Resilient PNT System Concepts for Critical Infrastructure

Dr. Arthur K. Scholz, Principal Engineer

The research in this presentation was conducted under contract with the U.S Department of Homeland Security (DHS) Science and Technology Directorate (S&T), under task order 70RSAT19FR0000040. The opinions contained herein are those of the contractors and do not necessarily reflect those of DHS S&T.

FFRDC POWERED BY S&T™

MITRE Corporation

22 September 2020

HSSEDI POC:
Dr. Arthur Scholz
ascholz@mitre.org

Approved for public release. Distribution unlimited.
Case Number 19-03383-03 / DHS Reference Number 17-J-00100-05

HSSEDI
Homeland Security Systems Engineering & Development Institute™

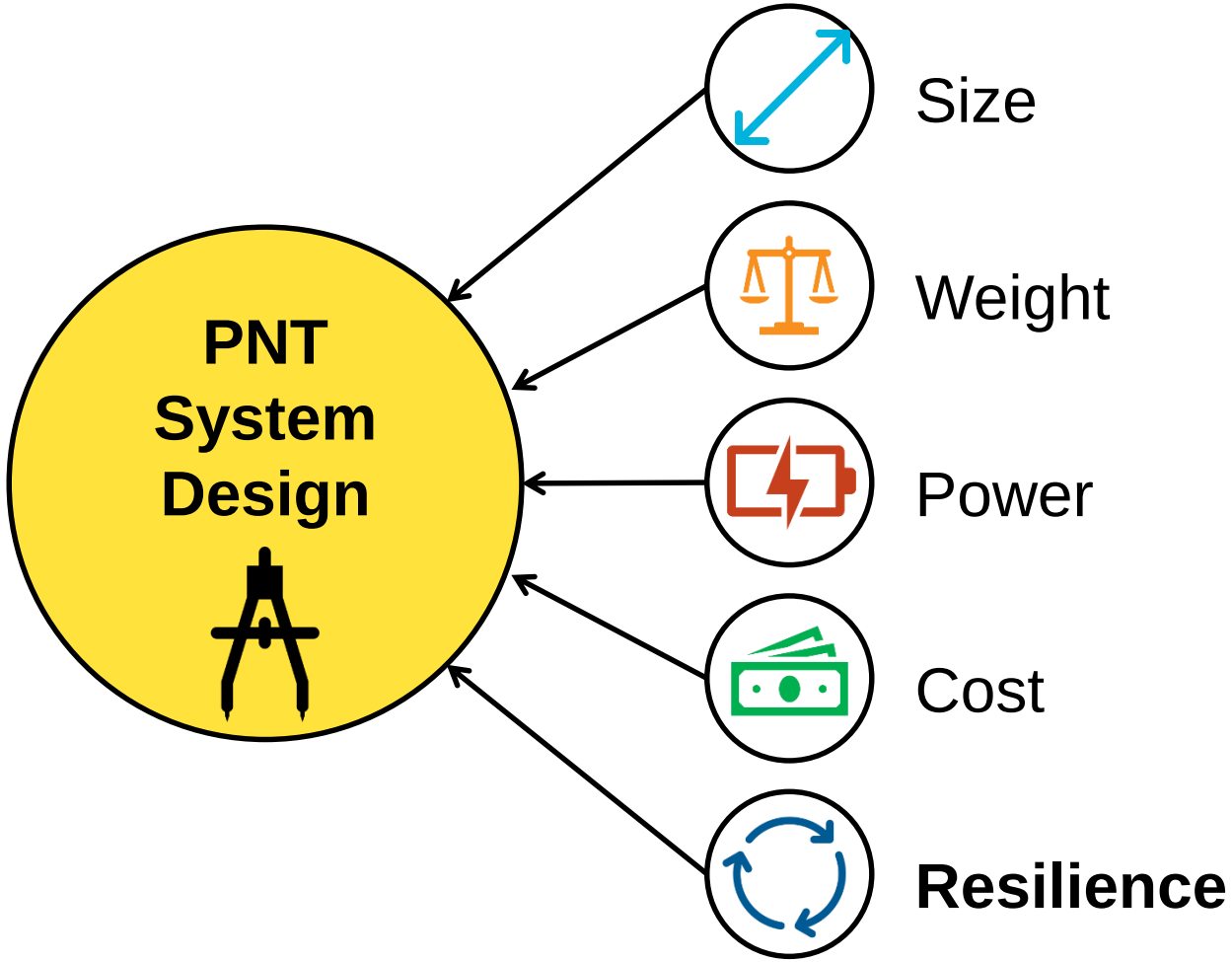
Resilient PNT – Audience: vendors and end users

- **Widespread use of PNT: from consumer products to highly interconnected national industries, such as utilities and the financial sector.**
- **PNT Systems are a target for adversaries seeking to inflict extensive and diverse damage in the civilian sector.**
- **Natural events and weather may also limit availability for PNT Sources requiring RF input, such as the Global Positioning System (GPS)**
- **Presidential Policy Directive (PPD)-21 definition of resilience:**
  - ***"The term "resilience" means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents." [1]***
- **Executive Order 13905 of Feb 12, 2020, *Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services***
  - ***" 'Responsible use of PNT services' means the deliberate, risk-informed use of PNT services, including their acquisition, integration, and deployment, such that disruption or manipulation of PNT services minimally affects national security, the economy, public health, and the critical functions of the Federal Government."***

Approved for public release. Distribution unlimited.
Case Number 19-03383-03 / DHS Reference Number 17-J-00100-05

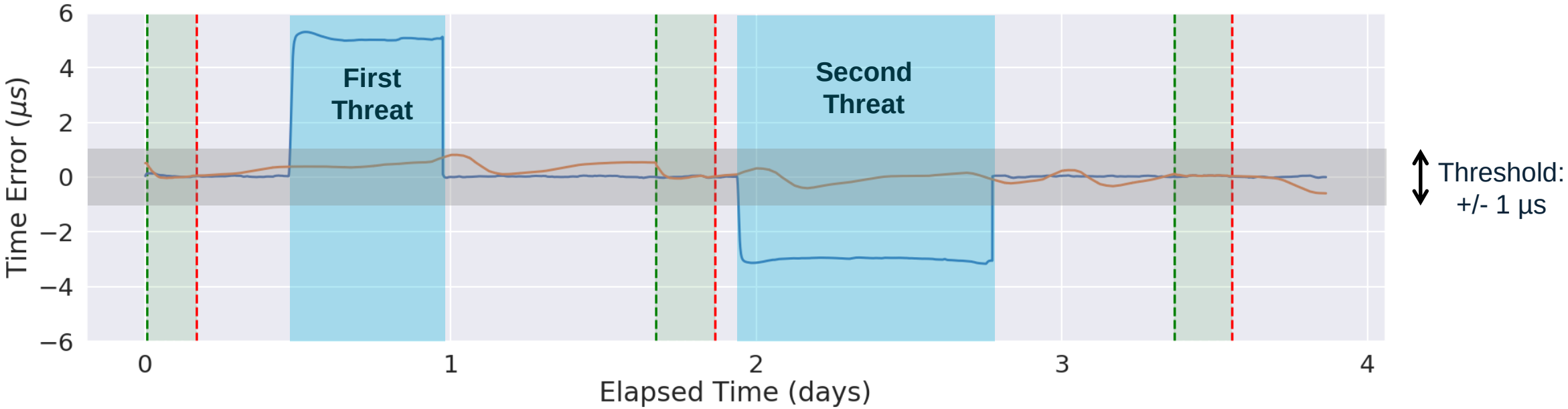
Trade-Space: Size, Weight, Power, Cost, and ***Resilience***

- **SWaP-CR:**
  Resilience is another dimension to the usual SWaP-C trade-space considerations.
- **A resilient PNT System will withstand and recover from disruptions. Without resilience, a system optimized only for SWaP-C may not perform when needed.**



Resiliency versus Accuracy

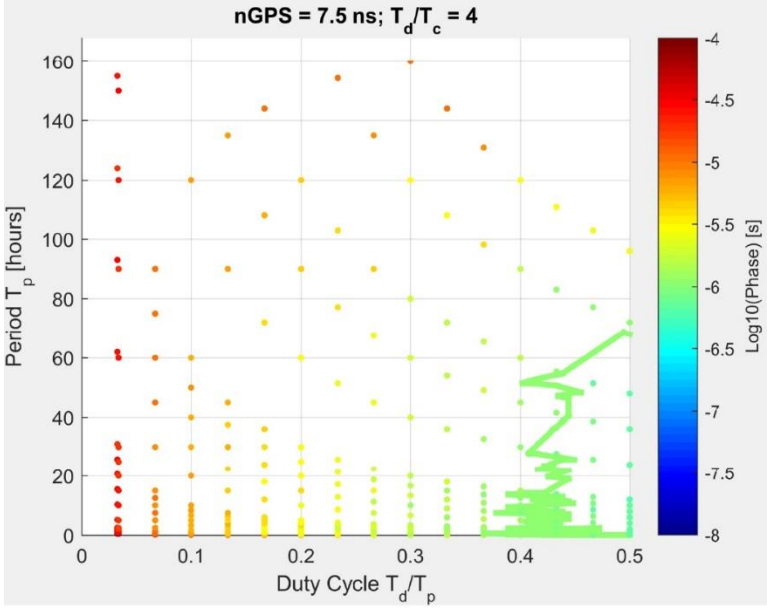
- **Optimize PNT Systems for resilient behavior rather than a typical metric, such as accuracy**
  - **Clock 1**: Not resilient to threats, better accuracy
  - **Clock 2**: Resilient to threats, accuracy is still within the application threshold

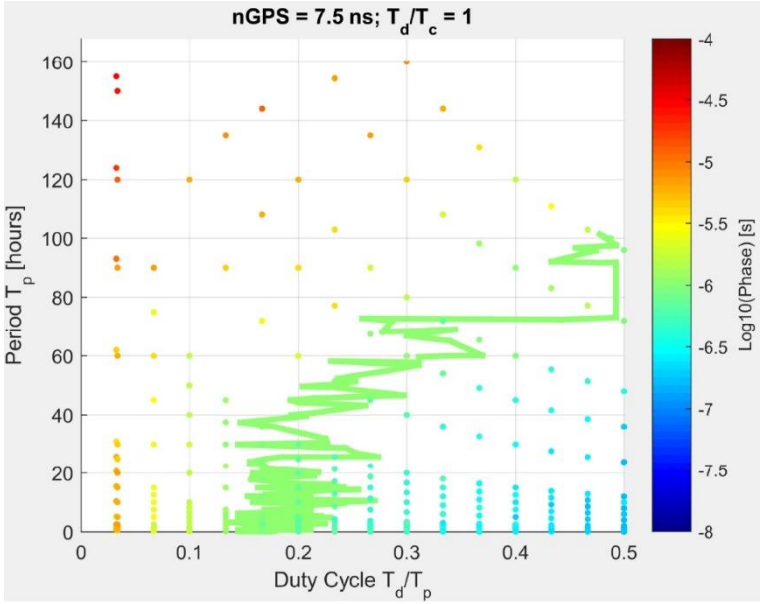


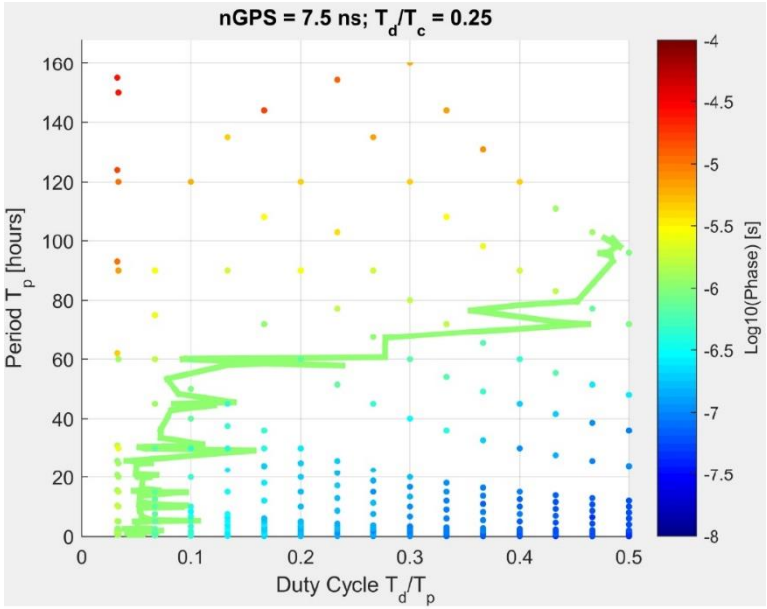
HSSEDI
Homeland Security Systems Engineering & Development Institute™

Resiliency versus Accuracy

- **Optimize PNT Systems for resilient behavior rather than a typical metric, such as accuracy**
- **Solution space: based on your application's needs, choose the appropriate trade-off between allowable error and resilience (and clock choice)**







Resources for Resilience

- **Reference Implementation and Reference Architecture documents by HSSEDI working with DHS**
- **Conformance Framework (CF) developed by Resilient PNT CF Working Group, bringing together manufacturers, integrators, government, and HSSEDI participation**

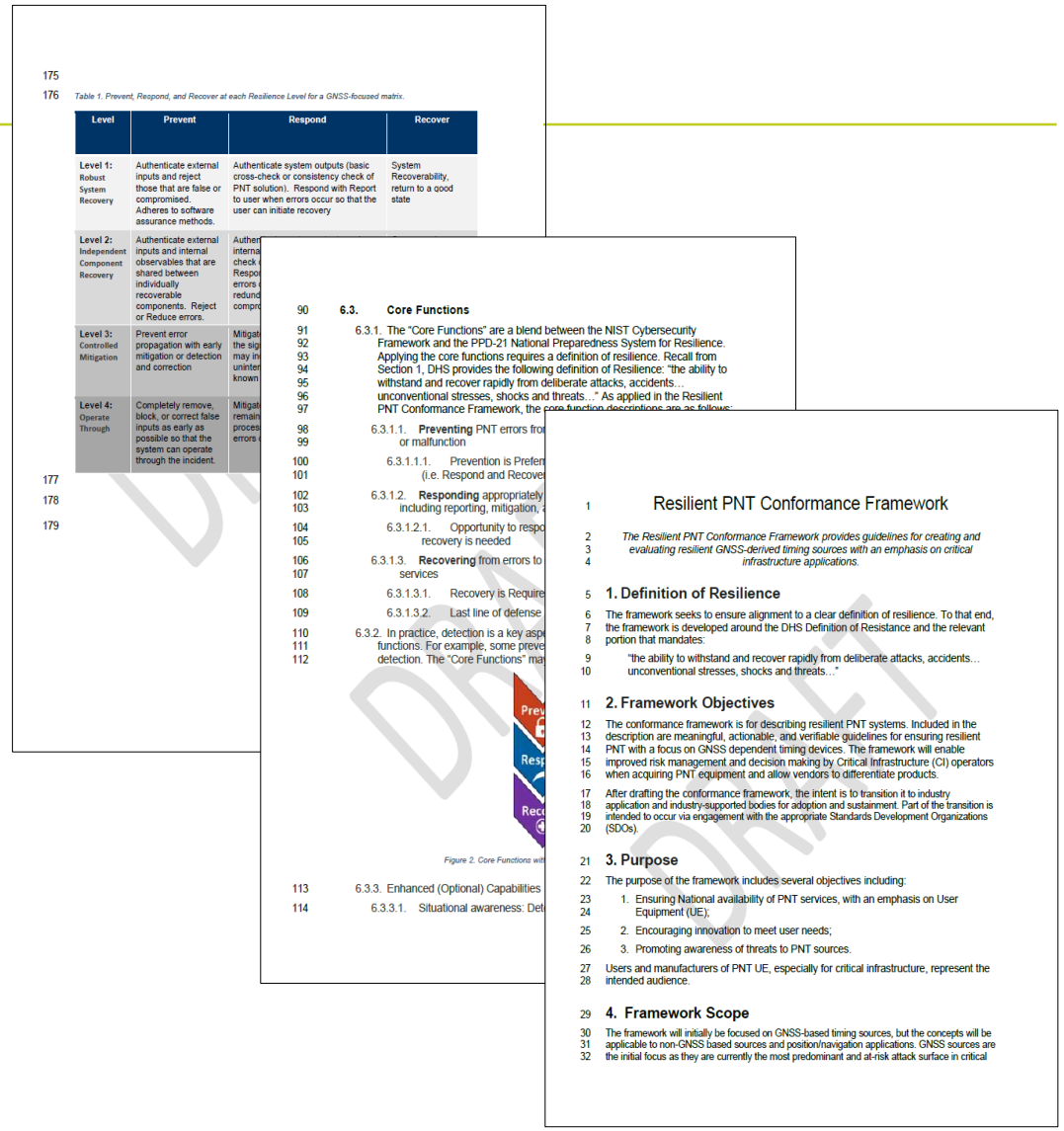


Table 1. Prevent, Respond, and Recover at each Resilience Level for a GNSS-focused matrix.

Level	Prevent	Respond	Recover
Level 1: Robust System Recovery	Authenticate external inputs and reject those that are false or compromised. Adheres to software assurance methods.	Authenticate system outputs (basic cross-check or consistency check of PNT solution). Respond with Report to user when errors occur so that the user can initiate recovery	System Recoverability, return to a good state
Level 2: Independent Component Recovery	Authenticate external inputs and internal observables that are shared between individually recoverable components. Reject or Reduce errors.		
Level 3: Controlled Mitigation	Prevent error propagation with early mitigation or detection and correction		
Level 4: Operate Through	Completely remove, block, or correct false inputs as early as possible so that the system can operate through the incident.		

6.3. Core Functions

6.3.1. The "Core Functions" are a blend between the NIST Cybersecurity Framework and the PPD-21 National Preparedness System for Resilience. Applying the core functions requires a definition of resilience. Recall from Section 1, DHS provides the following definition of Resilience: "the ability to withstand and recover rapidly from deliberate attacks, accidents… unconventional stresses, shocks and threats…" As applied in the Resilient PNT Conformance Framework, the

6.3.1.1. **Preventing** PNT errors fro or malfunction

6.3.1.1.1. Prevention is Prefer (i.e. Respond and Recove

6.3.1.2. **Responding** appropriately including reporting, mitigation,

6.3.1.2.1. Opportunity to respo recovery is needed

6.3.1.3. **Recovering** from errors to services

6.3.1.3.1. Recovery is Require

6.3.1.3.2. Last line of defense

6.3.2. In practice, detection is a key asp functions. For example, some preve detection. The "Core Functions" ma

Figure 2. Core Functions wit

6.3.3. Enhanced (Optional) Capabilities

6.3.3.1. Situational awareness: Det

Resilient PNT Conformance Framework

The Resilient PNT Conformance Framework provides guidelines for creating and evaluating resilient GNSS-derived timing sources with an emphasis on critical infrastructure applications.

1. Definition of Resilience

The framework seeks to ensure alignment to a clear definition of resilience. To that end, the framework is developed around the DHS Definition of Resistance and the relevant portion that mandates:

"the ability to withstand and recover rapidly from deliberate attacks, accidents… unconventional stresses, shocks and threats…"

2. Framework Objectives

The conformance framework is for describing resilient PNT systems. Included in the description are meaningful, actionable, and verifiable guidelines for ensuring resilient PNT with a focus on GNSS dependent timing devices. The framework will enable improved risk management and decision making by Critical Infrastructure (CI) operators when acquiring PNT equipment and allow vendors to differentiate products.

After drafting the conformance framework, the intent is to transition it to industry application and industry-supported bodies for adoption and sustainment. Part of the transition is intended to occur via engagement with the appropriate Standards Development Organizations (SDOs).

3. Purpose

The purpose of the framework includes several objectives including:

1. Ensuring National availability of PNT services, with an emphasis on User Equipment (UE);
2. Encouraging innovation to meet user needs;
3. Promoting awareness of threats to PNT sources.

Users and manufacturers of PNT UE, especially for critical infrastructure, represent the intended audience.

4. Framework Scope

The framework will initially be focused on GNSS-based timing sources, but the concepts will be applicable to non-GNSS based sources and position/navigation applications. GNSS sources are the initial focus as they are currently the most predominant and at-risk attack surface in critical

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

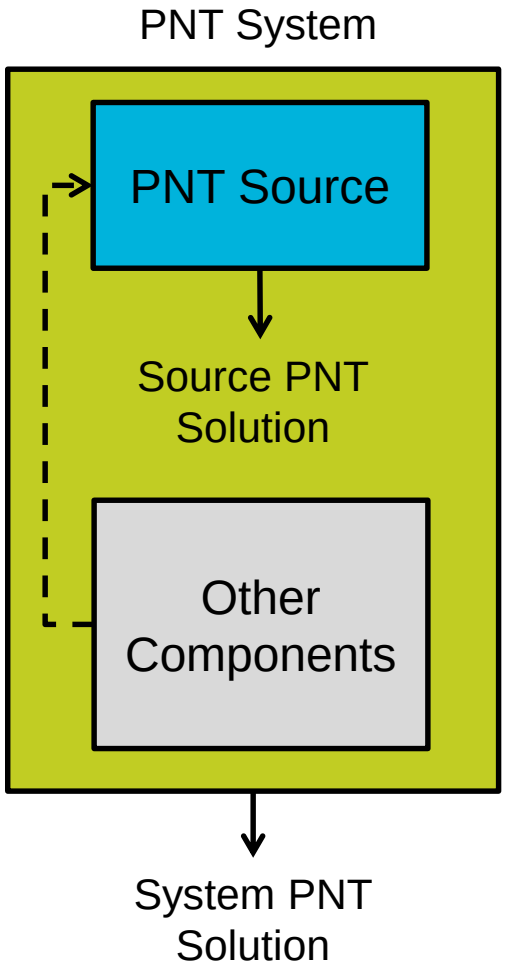
Decreasing degradation to the system PVT solution performance

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

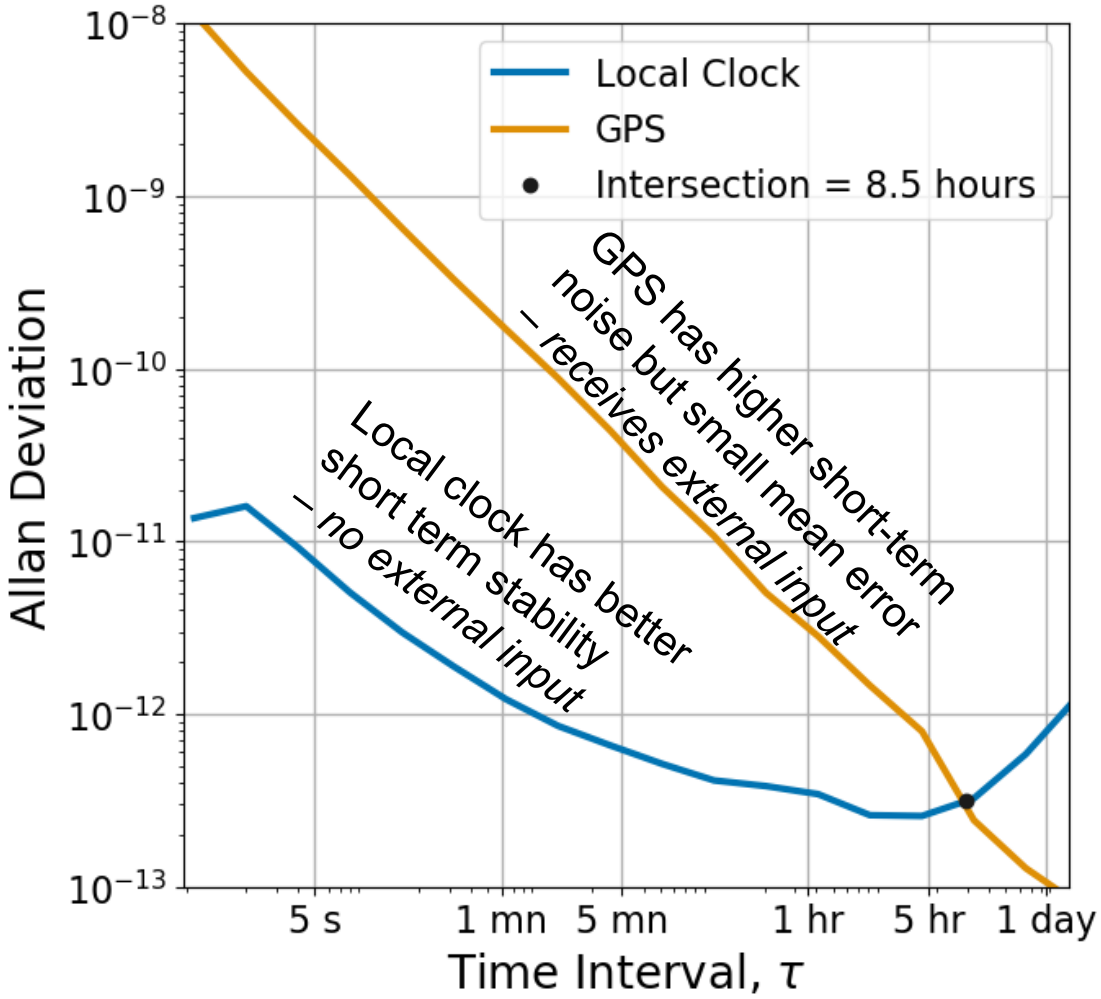
PNT Sources and PNT Systems



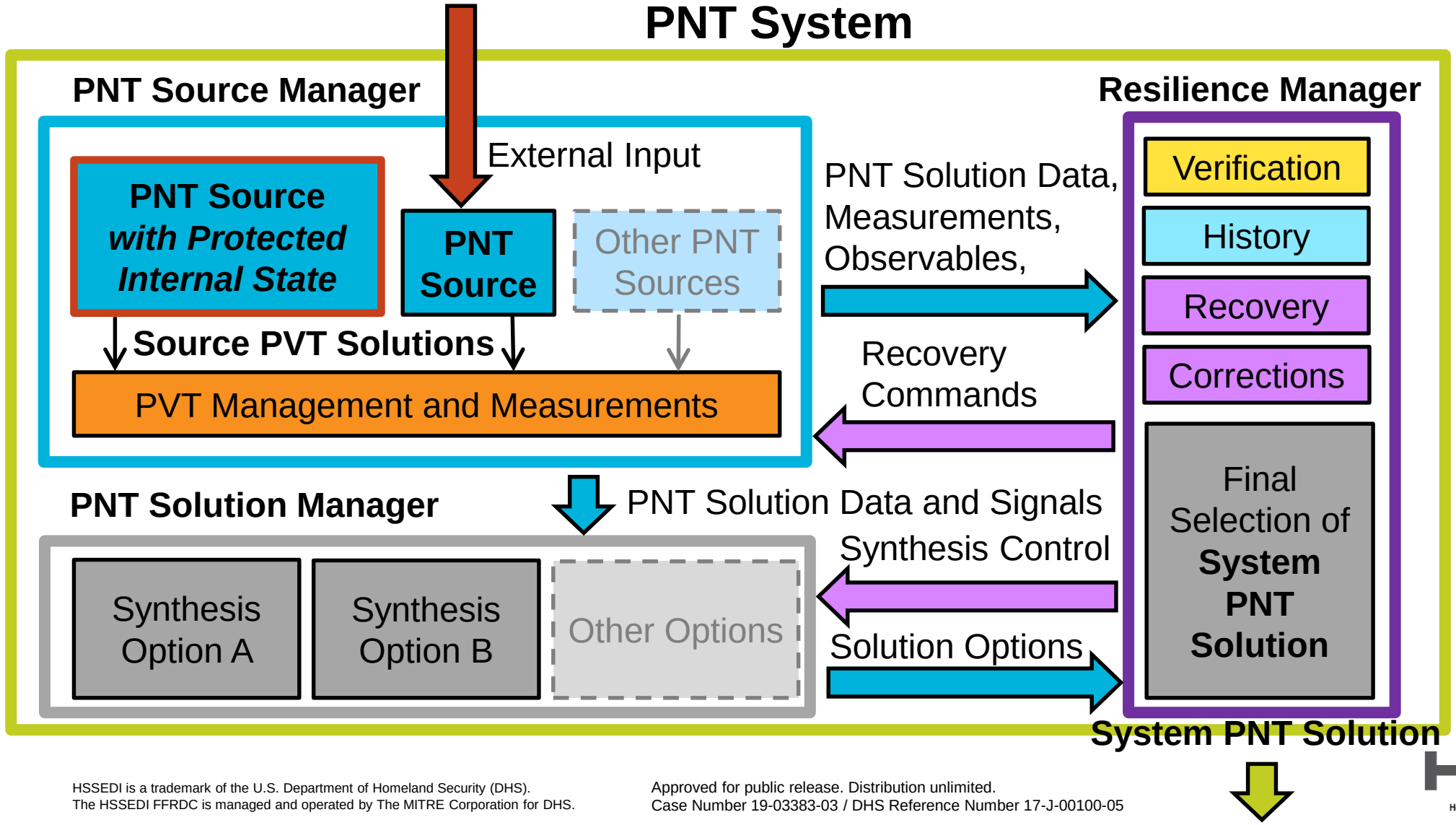
- **PNT Source:** A PNT System component that produces a Source PNT Solution.
  - Examples: oscillators and GNSS receivers
- **PNT System:** The components, processes, and parameters that collectively produce the System PNT Solution for the user.
- **PNT Solution:** The measurements or full solutions provided by a PNT System or PNT Source.
- **Resilient design includes:**
  - Selecting appropriate PNT Sources and managing them in a resilient way
  - Implementing resilient system architectures for PNT Systems that include resilient processes

Concepts for Resilient PNT Design: PNT Sources

- **Choose PNT Sources appropriate for the application**
  - ***Protected internal state***: PNT Sources that do not receive external input, such as oscillators
  - PNT Sources that receive ***external input*** are used to provide long-term stability to support the short-term stability of protected internal PNT Sources
  - PNT Sources that receive external input are vulnerable to external threats, so they need to be monitored and used carefully to maintain resilience



Resilient PNT Architecture

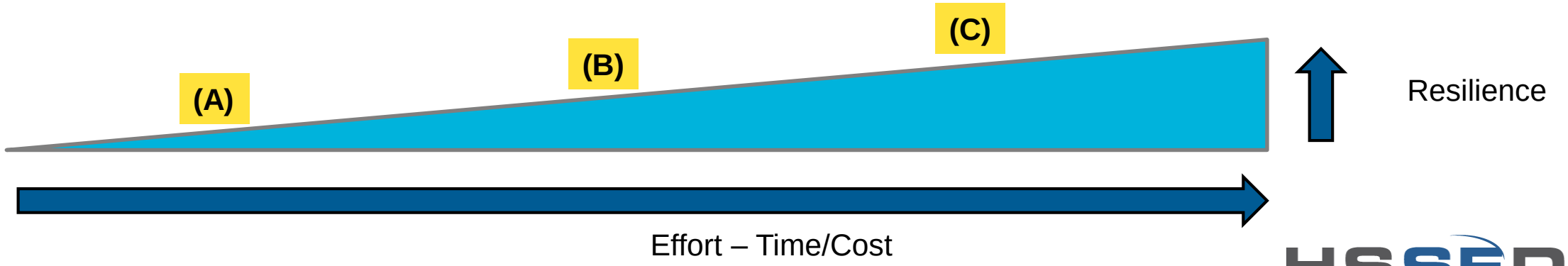


- **Different algorithms can be applied to the same protected internal state**
- **Internal state more protected without direct steering**

HSSEDI
Homeland Security Systems Engineering & Development Institute™

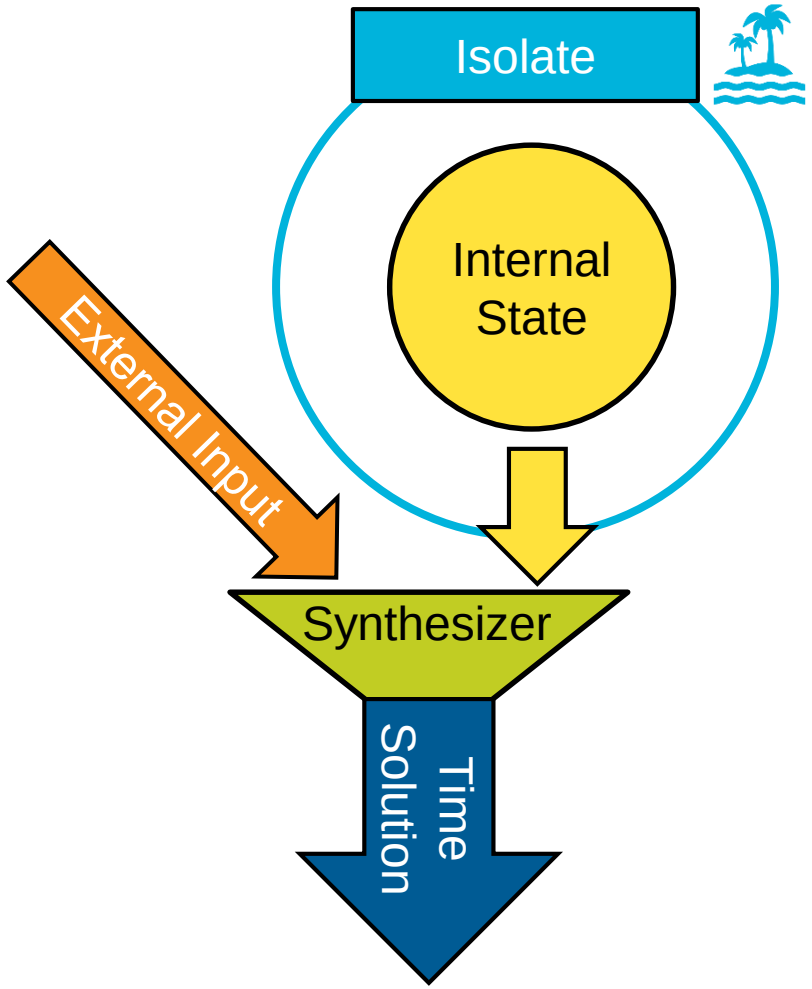
Resilient Approach to Control

- **Use known timing control algorithms in a resilient way**
  - **(A) Near term:** minor modifications to the execution of control algorithms in existing PNT Systems
  - **(B) Middle term:** Adding functions to existing control algorithms to increase resilience
  - There typically will be a trade-off between standard performance metrics and resilience. However, most PNT Systems have better performance than users need (orders of magnitude), so this trade-off is acceptable to gain resilience
- **Design and implement resilient control algorithms**
  - **(C) Long term:** PNT System architectures and control processes that are designed to be resilient from the ground up. Ensure the system meets both resilience and performance requirements.



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



Summary

- **Resilience should be considered part of the design space**
  - Not all systems require the highest level of resilience
  - There may be tradeoffs between performance, cost, and resilience
- **Use untrusted external sources sparingly**
  - Ideally protect an internal sensor (inertial, clocks, etc.)
- **Continue development of language and tools of resilience**
  - Allows end users to communicate needs to vendors and vendors to communicate capabilities to end users