Awareness

System PNT solution
example: time solution

PNT Assurance

Holistic Approach to Resilience with Technique Categories

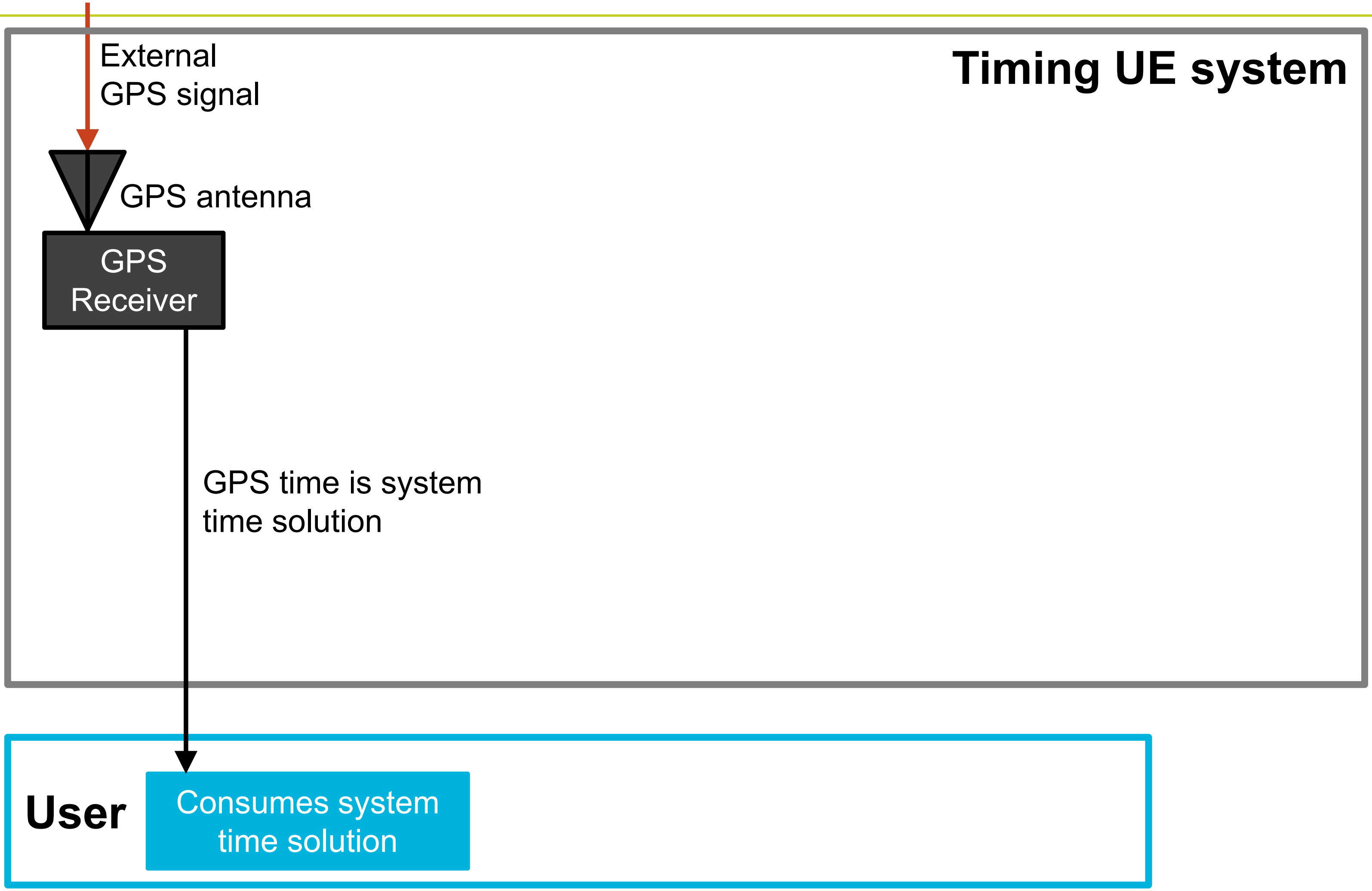
Holistic approach to PNT Resilience
Build robust systems: assume PNT systems will be attacked
Minimize attack surfaces: reduce exposure to external input
Skeptical outlook: do not assume trust
Threat agnostic: design for resilience to any anomaly rather than reacting to emergent threats
Defense in depth: PNT UE systems have layers – so does resilience

Resilience Technique Categories	
Recovery is the foundation of resilience: the system must be able to recover typical performance when the threat is removed	⊕
Limit external influence: minimize dependence on external input	↗↙
Verify external input: manage trust and use complementary anomaly detection methods	✓
Isolate to protect: maintain trusted internal states that are protected from external influence	🏝
Diversify to increase robustness: use multiple different PNT source types to avoid common mode failures	★ ▲ ● ■

- **There are other resilience techniques and categories not included in this brief**
- **Implementing some or all the techniques given here does not guarantee a PNT UE system is resilient**
- **Only the demonstrated ability to withstand and recover from disruptions makes a system resilient**

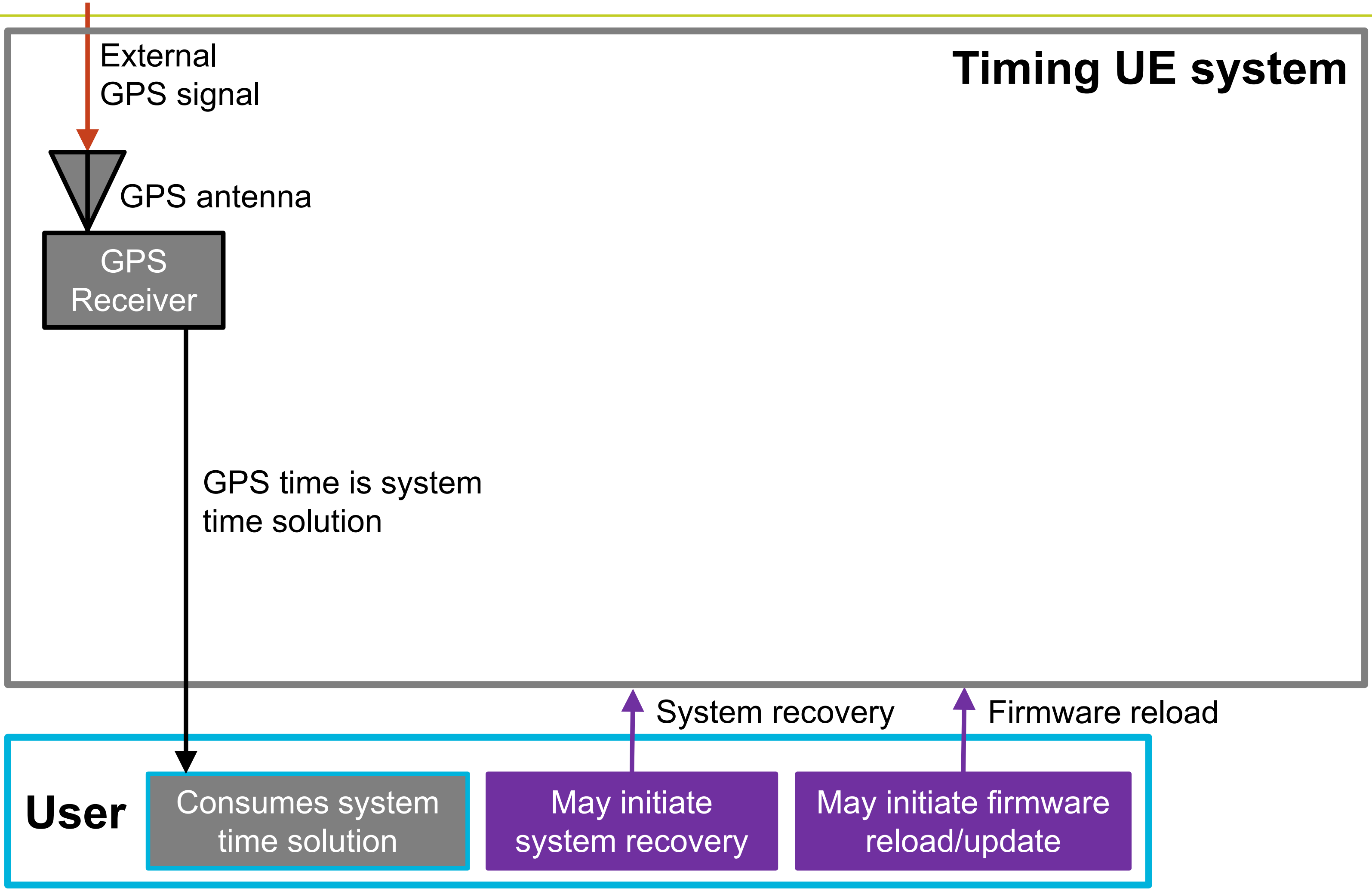
Timing Example – Start with a Non-Resilient GPS Receiver

- **A GPS receiver uses the external GPS signal to generate the system time solution for the user**
- **A non-resilient GPS receiver is essentially an open port, like a radio**
- **Start with a non-resilient source of time to show how resilience techniques can be added from different categories (recover, limit, verify, isolate, and diversify) to build up to resilient timing user equipment (UE)**



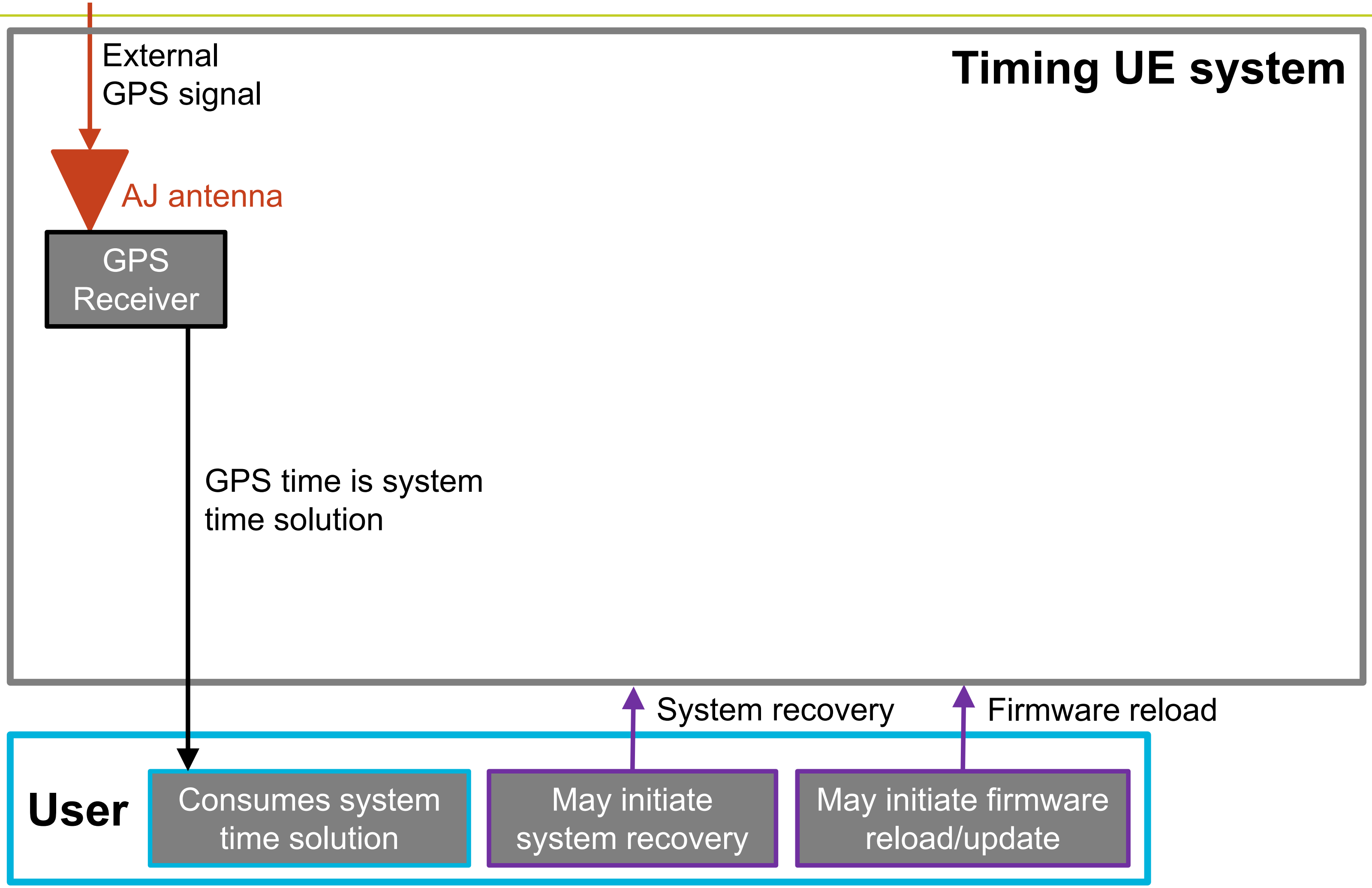
Recovery – the Foundation of Resilience

- **System recovery is the foundation of resilience – if the UE does not withstand the disruption, it must at least recover after**
- **All resilient timing UE systems must have a manual system recovery capability**
- **Return to defined performance after threat is removed**
- **Reset or rollback data stored to memory**
- **Firmware reload or update**


External GPS signal
Timing UE system
GPS antenna
GPS Receiver
GPS time is system time solution
System recovery
Firmware reload
User
Consumes system time solution
May initiate system recovery
May initiate firmware reload/update

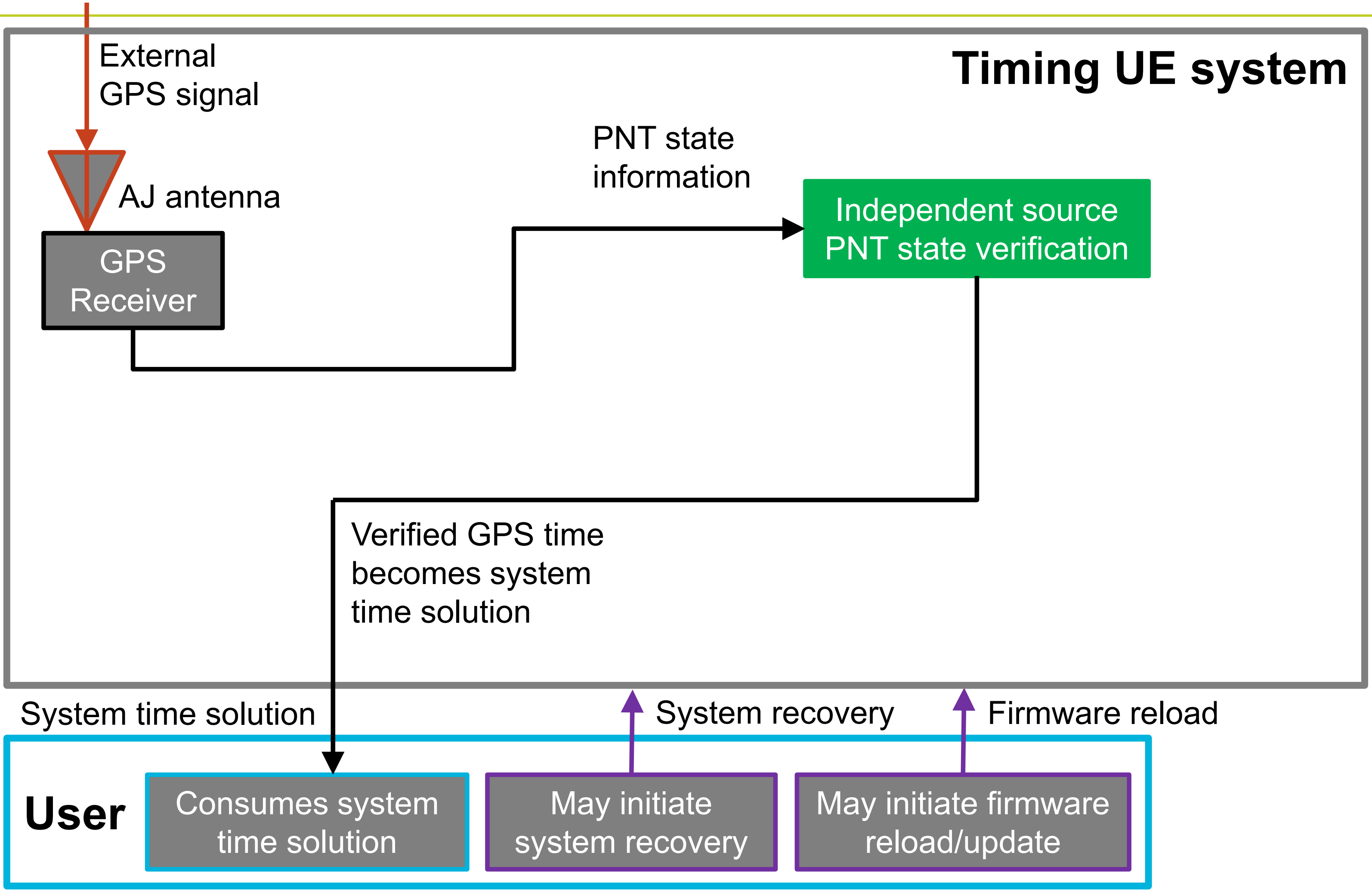
Limit External Input with an Anti-Jam Antenna

- **Anti-jam antenna limits the external input to the timing UE system**
  - Directional nulling
  - Frequency filters


External GPS signal
Timing UE system
AJ antenna
GPS Receiver
GPS time is system time solution
System recovery
Firmware reload
User
Consumes system time solution
May initiate system recovery
May initiate firmware reload/update

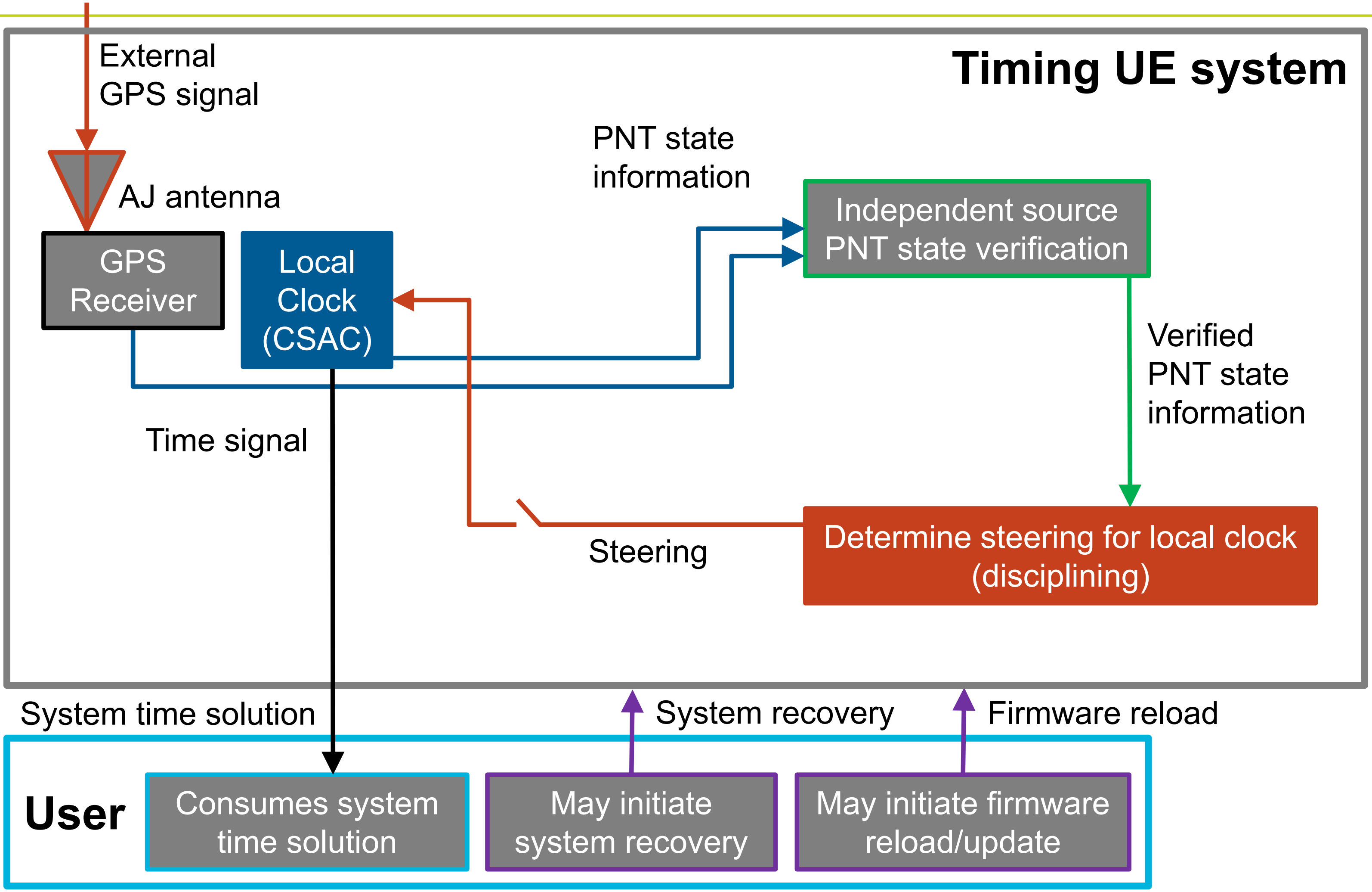
✓ Verify PNT State Information

- **Verify the PNT state information from the GPS receiver using techniques to detect different types of anomalies**
  - Examples: Anti-jam and anti-spoof techniques
- **Potential PNT state information observables from the GPS receiver:**
  - Source PNT solution, including position, velocity, and time (PVT)
  - Data that is stored to memory, like the navigation message information
  - Power measurements
  - Other internal observables


Timing UE system
External GPS signal
AJ antenna
GPS Receiver
PNT state information
Independent source PNT state verification
Verified GPS time becomes system time solution
System time solution
System recovery
Firmware reload
User
Consumes system time solution
May initiate system recovery
May initiate firmware reload/update

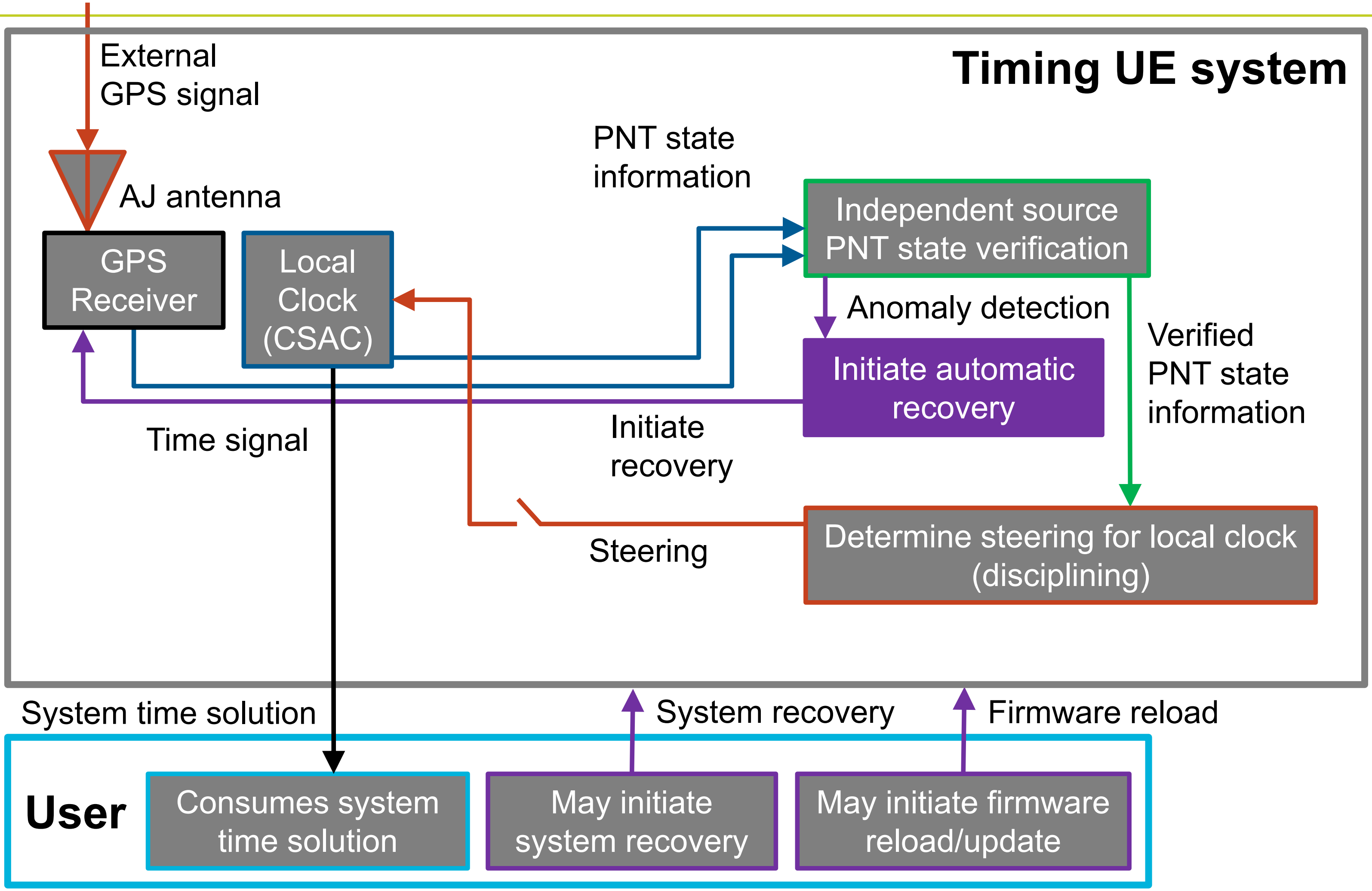
Limit When External Input is Used with an Isolated Local Clock

- **Add a local clock – an internal PNT source that does not receive external input directly**
  - A GPS-disciplined clock combines the short-term stability of the clock with long-term stability from GPS
- **Maintain isolation by independently verifying GPS PNT state information before using it for steering**
- **Flip method: default to free-running clock, only steer minimally to maintain necessary accuracy**
- **Benefit: minimize the attack surface from external input by limiting when GPS is used**


Timing UE system
External GPS signal
AJ antenna
GPS Receiver
Local Clock (CSAC)
PNT state information
Independent source PNT state verification
Verified PNT state information
Time signal
Steering
Determine steering for local clock (disciplining)
System time solution
System recovery
Firmware reload
User
Consumes system time solution
May initiate system recovery
May initiate firmware reload/update

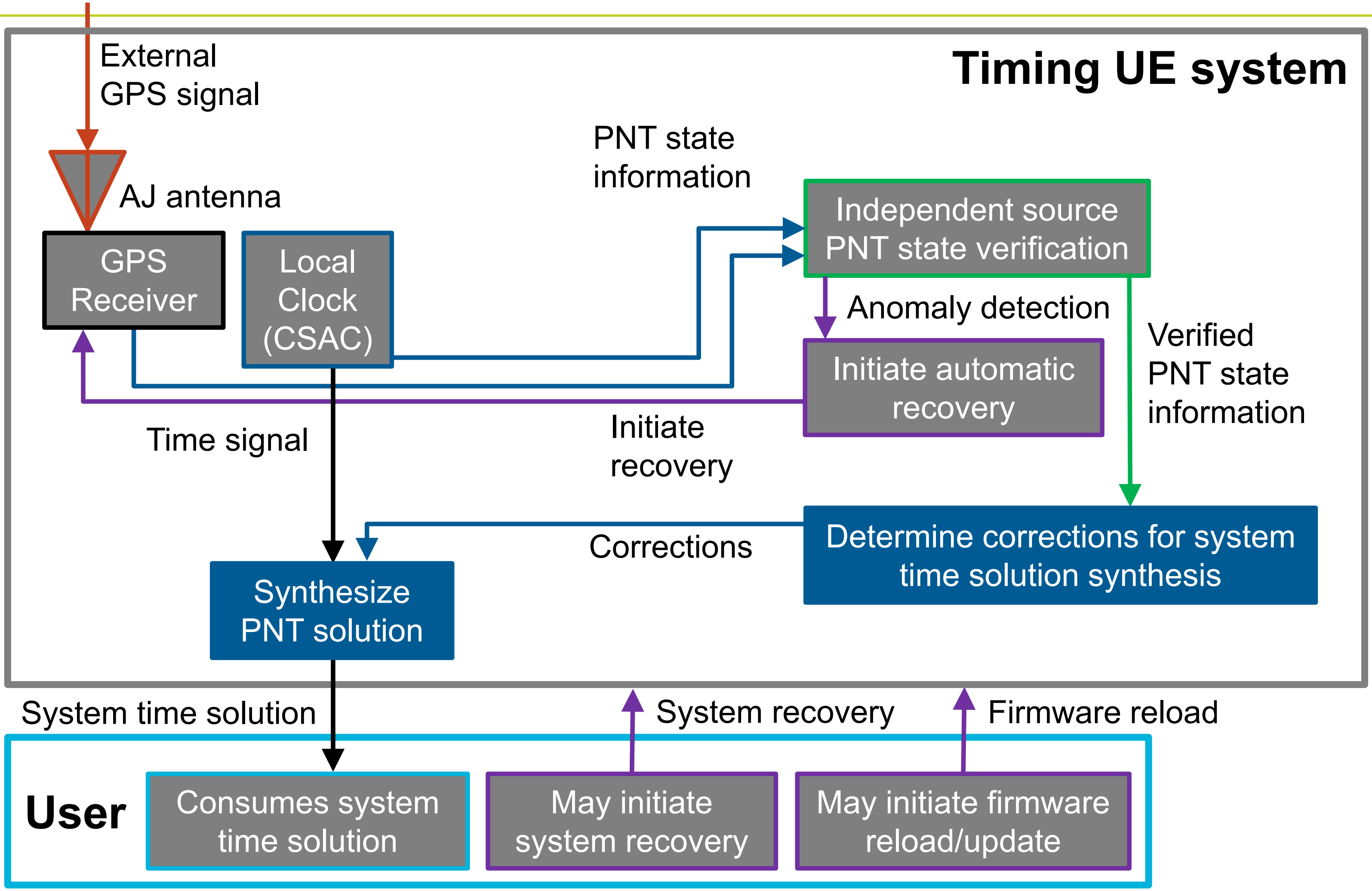
Automatic PNT Source Recovery

- **Automatic recovery** **ensures that compromised components are recovered as soon as possible (example: GPS receiver restart)**
- **While the GPS is being recovered, use only the local clock for the system time solution (holdover)**


Timing UE system
External GPS signal
AJ antenna
GPS Receiver
Local Clock (CSAC)
PNT state information
Independent source PNT state verification
Anomaly detection
Initiate automatic recovery
Verified PNT state information
Time signal
Initiate recovery
Steering
Determine steering for local clock (disciplining)
System time solution
System recovery
Firmware reload
User
Consumes system time solution
May initiate system recovery
May initiate firmware reload/update

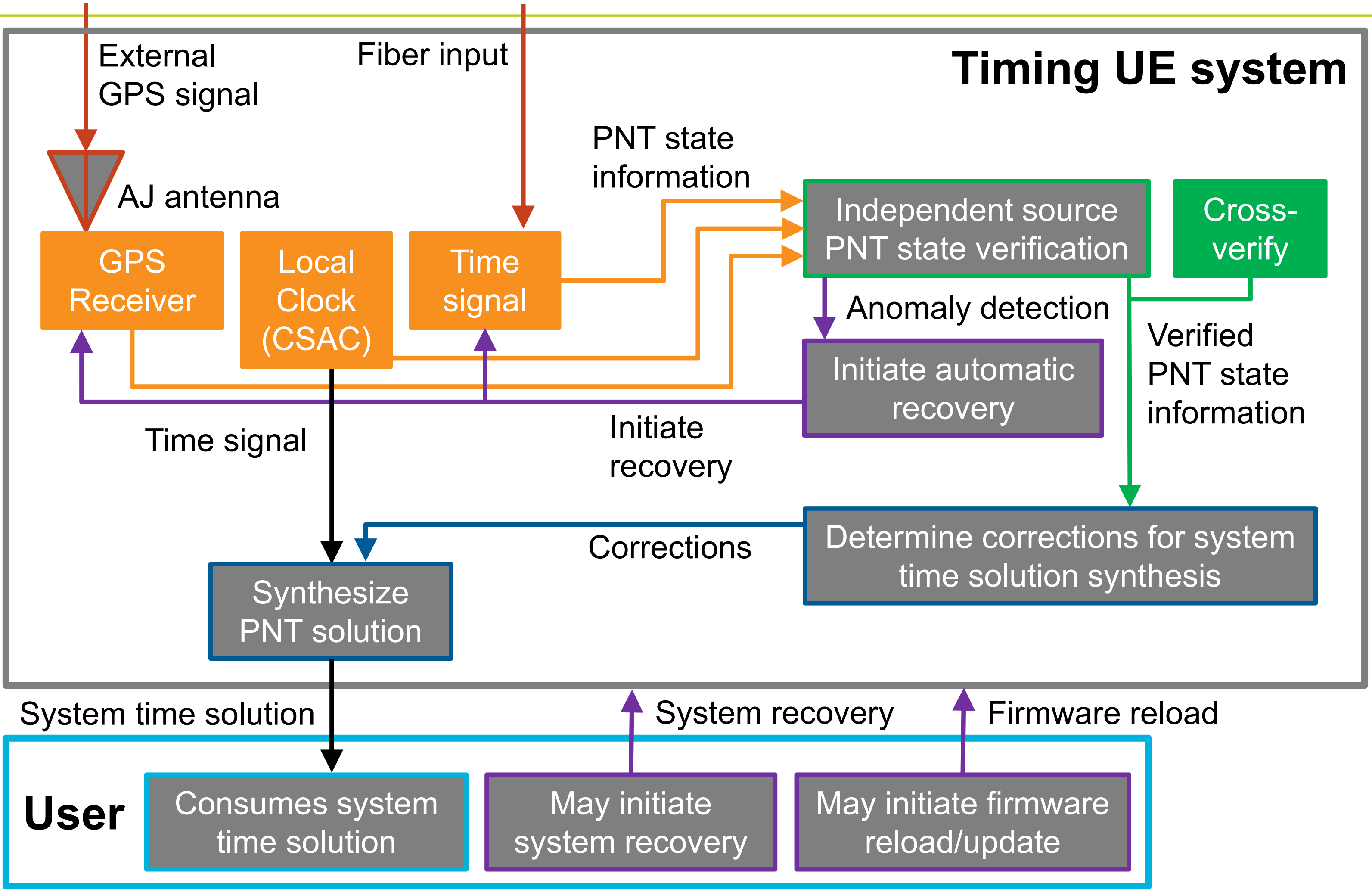
Isolate Local Clock from Direct External Input

- **Synthesize the system time solution using additional hardware with input from the local clock and corrections calculated from the verified GPS time**
- **Benefit: isolates the local clock to make a protected internal state (rather than steering directly)**
- **Benefit: synthesized System time solution can adapt quickly to changes when anomalies are detected**


Timing UE system
External GPS signal
AJ antenna
GPS Receiver
Local Clock (CSAC)
PNT state information
Independent source PNT state verification
Anomaly detection
Initiate automatic recovery
Verified PNT state information
Time signal
Initiate recovery
Corrections
Determine corrections for system time solution synthesis
Synthesize PNT solution
System time solution
System recovery
Firmware reload
User
Consumes system time solution
May initiate system recovery
May initiate firmware reload/update

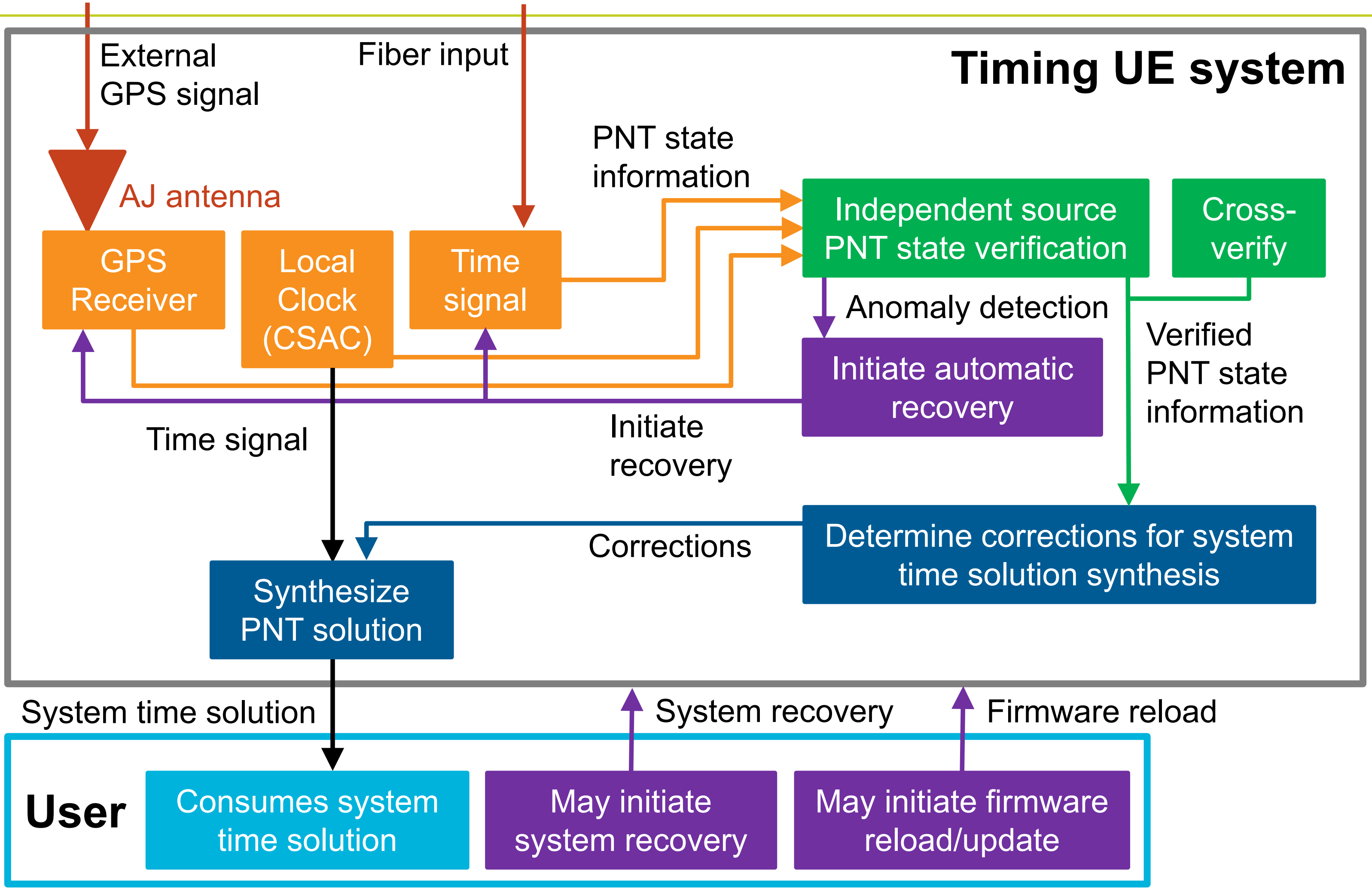
Diversify Technology Types and Cross Verify ✓

- **Diverse timing technology types minimize common mode failures**
- **The diverse timing technologies are isolated from each other. PNT state information is not combined until it is verified for each PNT source independently**
- **Cross-verification is possible when there are multiple source options**



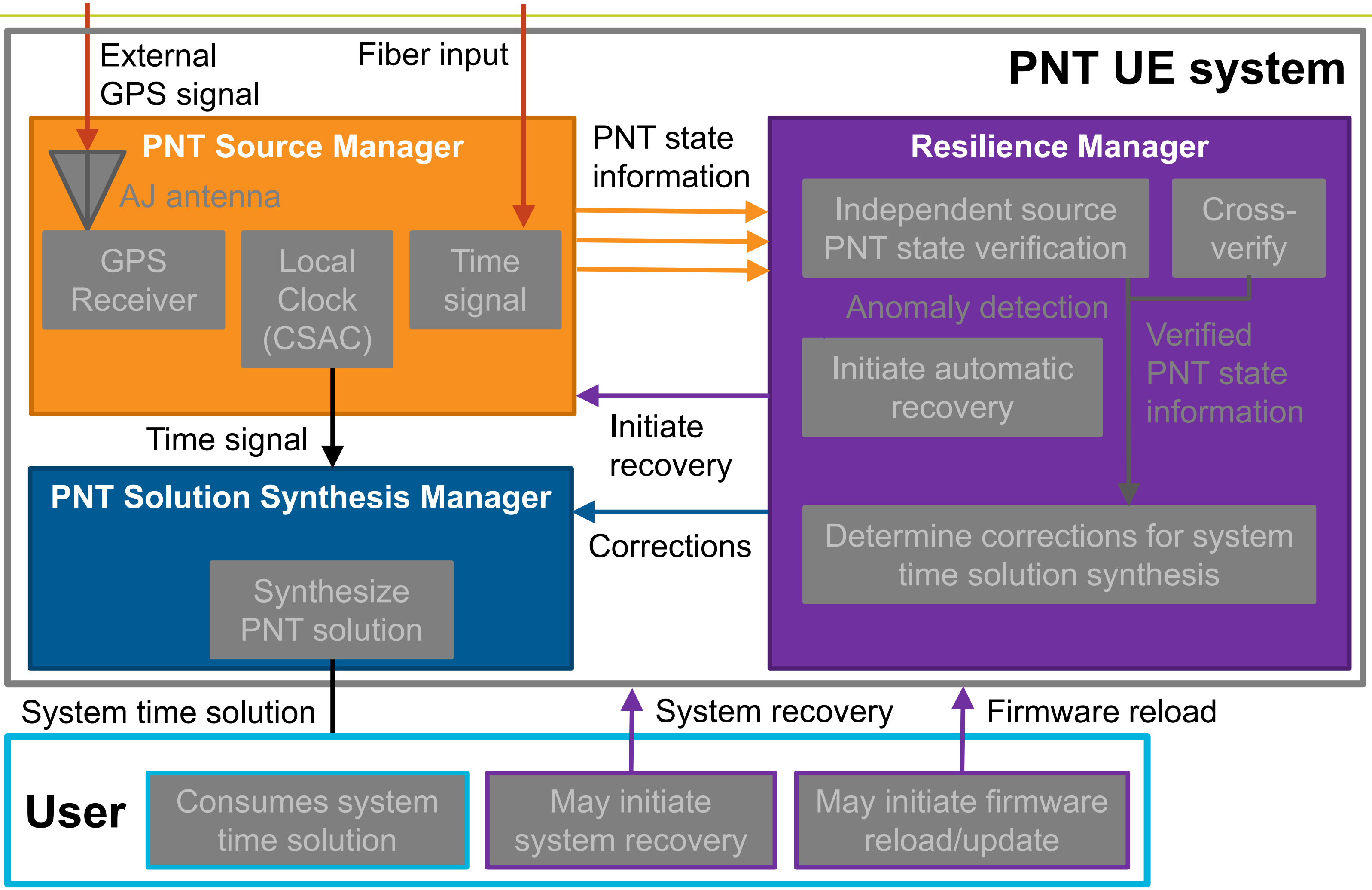
High Level Resilient Timing User Equipment System

- **Limits external input**
- **Diverse technology types**
- **Verifies PNT state information**
- **Automatic recovery of compromised components**
- **Protects internal state by isolating local clock**
- **Manual system recovery**



PNT User Equipment System Managers

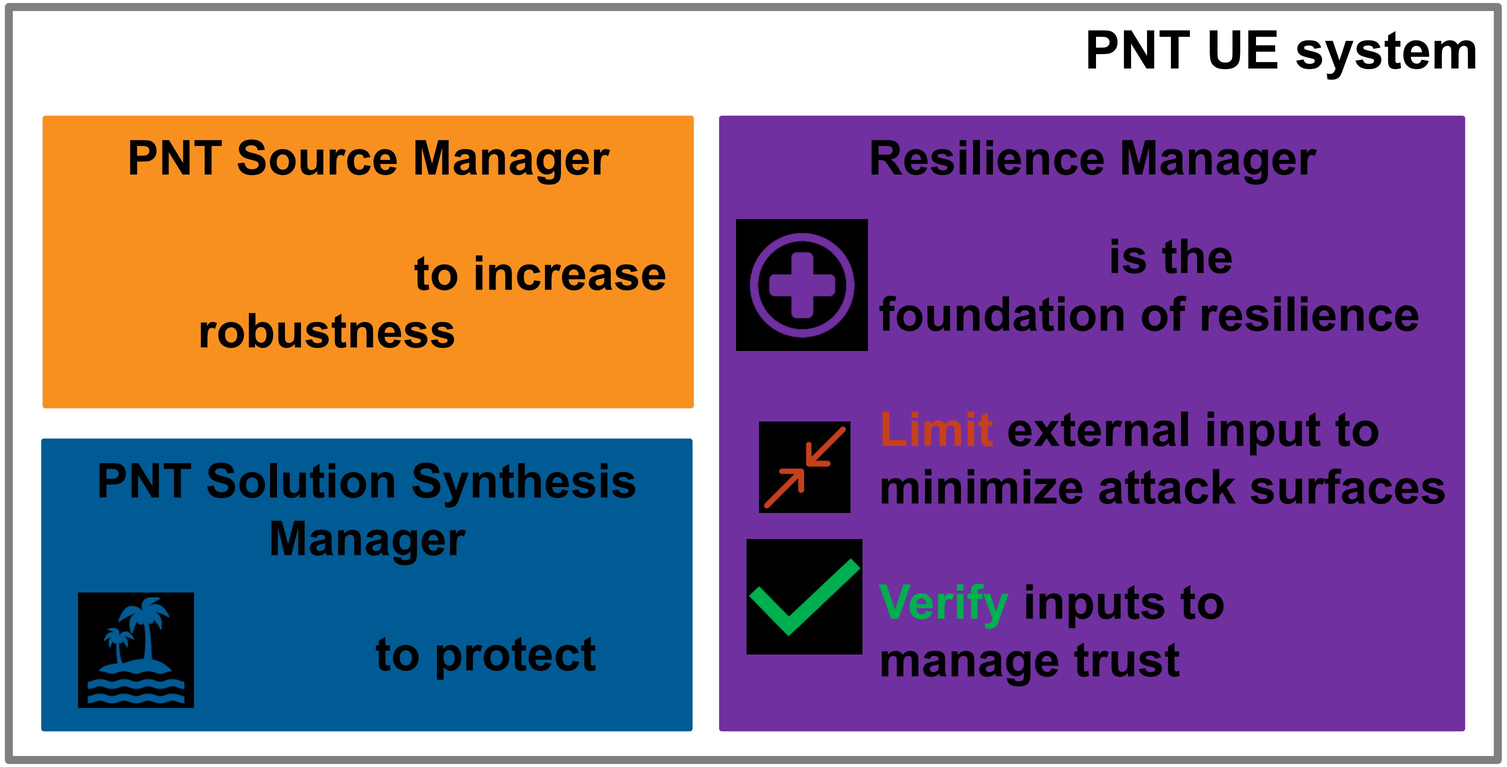
- **Dividing the timing UE system into sub-systems highlights essential PNT UE system architecture functions**
- **PNT Source Manager:** coordinates multiple different types of PNT sources
- **Resilience Manager:** verification steps, automatic recovery decisions, correction or steering calculations, and synthesis decisions
- **PNT Solution Synthesis Manager:** synthesizes system PNT solution using inputs



HSSEDI
Homeland Security Systems Engineering & Development Institute

Summary

- **Resilient PNT Reference Architecture provides a structured way to design PNT user equipment systems for resilience**
  - Supports the Resilient PNT Conformance Framework
  - Reference with examples and catalog of resilience techniques
- **Applying resilience concepts directly affects the design of resilient PNT architectures**
  - Timing UE system example with resilience built-up from 5 categories



PNT UE system

PNT Source Manager

to increase robustness

PNT Solution Synthesis Manager

to protect

Resilience Manager

is the foundation of resilience

Limit external input to minimize attack surfaces

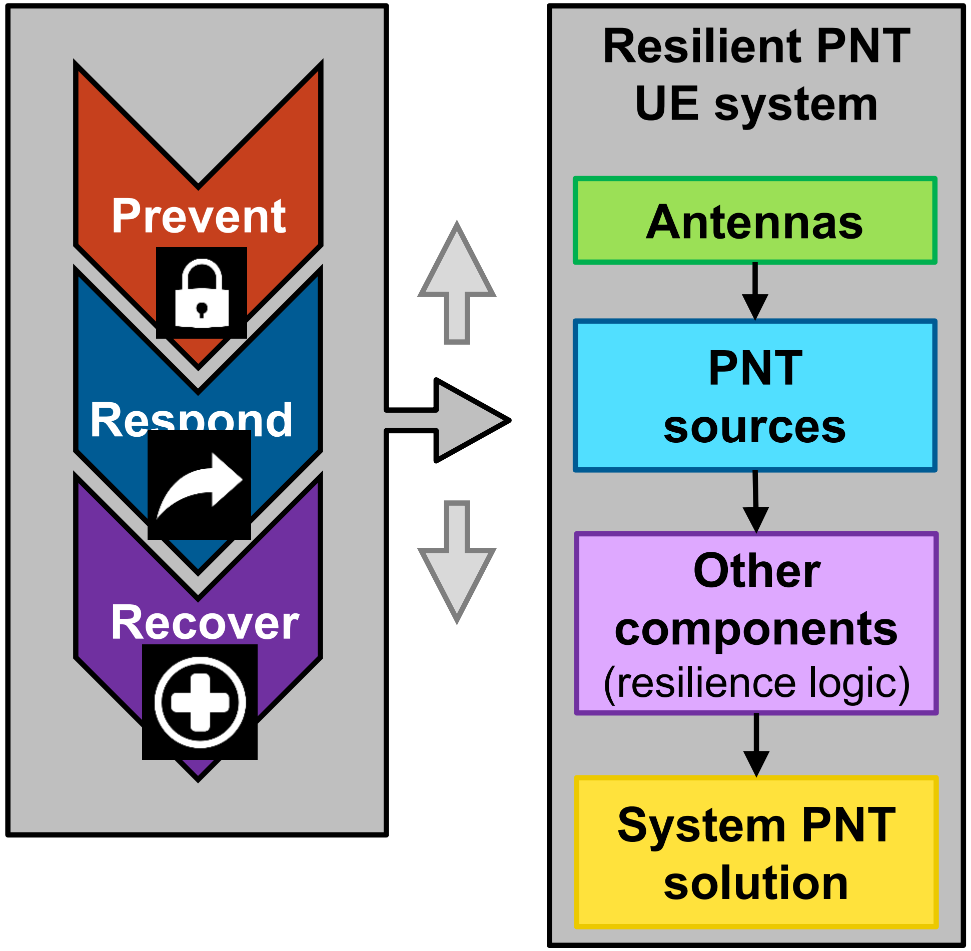
Verify inputs to manage trust

- **Regardless of design, outcomes prove resilience – withstanding and recovering from disruptions**
- **IEEE P1952™ working group Kickoff 15 September 2021 (website: https://sagroups.ieee.org/p1952/)**

Extra Slides

Core Functions of Resilience

- **The core functions provide a perspective for assessing resilience from any point in the system:**
- **Prevent:** The preferred function, if possible. How can the system be designed to prevent false information from propagating? How can errors and data corruption be prevented from reaching this point?
- **Respond:** Given that there is a threat condition, and it has corrupted some information or caused an error, how will the system respond to mitigate or correct the error?
- **Recover:** The minimum resilient behavior. If the PNT system is unable to fully withstand a disruption, how does it return to a good working state? How will the system recover if an error propagates beyond this point?



Architecture Interpretation of 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.

Level 1 Requirements from the Conformance Framework

- **Level 1 lays the groundwork for higher levels of resilience with requirements to ensure recovery**
- **Starting from the bare minimum makes sense because the levels are cumulative**

	Definition and Requirements
Level 1	**Ensures recoverability after removal of the 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.**

Level 2 Requirements from the Conformance Framework

- **Protect the system PNT solution by isolating compromised sources**
- **Recover individual PNT sources**
- **Can achieve with existing systems when used with available resilient functions**

	Definition and Requirements
Level 2	**Provides a solution (possibly with unbounded** degradation) during threat.** **Includes capabilities enumerated in Level 1 plus:** **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.**

Level 3 and 4 Requirements from the Conformance Framework

- Robust isolation of PNT sources
- Utilize diversity of PNT sources to cross-verify all PNT solutions
- Diversity of PNT source technology mitigates common mode threats

	Definition and Requirements
Level 3	Provides a solution (with bounded degradation) during threat. Includes capabilities enumerated in Levels 1 and 2 plus: 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 4	Provides a solution without degradation during threat. Includes capabilities enumerated in Levels 1, 2 and 3 plus: 8. Must have diversity of PNT source technology to mitigate common mode threats.