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

Version 1.0

U.S. DEPARTMENT OF HOMELAND SECURITY

Science and Technology

Reference herein to any specific commercial products, processes or services by trade name, trademark, manufacturer or otherwise does not necessarily constitute or imply its endorsement, recommendation or favoring by the U.S. government.

The information and statements contained herein shall not be used for the purposes of advertising, nor to imply the endorsement or recommendation of the U.S. government.

With respect to information contained herein, neither the U.S. government nor any of its employees make any warranty, express or implied, including, but not limited to, the warranties of merchantability and fitness for a particular purpose. Further, neither the U.S. government nor any of its employees assume any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product, or process disclosed; nor do they assert that its use would not infringe privately owned rights.

POINT OF CONTACT

Organization: The Department of Homeland Security (DHS) Science and Technology Directorate (S&T)

Email: gps4critical-infrastructure@hq.dhs.gov

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

ACKNOWLEDGEMENTS

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) thanks the individuals and organizations who have reviewed and commented on this document.

EXECUTIVE SUMMARY

The Global Positioning System (GPS) and other Global Navigation Satellite Systems (GNSS) have enabled widespread adoption of Positioning, Navigation, and Timing (PNT) services in many applications across modern society. PNT services have become an invisible but essential utility for critical infrastructure operations across many sectors, including the electric power grid, communications infrastructure, transportation, agriculture, financial services, and emergency services. Therefore, disruption of or interference with PNT systems has the potential to cause adverse impacts on individuals, businesses, and the nation's economic and military security. The existence and nature of threats to PNT services are well known, and both government and industry have recognized the need for resilient[1] PNT equipment that can withstand and recover from such threats.

The U.S. Department of Homeland Security (DHS) encourages a holistic, cybersecurity-based approach to PNT resilience. In collaboration with industry, efforts to achieve this approach began with the *Resilient PNT Conformance Framework* [1] and have transitioned to the IEEE P1952 Working Group for development into voluntary standards. To ensure broad applicability, the *Resilient PNT Conformance Framework* was designed to be solution-agnostic and outcome-oriented, and therefore did not include concrete implementation examples.

The *Resilient PNT Reference Architecture* continues where the *Conformance Framework* left off by describing a concrete application of resilience concepts for a holistic approach to next-generation resilient PNT. It provides example implementations of resilience techniques as well as reference designs of architecture instances that align with the resilience levels within the *Resilient PNT Conformance Framework*.

Additionally, the *Resilient PNT Reference Architecture* advances PNT resilience concepts by incorporating applicable modern cybersecurity principles. This assumes that not only will PNT user equipment (UE) encounter attacks and disruptions but that some of these will get through the UE's defenses. To address this, the Reference Architecture is designed around seven PNT resilience concepts, with the core principle being managed trust—a concept derived from Zero Trust Architectures, which limit the impact of attacks when they penetrate systems.

The goal of this Reference Architecture is to create a concrete vision for a holistic approach to Next Generation Resilient PNT systems, and careful application of the discussed concepts and techniques can produce PNT UE that are highly resilient to both current and future PNT threats and strengthen the resilience of our national critical infrastructure.

[1] The Presidential Policy Directive for Critical Infrastructure Security and Resilience (PPD-21) defines resilience as "… the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions" [2].

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1.0 INTRODUCTION

1.1 Resilient PNT User Equipment for Critical Infrastructure

Global Navigation Satellite Systems (GNSS) are reliable, affordable, and ubiquitous services providing Positioning, Navigation, and Timing (PNT) information for many Critical Infrastructure (CI) applications. The Global Positioning System (GPS) is one GNSS that is widely used for PNT services in PNT user equipment (UE). However, most PNT UE was not designed with resilience as a priority and may be vulnerable to unintentional disruptions and targeted attacks enabled by progressively lower barriers to entry for attack capabilities. As a result, many CI sectors could lose access to PNT information if GPS or other GNSS services were disrupted, which also endangers downstream applications [3]. To prevent widespread failures, all components of civilian CI should incorporate resilient PNT UE [4].

Non-resilient GNSS receivers operate like simple radios with open ports, unconditionally accepting input, and are unequipped to adapt when GNSS signals are disrupted or manipulated. Modern PNT UE can leverage its similarity to computers, which allow adaptation of modern cybersecurity concepts to protect interfaces, monitor observables for consistency, manage risk, contain impacts from anomalous events, mitigate vulnerabilities, and apply a layered defense [5] [6] [7] [8] [9]. The U.S. Department of Homeland Security (DHS) encourages system designers to develop PNT UE with a holistic approach to PNT resilience [10]. The holistic approach recognizes that PNT resilience is a property of the whole PNT UE system, which is a combination of integrated elements that may or may not be resilient on their own.

The Definition of PNT Resilience

The Presidential Policy Directive for Critical Infrastructure Security and Resilience (PPD-21) defines resilience as:

> *… the ability to prepare for and adapt to changing conditions and <u>withstand and recover</u> rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.” [2]*

Withstanding threats implies continuing to provide PNT solutions in the event of malicious or accidental disruptions. Recovery signifies an ability to return to typical performance after attacks or disruptions have affected the system.

Using this definition, evaluators can rate PNT UE resilience based on the UE’s ability to recover from attacks or disruptions and its degree of resistance to PNT information degradation or loss. The *Resilient PNT Conformance Framework* (CF) [1] uses this approach to define four levels of PNT resilience and lays the groundwork for developing PNT UE that meets the requirements for each level. This Reference Architecture (RA) supports the CF by providing specific examples of resilience techniques and PNT UE system architecture instances that can meet the requirements of the different resilience levels. Section 1.2 outlines the structure of this document.

1.2 Reference Architecture Purpose and Format

This RA provides a structured way to design resilient civilian PNT UE systems based on a set of PNT resilience concepts. In this document, specific methods for implementing a particular aspect of resilience are called resilience techniques. The RA includes examples of architecture instances showing how systems can combine multiple resilience techniques to produce resilient outcomes and meet the requirements for different resilience levels as defined in the CF [1]. It also includes a categorization of resilience techniques to show the breadth of resilient behaviors and motivate the development of new approaches. The RA provides these examples to clarify the ideas in the CF. System designers have many ways to develop resilience in a PNT UE system. The examples presented show possible ways to implement resilience and are not meant to constrain the possible resilient PNT UE system designs which innovators could develop.

Definitions of PNT Resilience Concepts and Techniques

PNT resilience concepts: behavior models that describe how to impede attacks and minimize performance degradation due to threats and disruptions in a PNT UE system.

PNT resilience technique: a specific method for implementing a particular aspect of PNT resilience.

PNT resilience technique categories: groupings of PNT resilience techniques using a common strategy for implementing resilient behaviors.

Note that all PNT resilience concepts and techniques discussed in this document apply to civilian PNT UE systems. Resilience methods that require changes to existing PNT services and infrastructure, including GNSS signals, satellites, and ground stations, are also out of scope for this RA. The document only covers the resilience techniques and architectures of PNT UE systems, namely, the PNT equipment developed, integrated, and manufactured for consumer applications.

This document contains the following sections:

- **Section 1.0 Introduction**
  DHS S&T intends this RA to support the CF [1] with specific resilience concepts, technique categories, and concrete reference architecture implementations to aid in the development of resilient PNT UE. Section 1.0 introduces the document and describes the content of each section.

- **Section 2.0 Resilient PNT Conformance Framework**
  This section summarizes essential ideas defined in the CF [1], including the core functions of resilience and the resilience levels. Terms from the CF for the generic components, input, and output of a PNT UE system are also introduced to facilitate descriptions throughout the document using consistent language.

- **Section 3.0 PNT Resilience Concepts and Categories**
  System designers should assume that PNT UE will encounter threats and disruptions. To prepare PNT UE systems, they should implement PNT resilience concepts by integrating PNT resilience techniques into system designs using a holistic approach. This section shows how to adapt cyber resiliency concepts as well as Zero Trust

Architecture ideas and other cybersecurity concepts to the unique characteristics of PNT UE systems. PNT resilience concepts include assuming attacks and disruptions, defense in depth, minimizing attack opportunities, managed trust, protecting internal PNT sources, using broadly applicable threat mitigations, and recovering from successful attacks when needed. Subsections link the PNT resilience concepts to seven resilience technique categories: *Obfuscate, Limit, Verify, Isolate, Mitigate, Diversify,* and *Recover*.

- **Section 4.0 Graduated Resilience Level Architecture Examples**
  This section provides sample instances of resilient PNT UE system architectures that progress from lower to higher levels of resilience, showing how system designers can layer diverse resilience techniques to achieve different levels of resilient behavior. The examples in this section focus on a timing-only architecture, but system designers can apply the same concepts to develop positioning and navigation capabilities as well (see Section 5.3 for some examples). This section also shows how the elements from each architecture instance example fit into the seven categories of resilience techniques and introduces the idea of using three PNT UE Subsystems, which constitute part of the underlying RA, to organize the objectives of resilient PNT UE architectures.

- **Section 5.0 Integration of Resilience into Complete PNT UE Systems**
  Resilient PNT UE systems are composed of different resilience techniques combined to produce resilient outcomes. This section further explores how to design resilient PNT UE systems by presenting a discussion of the purposes and challenges confronting each of the three PNT UE subsystems. This includes handling complementary PNT sources in the PNT Source Controller, implementing defense in depth within the Resilience Manager, and overcoming challenges for the PNT Solution Synthesis Agent within position and navigation UE systems. Section 5.0 also considers PNT resilience in the broader context of the overall PNT user space, where it can overlap with the related objectives of PNT assurance and PNT situational awareness (SA).

- **Section 6.0 Summary: Next Generation Resilient PNT Architectures**
  This section reviews the main ideas from the previous sections and relates them to the objectives of next generation resilient PNT, which includes PNT assurance, PNT SA, and the resilient PNT UE objectives represented by the roles of the three PNT UE system subsystems: PNT Source Controller, Resilience Manager, and System PNT Solution Synthesis Agent.

- **Appendix A: Resilience Technique Examples**
  This appendix describes each of the seven categories of resilience techniques in detail to enable UE designers to visualize resilient qualities and aid in selecting appropriate techniques and developing new ones. These categories are *Obfuscate, Limit, Verify, Isolate, Mitigate, Diversify,* and *Recover*. The appendix briefly describes examples of specific resilience techniques to help clarify the resilient behavior included in each category. The appendix does not include a comprehensive list of all possible resilience techniques, and the examples included should not be interpreted as DHS’s preferred methods.

- **Appendix B: PNT Threats and Disruptions**
  This appendix summarizes in broad terms the different types of PNT threats and disruptions that can affect PNT UE systems.

- **Appendix C: PNT UE Boundaries**
  The outer boundary of PNT UE defines the equipment for which resilience behaviors are evaluated. This appendix summarizes three recursive outer boundaries that were defined in the CF [1]: fundamental PNT measurements, PNT integrated receiver, and PNT system of systems.

- **Appendix D: Definitions**
  A list of definitions for key terms used in this document.

- **Appendix E: Acronyms**
  A list of acronyms used in this document.

Figure 1 shows the connections between the ideas in Sections 2.0-6.0 and Appendix A. As noted, Section 2.0 introduces the core ideas from the CF.

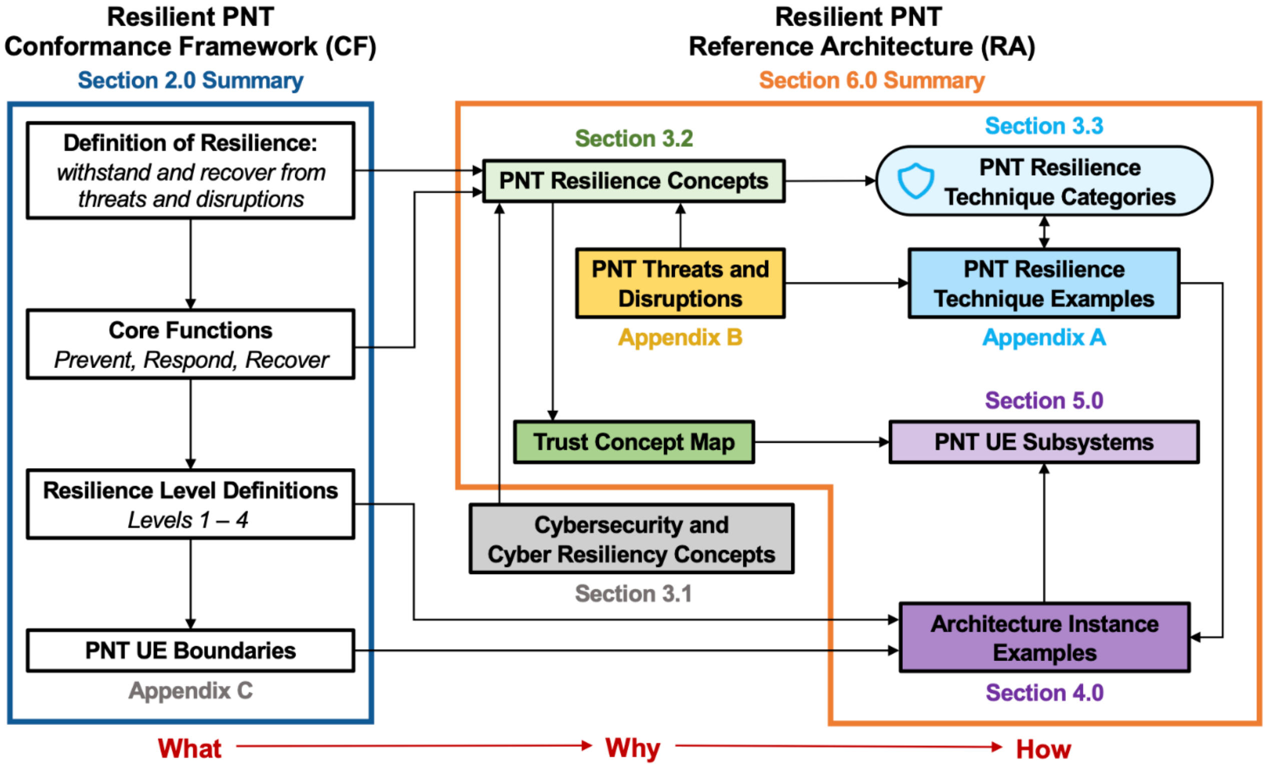

Resilient PNT
Conformance Framework (CF)
Section 2.0 Summary
Resilient PNT
Reference Architecture (RA)
Section 6.0 Summary
Definition of Resilience:
withstand and recover from threats and disruptions
Core Functions
Prevent, Respond, Recover
Resilience Level Definitions
Levels 1 – 4
PNT UE Boundaries
Appendix C
Section 3.2
PNT Resilience Concepts
Section 3.3
PNT Resilience Technique Categories
PNT Threats and Disruptions
Appendix B
PNT Resilience Technique Examples
Appendix A
Section 5.0
Trust Concept Map
PNT UE Subsystems
Cybersecurity and Cyber Resiliency Concepts
Section 3.1
Architecture Instance Examples
Section 4.0
What
Why
How

Figure 1. Conceptual map of the ideas in this RA (orange box) and connections with the main ideas in the CF (blue box).

Many examples in this document focus on GNSS. This reflects the abundance of GNSS-related material in the open literature and is not intended to promote GNSS over other PNT sources. The RA contains many concepts and terms from GNSS, and efforts to place relevant definitions in the appendix have been made. However, an in-depth discussion of GNSS receiver signal processing is beyond the scope of this document. More information can be found in GNSS textbooks [11] [12].

System designers must consider both the specific resilience techniques chosen and the way they are incorporated in the PNT UE system to achieve resilient outcomes. DHS S&T intends this document to support the CF with specific resilience concepts and concrete reference architecture implementations to aid in the development of resilient PNT UE. Additionally, this reference architecture is intended to explain the relevance and role of incorporating cybersecurity concepts for Next Generation Resilient PNT.

2.0 THE RESILIENT PNT CONFORMANCE FRAMEWORK

This section reviews the main concepts contained in the CF [1]. DHS S&T and CISA developed the CF with industry and government partners collaborating in a working group. The document uses three core functions to explain ways of implementing resilience. It also describes four levels of resilience and their associated requirements and outlines high-level architecture concepts for the lower levels. The level definitions in the CF were non-prescriptive to encourage innovation. Additionally, the levels were designed with market adoption and feasibility in mind, bridging from currently available UE features to next generation resilient PNT. The definitions of the four levels of resilience facilitate the adoption of resilient PNT UE and lay the groundwork for standards development. Overall, the CF introduces a common language for PNT resilience that can be shared by PNT users, manufacturers, integrators, vendors, and government across CI sectors.

This section includes four subsections and connects to later sections as follows

- **Section 2.1** defines general terms for PNT UE systems and their sub-components.
- **Section 2.2** reviews the core functions of resilience introduced in the CF: *Prevent, Respond,* and *Recover*.
- **Section 2.3** summarizes the four levels of resilience defined in the CF and shows how they connect to the core functions of resilience.
- **Section 2.4** points to the CF to review software assurance practices for PNT UE.
- **Section 3.0** defines seven PNT resilience concepts and connects them to the core functions of resilience from Section 2.2.
- **Section 4.0** describes resilient PNT UE architecture instance examples, using the terms described in Section 2.1, to meet the requirements for the resilience levels summarized in Section 2.3.

2.1 General Terms for Resilient PNT UE

This RA uses general terms for components of resilient PNT UE systems, as defined in the CF [1], to facilitate discussions about system architectures. Figure 2 shows the generic terms used in a schematic diagram of a PNT UE system. This diagram adds to Figure 2 from the CF [1] to emphasize that the generic PNT system applies to UE and to include PNT state information, PNT assurance, and PNT SA. Appendix C describes three recursive boundaries to define different scopes of PNT UE over which PNT resilience can be evaluated.

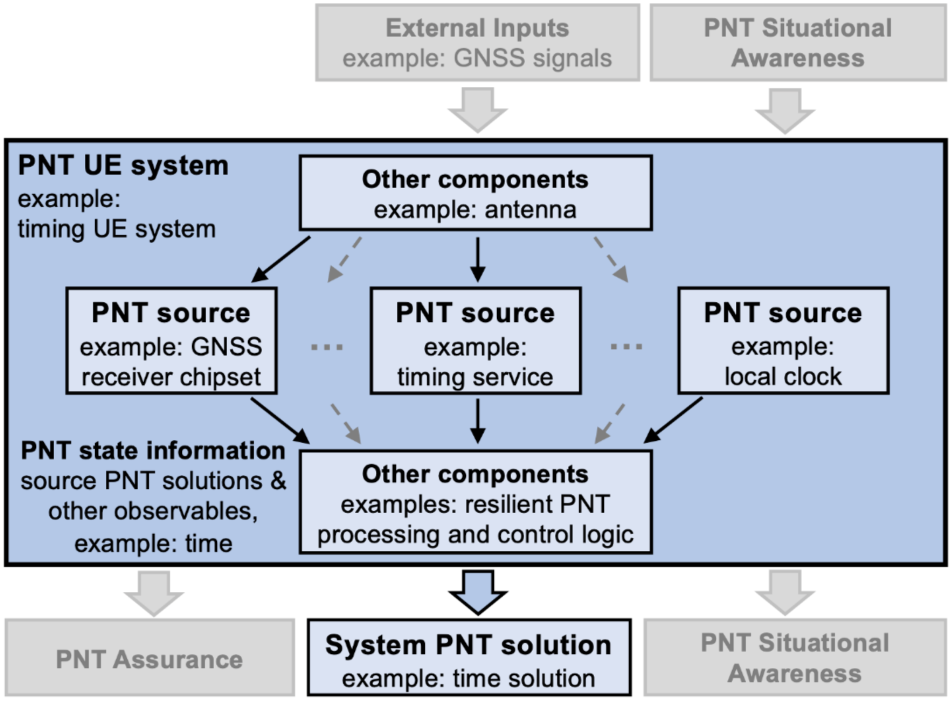


Figure 2. Generic components of a PNT UE system.

The **PNT UE system** contains the integrated components and processing that collectively provide a **system PNT solution** to the user. Example PNT UE systems include UE for timing or navigation applications. These systems can comprise multiple different components and subsystems. The PNT UE system must include one or more **PNT sources**, which may or may not rely on **external input** to the system. PNT UE systems can synthesize the system PNT solution using **PNT state information** from multiple PNT sources through a variety of methods. A PNT UE system may include **other components** to aid in the generation of a system PNT solution and perform resilient functions.

In the context of this RA, **PNT sources** include the sensors and signal processing components of the PNT technology that provide PNT state information within PNT UE systems. Some PNT sources rely on external input, such as GNSS receivers that sense and process signals radiated from satellites; and network connections using different protocols to communicate with remote PNT sources. PNT UE may use other components, such as different types of antennas, to collect external signals and provide them to PNT sources that require external input. Examples of sources that do not require external input are local clocks that generate an independent timing signal and Inertial Navigation Systems (INS) that use inertial sensors to measure relative position. Some different types of PNT sources are categorized in Appendix C.

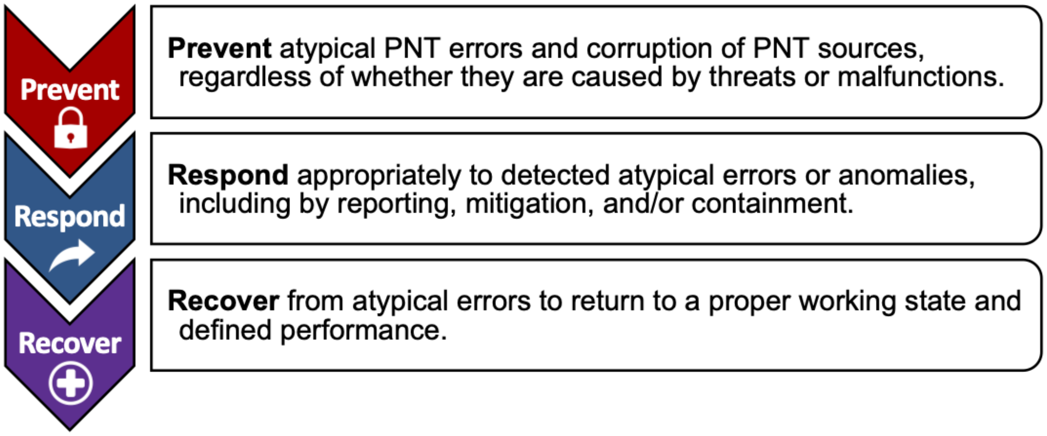
The different PNT sources pass **PNT state information** to other internal components that process the information and execute resilient functions to produce the system PNT solution for the user. PNT state information includes the position, velocity, navigation information, time, and/or other observables captured from the PNT sources. Observables are measured quantities or calculated values used in a system's internal signal processing, such as signal power measurements. Other system components can use the PNT state information to apply resilience techniques and execute resilient behavior.

The **system PNT solution** consists of the PNT information output to the user. Navigation UE systems include position, velocity, navigation, and time information in the system PNT solution. For timing UE, the system PNT solution would only include time information. However, the internal PNT state information for timing UE systems may include other observables if various resilience techniques can use them. An example would be verifying that a stationary GPS receiver used for its time solution continues to report the correct known position of the antenna.

In addition to resilient system PNT solutions, next generation PNT UE systems will likely produce **PNT SA** and **PNT assurance**, which is a rigorous assessment of integrity used to establish trustworthiness. These products are related to and intersect with PNT resilience but may not be necessary to construct resilient PNT UE systems. Devices outside the PNT UE system may also produce PNT SA information and provide it as an input to support resilience techniques. Section 5.4 describes the overlap between PNT SA, assurance, and resilience with respect to the overall user space for next-generation PNT UE.

2.2 The Core Functions of Resilience

The CF [1] introduces the three core functions of resilience: *Prevent, Respond*, and *Recover*. The core functions broadly categorize the capabilities necessary for achieving resilience as defined in PPD-21 [2] and are described in Figure 3.



Prevent atypical PNT errors and corruption of PNT sources, regardless of whether they are caused by threats or malfunctions.

Respond appropriately to detected atypical errors or anomalies, including by reporting, mitigation, and/or containment.

Recover from atypical errors to return to a proper working state and defined performance.

Figure 3. Core functions of resilience from the CF [1].

The typical performance of a PNT UE system is the product of the inherent capabilities of the system, which may be bounded by a typical error level. For example, typical errors for a free-running clock will include drift as part of normal operation. Atypical errors are outside of the calibrated uncertainty bounds of the system within a specified confidence interval and may be caused by threats or malfunctions. Atypical errors can include the case where the error is less than the expected performance error due to manipulation.

The ***Prevent*** core function refers to preventing atypical PNT errors as well as corruption of PNT sources, regardless of the cause. This is the first line of defense because if prevention succeeds, response to and recovery from those atypical errors are unnecessary.

The ***Respond*** core function entails reacting appropriately to detected anomalies, with possible responses including reporting, mitigation, containment, and backup options. A suitable response to an atypical PNT error allows the PNT UE system to avoid the actions involved in recovery.

The ***Recover*** core function indicates that PNT UE should always have the capability to recover from threats and disruptions as the last line of defense. All resilient PNT UE systems must be able to recover typical performance and return to a proper working state. Recovery appears explicitly as a core function, a PNT resilience concept (Section 3.2), and a PNT resilience technique category (Appendix A.7) because it is an essential part of the definition of resilience.

2.3 PNT Resilience Levels

The four resilience levels defined in the CF [1] rank degrees of resilience. Resilience levels give CI applications and other PNT users the ability to specify the type of resilience they need. The levels also provide a framework for system integrators and manufacturers to communicate with each other to produce resilient PNT UE that meets the specified user needs. Improving the resilience level of a PNT UE system will likely increase the complexity and cost.

The rows in Table 1 give the minimum requirements for each resilience level, including numbered requirements and overall system performance requirements. The columns show how each numbered requirement is aligned with the three core functions described in Section 2.2. The levels are cumulative, so each higher level incorporates all the numbered requirements for the levels below it. Factors such as implementation cost and technology availability may drive gradual upgrades to the PNT UE ecosystem over time. High level PNT UE system of systems for CI applications may be built from PNT integrated receivers and fundamental PNT measurements with lower resilience levels. Appendix C provides further discussion of the different resilience levels that may apply to different PNT UE boundaries.

The performance requirements describe the expected behavior of a PNT UE system at each level when faced with a threat. Performance is measured by the metrics relevant for the application using the PNT UE. Relevant performance metrics may include accuracy, availability, integrity, continuity, and/or coverage. As described in the CF [1], a complete statement expressing the demonstrated resilience level of a PNT UE system would include a quantitative statement about the measured performance in terms of the relevant metrics for the application and a description of the threat models used for the resilience evaluation. PNT users can choose appropriate PNT UE systems for their application based on the evaluated resilience level given for combinations of relevant performance metrics and threat models.

Intended Use of Resilience Levels

Level 1 *is intended to be easily achievable, even for low-cost PNT UE, which account for a large segment of the market.* Generally appropriate for non-critical applications, Level 1 creates a sound foundation on which to base higher-level systems.

Level 2 *is likely the minimum resilience level that CI applications can accept*. Continuing to provide a PNT solution during a threat or disruption generally requires improved hardware and software functionality as compared to Level 1, with an anticipated higher cost.

Level 3 *delivers acceptable PNT solutions in the presence of a threat or disruption for a longer duration than lower levels*. Choosing this level of resilience over Level 2 depends on the relevant timeframes for the application criticality and potential threats and disruptions.

Level 4 *is the highest level of resilience, providing performance unaffected by a threat or disruption.* This level reflects evolutionary resilience goals for the CI PNT environment.

Table 1. Cumulative PNT resilience level requirements, from the CF [1].

Resilience Levels*	Performance Requirement	Prevent	Respond	Recover
Level 1	**Ensures recoverability after removal of the threat.** With numbers (1)-(3)	(1) Must verify that stored data from external inputs adheres to values and formats of established standards.	(2) Must support full system recovery by	
				(3) Must include the ability to securely reload or update firmware.
Level 2**	**Provides a solution (possibly with unbounded*** degradation) during threat.** With numbers (1)-(5)	(4) Must identify compromised PNT sources and prevent them from contributing to erroneous PNT solutions.		
			(5) Must support automatic recovery of	
Level 3	**Provides a solution (with bounded degradation) during threat.** With numbers (1)-(7)	(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.** With numbers	(8) Must have diversity of PNT source technology to mitigate		
Note	* **Level 0** indicates a source or system that does not meet the criteria in Level 1, and thus is considered a non-resilient system or source. ** CI applications will likely require Level 2 resilience at a minimum. *** The output can deviate within a manufacturer defined envelope.			

Level 1 is the lowest level of PNT resilience, serving as the foundation for all the levels above it by laying out minimum recovery requirements. This level focuses on recovery as the appropriate response when a threat or disruption is over. This level also includes basic verification steps to confirm that external inputs adhere to established standards and thus prevent nonconforming data from being stored to memory. As the minimum ranking, Level 1 resilience would not be appropriate for most CI applications. However, this level provides an entry point to introduce some resilience attributes with minimal upgrades to existing devices, which can enable widespread implementation in user products. Systems with higher levels of resilience may also incorporate Level 1 components with the expectation that recovery can be commanded by system functions.

At **Level 2**, a resilient PNT UE system responds to the presence of a threat by temporarily isolating compromised PNT sources to prevent them from contributing to the system PNT solution. Internal monitors determine when it is safe to initiate automatic recovery. Overall, the Level 2 system must continue to provide a PNT solution in the presence of a threat, but the requirements do not place any bounds on the degree of performance degradation during this time. The Level 2 requirements imply the need for a local, physical PNT source to use for holdover, but do not stipulate the number and type of PNT sources. Level 2 is likely the minimum resilience level that is suitable for CI applications.

Level 3 involves isolating PNT sources from each other to prevent cross-contamination when one PNT source is compromised. This level is also the first to explicitly require cross-verification between PNT solutions from different PNT sources. To achieve Level 3, resilient PNT UE systems may require additional hardware, which may include three or more PNT sources. PNT UE systems at Level 3 may exhibit degraded performance in the presence of a threat but must place bounds on the level of degradation. The difference between Level 3 and Level 2 performance is that Level 3 resilient PNT UE systems must maintain performance within the defined bounds indefinitely, whereas Level 2 systems can exhibit unbounded, continually increasing degradation throughout the duration of the threat.

At **Level 4**, the required diversity among the PNT source types prevents local sources from losing validated external input when other PNT sources are disrupted. In the presence of a threat that affects one type of PNT source, resilient PNT UE systems can respond by using different types of PNT sources and the affected PNT sources can recover when the threat is removed or the disruption is over. The difference between the system PNT solution performance for Level 3 versus Level 4 is that Level 3 is allowed to have a bounded performance degradation during the threat, while Level 4 systems must maintain their performance regardless of threat conditions.

Level 0 refers to PNT UE systems that do not meet the minimum resilience requirements for Level 1. This provides a term for non-resilient systems in the context of the resilience levels.

2.4 Software Assurance

Modern PNT UE systems include significant amounts of software and should be treated like computers when it comes to incorporating appropriate software assurance. The CF [1] and this document do not focus on software assurance, but such assurance remains an important aspect of resilient PNT UE design that ensures software performs as expected. Software assurance is covered in depth elsewhere [13] [14]. The CF includes a list of example software assurance techniques to facilitate their adoption in resilient PNT UE systems.

3.0 PNT RESILIENCE CONCEPTS AND CATEGORIES

To achieve the desired resilience for next generation PNT UE, system designers should be guided by PNT resilience concepts based on inherent PNT characteristics and inspired by mature resilience and security practices from related domains. Modern PNT UE systems include features executed on internal computers and handle different types of digital information, so it is sensible to implement cybersecurity and cyber resiliency practices directly in these systems to manage risk. Further, when cybersecurity and cyber resiliency concepts are adapted to the PNT domain, they can also contribute to the development of resilience concepts tailored specifically to PNT UE characteristics.

This section includes three subsections and connects to later sections as follows:

- **Section 3.1** outlines the role of cybersecurity and cyber resiliency for next generation PNT UE systems.
- **Section 3.2** describes seven PNT resilience concepts from the perspective of managing trust in PNT UE systems.
- **Section 3.3** maps the seven PNT resilience concepts to seven categories of PNT resilience techniques that system designers can use to implement the concepts.
- **Section 4.0** includes specific resilience techniques from each of the seven categories in examples of graduated resilience level architectures.
- **Appendix A** describes the seven resilience technique categories in detail and describes additional examples of resilience techniques.

3.1 The Role of Cybersecurity and Cyber Resiliency in Next Generation PNT

Cybersecurity and cyber resiliency practices protect computer systems and digitally formatted information. ***Cybersecurity*** protects information and systems by preventing, detecting, and responding to attacks [6]. One approach to cybersecurity seeks to limit harm by making it difficult for attackers to achieve their desired effects on the system. For example, ***Zero Trust*** concepts assume attacks will happen and minimize uncertainty by enforcing least privilege access decisions [15]. ***Cyber resiliency*** includes the ability to anticipate, withstand, recover from, and adapt to different types of attacks and disruptions that can affect computer systems and other hardware that handles digital information [5]. Both cybersecurity and cyber resiliency practices apply to PNT UE systems because they include computer elements and handle digital information. Further, PNT UE systems that receive external input should apply similar risk management methods at external interfaces as computer systems use when connected to a network. Adapted to the PNT domain, cybersecurity and cyber resiliency practices can guide the development of risk management concepts tailored to PNT UE systems.

The *NIST Framework for Improving Critical Infrastructure Cybersecurity* [6] provides guidance to help organizations better manage cybersecurity risk. It organizes risk management activities into five high-level functions: *Identify, Protect, Detect, Respond*, and *Recover*. The security concepts from the document can be adapted to other domains. For example, the *Foundational PNT Profile* [7] [8] applies the *NIST Cybersecurity Framework* [6] to PNT services. The ideas in these documents are oriented towards improving risk management and risk reduction practices for organizations, but the guidance to identify risks, prepare for attacks, monitor for anomalies, contain or mitigate problems, and restore capabilities can also apply broadly to resilient system design.

Inspired by the five high-level functions for risk management identified by the *NIST Cybersecurity Framework* [6]*,* the CF [1] developed three core functions for resilient PNT UE system designs: *Prevent, Respond,* and *Recover*, which were introduced in Section 2.2. There are differences between the two sets of functions because of the different domains that they apply to; the *NIST Cybersecurity Framework* provides security guidance to organizations while the CF provides resiliency guidance for PNT UE systems. Note that the *Detect* function for risk management is included implicitly in the core functions of resilience for PNT UE because some methods to prevent, respond to, and recover from threats may involve detecting the effects of threats on a PNT UE system and reacting to them. The *Identify* cybersecurity function can apply to engineering activities to categorize and prepare for threats and hazards that could impact PNT services by implementing *Prevent, Respond*, and *Recover* functions to produce resilient PNT UE system architectures.

Cyber resiliency engineering is a related discipline that seeks to develop more trustworthy systems that can anticipate, withstand, recover from, and adapt to different types of attacks and disruptions. Techniques and approaches to implement cyber resiliency are described in Developing Cyber-Resilient Systems, *NIST Special Publication 800-160, Volume 2, Revision 1 (NIST SP 800-160, V2 R1)* [5]. In addition to assuming attacks, cyber resiliency recognizes that the effects of attacks may not be detected immediately or may never be detected. *NIST SP 800-160, V2 R1* [5] describes several methods to build cyber-resilient systems that are not dependent on direct threat detection, including techniques for *Coordinated Protection, Deception, Diversity, Redundancy, Unpredictability*, and the *Predefined Segmentation* approach, among others. Cyber resiliency techniques that involve detecting the effects of attacks to some degree include *Analytic Monitoring, Contextual Awareness*, and *Substantiated Integrity*, as well as the *Consistency Analysis* approach. The next subsections describe PNT resilience concepts (Section 3.2) and PNT resilience techniques (Section 3.3) that are related to these cyber resiliency techniques and approaches.

While threat detection techniques are an important part of PNT resilience, this RA also recognizes PNT UE architecture approaches that implement resilient behavior without directly requiring detection. Cybersecurity and cyber resiliency concepts can be used as a guide to inspire PNT resilience concepts for PNT UE systems both with and without requiring detection. For example, the *Segmentation* cyber resiliency technique includes two approaches that can be adapted in different ways to implement PNT resilience. The *Dynamic Segmentation and Isolation* approach can be used to isolate resources in response to detected threats to contain negative effects. In contrast, the *Predefined Segmentation* approach divides resources based on trustworthiness or criticality to protect them separately and isolate them if necessary [5]. This approach contains the effects of threats and supports controlled risk management between segmented elements. From cybersecurity, *Zero Trust* concepts acknowledge that threats can be present both inside and outside traditional network boundaries, so they enforce least privilege access decisions between elements [15]. A *Zero Trust Architecture* eliminates implicit trust in any one element or service and instead requires continuous verification [5] [15]. These ideas can be adapted to PNT resilience concepts to manage PNT information in a controlled and deliberate way, appropriate for its merited trustworthiness, both within the PNT UE system and at external interfaces.

3.2 PNT Resilience Concepts for a Holistic Approach

PNT resilience concepts explain how to prevent, respond to, and recover from the effects that threats and disruptions can have on a PNT UE system. A *holistic* approach to applying PNT resilience concepts considers the resilient behaviors of individual elements, their interactions with each other, and how they are integrated collectively into the overall system to produce resilient outcomes, which include the ability to withstand and recover from threats and disruptions. Section 3.1 reviewed how PNT resilience concepts can be inspired by cybersecurity and cyber resiliency practices to manage risk in a PNT UE system and make it hard for attacks and disruptions to cause problems. This subsection describes seven PNT resilience concepts that can be integrated using a holistic approach to develop resilient PNT UE system designs.

Risk management concepts describe how data and components with different degrees of trustworthiness should be handled in a system to control the effects of an attack or disruption. In the context of this RA, *trustworthiness* is the degree to which users can have reasonable confidence that a UE element has *integrity*, which in turn is the property of conforming to expected behaviors, preserving quality, and avoiding manipulation. PNT assurance quantifies the level of confidence that PNT information has integrity, which can be a rigorous way to establish a level of trustworthiness. Relative degrees of trustworthiness can also be determined based on the inherent properties of a UE element and how it is integrated into the PNT UE system.

Instead of showing the physical layout of a resilient PNT UE system, Figure 4 depicts PNT resilience concepts on a conceptual trust map centered around degrees of trustworthiness within the system. The trusted core, shown at the center of Figure 4, reflects the aspects of the system that merit a greater trustworthiness. The outer edge of the system, depicted by the red outer band, contains elements that are inherently untrusted because they are attack surfaces. Boundaries are established between the trusted core and the untrusted edge of the system to create isolation between the different components and functions. PNT information that comes into the system at the untrusted edge can transition to the trusted core to be part of the system PNT solution through a controlled verification process that includes different methods to monitor for anomalies at the boundary interfaces.

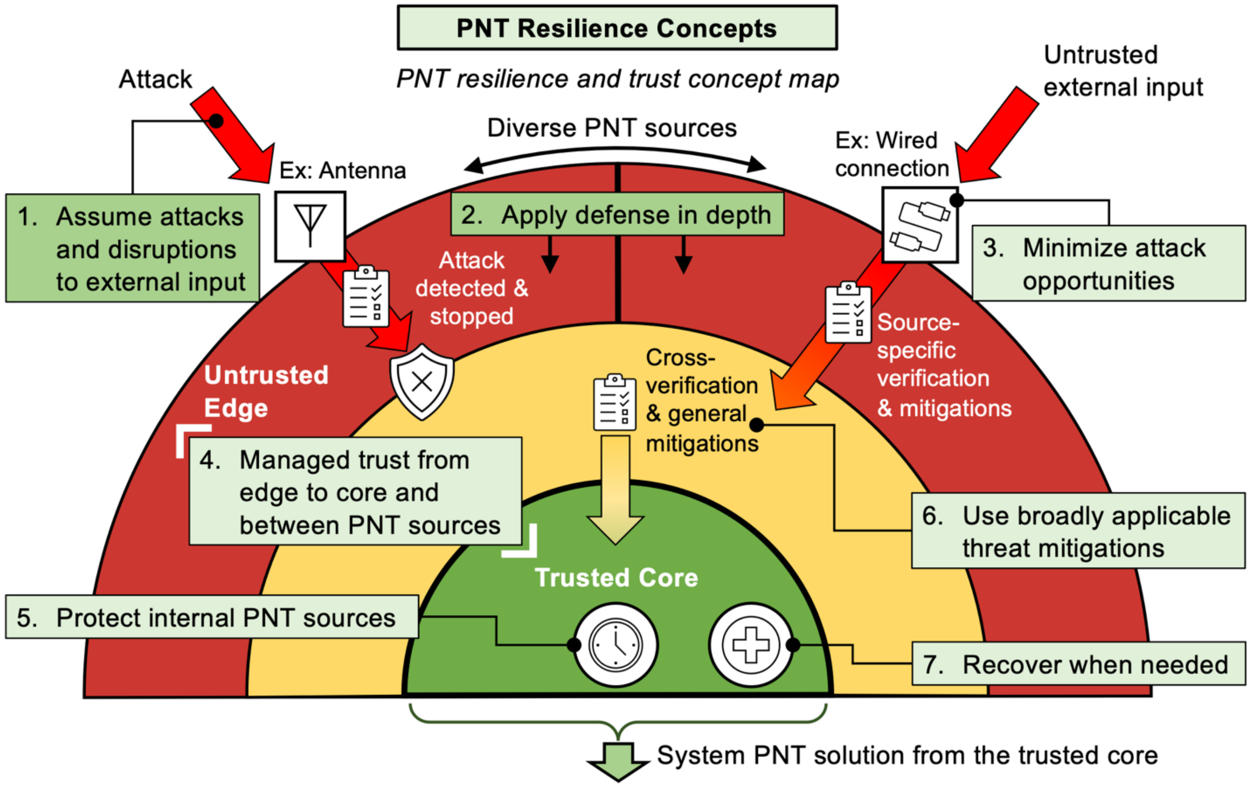

PNT Resilience Concepts
PNT resilience and trust concept map
Attack
Untrusted external input
Diverse PNT sources
Ex: Antenna
Ex: Wired connection
1. Assume attacks and disruptions to external input
2. Apply defense in depth
3. Minimize attack opportunities
Attack detected & stopped
Source-specific verification & mitigations
Untrusted Edge
Cross-verification & general mitigations
4. Managed trust from edge to core and between PNT sources
6. Use broadly applicable threat mitigations
Trusted Core
5. Protect internal PNT sources
7. Recover when needed
System PNT solution from the trusted core

Figure 4. Conceptual representation of trust in a PNT UE system and PNT resilience concepts. The managed trust concept relies upon verification and isolation methods.

PNT UE systems can have internal PNT sources that produce PNT state information based on measured physical qualities and do not require external input after an initial training or calibration is completed. Examples of internal PNT sources include local clocks, such as rubidium or cesium atomic clocks, and Inertial Navigation Systems (INS), which contain different types of inertial sensors to measure relative motion. These types of sensors inherently merit greater trust when they are protected from the influence of external input, so they can reside in the trusted core depicted in Figure 4. These internal PNT sources should also be protected from supply chain issues and cyber-attacks to justify the assumption of their integrity.

The PNT information in the trusted core generates the system PNT solution. That information includes output from protected internal PNT sources and information from external input that has been verified at the controlled boundary interfaces between system layers. Recovery functions also reside in the trusted core because reset and rollback recovery states must come from trustworthy PNT state information.

The list below summarizes the PNT resilience concepts shown in Figure 4. In Section 3.3 the PNT resilience concepts are applied to form categories of resilience techniques.

PNT Resilience Concepts

1. **Assume attacks and disruptions to external input**
   System designers should assume that all types of PNT services providing external input can and will be attacked and disrupted, that the effects from some attacks will manifest within the system, and that these attacks will become more sophisticated over time. The untrusted edge, where external input enters the system, is the most likely attack surface. However, attacks and disruptions can cause a variety of different effects throughout the system, so to be prepared, a resilient defense must incorporate diverse techniques that work together to withstand threats and enable recovery.

   PNT services include any source and method of distributing PNT information. During transmission the PNT information can be partially or fully blocked, so resilient PNT UE systems should be prepared for disruptions where external input is degraded or absent. Transmitted PNT information may also be intercepted and manipulated to deceive the receiver, so any external information that comes into the resilient PNT UE system could be incorrect and should not be inherently trusted. Further, any part of the PNT UE system may fail due to internal errors or external attack. Even PNT UE systems designed primarily to withstand threats must include the ability to recover because unexpected failures may occur or new threats may break through their defenses. System designers should assess possible threats, vulnerabilities, and failures and design PNT UE systems to be prepared to prevent, respond, and recover from these problems with a holistic approach to PNT resilience.

2. **Apply defense in depth**
   This concept is depicted by the layers of defense from edge to core for each of the diverse PNT sources around the red outer band in Figure 4. The PNT UE builds a strong defense from complementary layers that work together to prevent, respond to, and recover from a variety of different issues that may arise in the system. This includes controlling external interfaces where attackers can gain access, protecting the trusted core, and evaluating elements and information between the edge and trusted core for manipulation or malfunction.

   The resilience concept of defense in depth involves layering different types of resilience techniques to reduce the likelihood that an attack or disruption will defeat a system's defenses. Resilience techniques have different strengths and weaknesses and layering them together throughout a system has the cumulative effect of covering individual shortcomings. In the event a particular layer of defense is defeated, there will remain additional layers of defense to impede or block attacks. This not only significantly increases the difficulty for an attack to disrupt a system, but these different layered defenses also provide protection against a broader set of attacks than a single layer of defense.

3. **Minimize attack opportunities**
   As a first line of defense, system designers should make it hard to gain access to the system. They should determine the attack surfaces of the PNT UE system and minimize or obfuscate them as much as possible to prevent threat impacts. Limiting reliance on external input also helps moderate the effects of threats and disruptions to PNT services.

   Interfaces at which PNT information is received from outside the PNT UE system are attack surfaces where incorrect information can be injected or true information can be denied. Obfuscating or disguising input interfaces where external input is consumed can make it harder for outside threats to deceive the PNT UE system. These attack surfaces can also be minimized by limiting the allowed input at the interfaces. For example, interfaces can limit the allowed frequency and arrival direction of radiated signals received by the PNT UE system.

Besides minimizing attack surfaces to protect PNT UE systems, system architectures can also include methods to reduce exposure to external input. To implement this concept, designers can add internal PNT sources that do not require external input, such as local clocks, to PNT UE systems to enable holdover periods without external input. Limiting the influence of external input can make it harder for outside threats to deceive the PNT UE system.

4. **Managed trust from edge to core and between PNT sources**
   Because of the assumption that PNT UE systems will be attacked, and some attacks will penetrate the defenses, the UE should practice managed trust to control information distribution within the system. The concept of *managed trust* in this context is adapted from the idea of *zero trust architectures* in cybersecurity. Managed trust is a multifaceted concept that leverages several different types of resilience techniques to limit the use of external input, isolate components from each other to prevent corruption from spreading vertically or laterally, and verify external input before it is allowed to influence the system PNT solution.

   In a managed trust architecture, PNT information is controlled deliberately based on its trustworthiness. This concept includes limiting the external input allowed into the system and restricting how external input propagates through the system vertically through rigorous verification procedures. Lateral isolation of components is also needed, especially between different PNT sources at the untrusted edge of the system where external input is received. This prevents threats that affect the information from one PNT source from spreading laterally within the system to corrupt the information from other PNT sources.

   Components at the untrusted edge of a device, such as PNT sources that accept external input, have the highest exposure to threats. The UE should not trust information from these PNT sources until it is checked for consistency and/or authenticated, which occurs in the layers of defense providing boundaries between the untrusted edge and the trusted core in Figure 4. In contrast, components that do not accept external input, such as internal physical PNT sources, have inherent trustworthiness and should be adequately protected to preserve integrity. When information must be shared between components, the interaction should take place in a controlled and deliberate manner to maintain the inherent trustworthiness of the internal PNT sources. Trustworthiness must be established before PNT information is used in any way that contributes to the system PNT solution

5. **Protect internal PNT sources**
   This concept is related to the idea of managed trust but is specific to internal PNT sources that can generate PNT information from physical measurements. Internal physical PNT sources include local clocks, such as rubidium or cesium atomic clocks, that provide relative time and different types of inertial sensors that provide relative positioning information. The PNT solutions from physical PNT sources are inherently more trustworthy because they are generated without external influence. Isolation of internal PNT sources should be preserved to protect them from attacks and maintain trustworthiness.

Some PNT UE systems overcome drift in physical PNT sources by directly steering or disciplining with reference to a PNT source that receives external input. However, any external influence, including disciplining to verified external input, would reduce the protection around the internal PNT source. Although limits can be used to reduce times necessary for disciplining, it is more secure to isolate internal physical sources completely from external influence and allow them to free-run without disciplining. The PNT UE system can apply corrections to drifting PNT solutions as part of the process to build the system PNT solution from a combination of PNT state information from different sources, which can include verified PNT information from sources receiving external input in addition to the output from protected internal states.

6. **Use broadly applicable threat mitigations**
   Broadly applicable threat mitigations limit or block the effects that a wide variety of threats can have on the system. When an attack affects the untrusted edge of the resilient PNT UE system, the effects can be specific to the type of PNT source that was attacked, and system designers can apply specific techniques to mitigate the threat at that point in the system. As PNT information is processed through the system layers, more universal mitigations can address the negative effects that manifest at deeper layers of defense.

   The PNT UE system design can isolate components to contain the negative effects of attacks and disruptions so that corruption does not spread between system components. When false manipulated signals are detected, a PNT UE system can use different methods to recover the true PNT signals by recognizing their unique characteristics. These methods may not be effective in all cases, so they should be used in combination with other mitigations. The PNT UE system can include diverse types of PNT sources to avoid common mode failures. When attacks target one type of PNT source or signal, or disruptions affect a particular type of PNT service, PNT information is still available from the unaffected sources.

7. **Recover when needed**
   A defense may fail or a new type of threat, issue, or malfunction could occur. The methods used to continue operating during an attack may cause performance degradation, fail to execute as intended, or be inappropriate to the specific threat. Any time threats and disruptions are able to affect the operation of the PNT UE system, a reliable recovery capability is necessary as a last line of defense to return the system to a proper working state and typical performance quality.

   In addition to recovery, PNT UE may require other resilient functions to identify when recovery is necessary, monitor when it is safe to recover, and confirm that recovery has succeeded. Methods to implement managed trust and deploy defense in depth may be needed to support these aspects of recovery.

Together, these concepts represent a holistic approach to PNT resilience because they recognize that the resilience of the whole system depends on the resilience of individual components and subsystems as well as that of the overall integrated system. When used together, the PNT resilience concepts fully cover the core functions of resilience from the CF [1]. Figure 5 shows each of the PNT resilience concepts in a row extending across the applicable core function columns. The concepts are numbered to correspond to the list above.

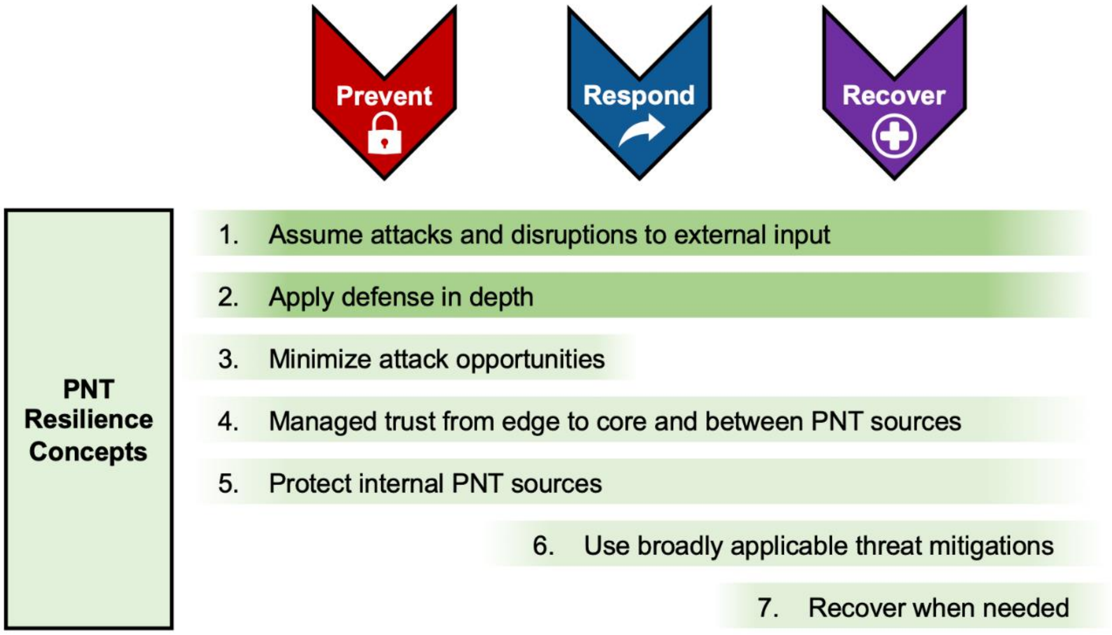

Prevent
Respond
Recover
PNT Resilience Concepts
1. Assume attacks and disruptions to external input
2. Apply defense in depth
3. Minimize attack opportunities
4. Managed trust from edge to core and between PNT sources
5. Protect internal PNT sources
6. Use broadly applicable threat mitigations
7. Recover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

Figure 5. The PNT resilience concepts cover the core functions of resilience from the CF.

The PNT resilience concepts fully cover the Prevent, Respond, and Recover core functions. The connection between the Recover concept and core function is clear. Several of the other concepts extend across multiple core functions as they can serve multiple roles in the PNT UE system. The core function that applies to the greatest extent depends on the specific resilience technique used to implement the PNT resilience concept. Figure 5 shows these connections between PNT resilience concepts and core functions:

- All three core functions describe ways to implement resilience when attacks and disruptions occur.
- Applying defense in depth involves implementing a variety of different defenses, which can include prevention, response, and recovery functions.
- Minimizing attack opportunities is one way to prevent some manipulated external input from entering or being used in the UE system.
- Managing trust from edge to core is a way to prevent corrupted information from propagating and to respond appropriately when issues are detected, which may include recovery.
- Protecting internal sources prevents them from being corrupted by untrusted external input and may be used to respond to detected issues and recover expected performance.
- Broadly applicable threat mitigations can include techniques to respond to threat detection or recover information, signals, or performance to alleviate the effects of a threat.

3.3 PNT Resilience Technique Categories

Categories can be used to group PNT resilience techniques by how they implement PNT resilience concepts. This subsection defines seven resilience technique categories: *Obfuscate* characteristics, *Limit* untrusted external input, *Verify* external input, *Isolate* components, *Mitigate* the effects of threats, *Diversify* technologies, and *Recover* performance when it is safe to do so. Figure 6 shows how the resilience technique categories implement the PNT resilience concepts from Figure 4. Most resilience technique categories can be used to implement multiple PNT resilience concepts. Further, the resilience technique categories are not mutually exclusive, so some resilience techniques may apply to multiple categories (see Appendix A.8). This categorization is intended to organize existing techniques in a way that facilitates architecture development and encourages innovation.

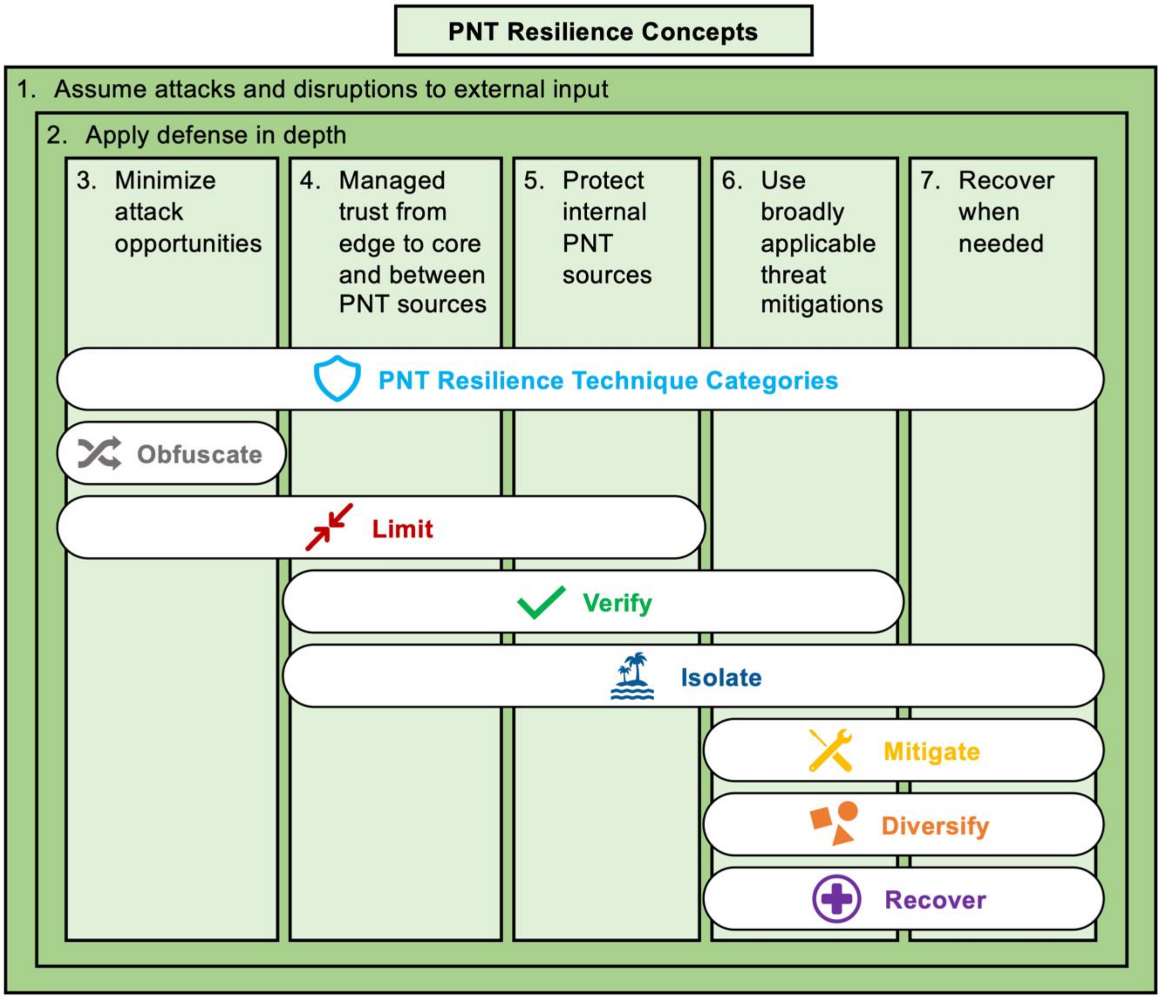

PNT Resilience Concepts
1. Assume attacks and disruptions to external input
2. Apply defense in depth
3. Minimize attack opportunities
4. Managed trust from edge to core and between PNT sources
5. Protect internal PNT sources
6. Use broadly applicable threat mitigations
7. Recover when needed
PNT Resilience Technique Categories
Obfuscate
Limit
Verify
Isolate
Mitigate
Diversify
Recover

Figure 6. PNT resilience technique categories related to PNT resilience concepts. The PNT resilience technique categories are indicated by white bars with colored text and the PNT resilience concepts are in green boxes. The first two PNT resilience concepts in dark green boxes overlap with all other PNT resilience concepts and PNT resilience technique categories.

The assumption that attacks and disruptions will happen motivates all categories of PNT resilience techniques. To prepare for attacks that penetrate outer defense layers, resilient PNT UE systems should apply the defense in depth concept to incorporate resilience at all levels throughout the system with a variety of complementary techniques. Figure 10 in Section 4.4 provides one architecture instance example demonstrating how a PNT UE system can utilize resilience techniques from each of the seven categories to meet the requirements for Level 3 or 4 resilience, as defined in Section 2.3.

The list below describes the resilience technique categories and connects them to the PNT resilience concepts from Section 3.2. Appendix A provides lists of specific examples for each resilience technique category.

Resilience Technique Categories

1. ***Obfuscate* characteristics to confuse attackers.** *(See Appendix A.1)*

   This category contains different methods to conceal or disguise attack surfaces to minimize attack opportunities. Interfaces where external input is brought into the system are common attack surfaces. Some *Obfuscate* techniques hide or disguise system input components such as antennas or other input hardware from potential attackers. Spoofers can use location information to tailor their attacks to a particular target, so hiding target locations can reduce the effectiveness of attacks. PNT UE systems can also take advantage of PNT signals that are fully or partially encrypted to hide content and enable authentication methods.

2. ***Limit* external input to minimize attack opportunities.** *(See Appendix A.2)*

   Attack opportunities can be minimized by limiting both the external input admitted to the system and limiting the use of external input within the PNT UE system. Both methods of limiting can be part of a managed trust architecture because they are ways to control external input at the outer boundary of the PNT UE system.

   The interface where external input is received at the untrusted edge of the system is an attack surface that can be minimized using different methods to control the external input accepted by the PNT UE system based on its characteristics. Resilience techniques can use filters to limit the allowed frequency intake and beamforming methods to constrain the direction of received incoming signals.

   While it may not be possible to eliminate the dependence on external inputs in a PNT UE system, limiting exposure to these attack surfaces is one way to reduce the impact of attacks. For example, a PNT UE system can be designed with a free-running internal sensor as the primary PNT source and the duration of exposure to external input can be regulated by only using occasional disciplining from verified external input.

3. ***Verify* external input for managed trust.** *(See Appendix A.3)*

   The PNT UE system can employ different verification methods to evaluate integrity and determine which PNT information is acceptable to apply towards the system PNT solution. Verification includes methods to monitor for the effects of manipulation or interference, which may be due to intentional attacks or inadvertent events. Detection methods called anti-jam and anti-spoof algorithms fall into this category.

   Threat and anomaly detection can range from simple consistency monitors to searching for more complex characteristics that can emerge during signal processing, as well as techniques to authenticate information. Techniques to compare PNT information across output from different PNT sources can identify outliers that may be manipulated or degraded beyond acceptable limits.

   In a managed trust architecture, untrusted external input should be confirmed using different techniques from the Verify category before it is allowed to contribute to the system PNT solution or steer protected internal physical PNT sources. To produce resilient outcomes, verification techniques should be implemented together with resilience techniques from other categories to provide appropriate responses when threats and disruptions are detected. However, system designers must recognize that even verified external input carries some risk of manipulation. Resilience techniques that do not depend on detection can be implemented to mitigate the risk that manipulated PNT information from coordinated threats may slip through undetected.

4. ***Isolate* components to protect from external influence.** *(See Appendix A.4)*
   Isolating components from each other implements managed trust by preventing untrusted information from spreading. This broadly applicable threat mitigation limits damage from spreading through the PNT UE system, whether it is due to threats or other sources of system faults and failures. When PNT sources are isolated from each other, threats that target one PNT source cannot affect the other sources. When one PNT source is compromised, the UE system can use the remaining sources to form the system PNT solution, allowing the system to operate through the threat.

   It is especially important to isolate internal physical sources from untrusted external input to protect them and maintain their integrity. Internal physical PNT sources include local clocks and INS, which do not require external input to produce PNT information. For example, if a GNSS receiver or other PNT source that accepts external input is used to steer or discipline the behavior of an inernal PNT source (such as a local clock or INS), the PNT state information from the internal PNT source may be corrupted if the external input is manipulated. To prevent this from happening, steering or disciplining should be limited, and the UE should verify PNT information from external input before using it. The strictest protection for internal physical PNT sources is to isolate them from all steering or disciplining and allow them to free run indefinitely. To remedy drift, the UE can apply corrections when the system PNT solution is formed.

   Techniques to isolate internal PNT sources can effectively mitigate a broad range of threats and limit their impacts when they penetrate system defenses. However, these techniques can also greatly increase PNT UE system complexity by requiring additional capabilities to apply corrections and synthesize the system PNT solution while maintaining protection of the internal PNT sources.

5. ***Mitigate* the effects of threats.** *(See Appendix A.5)*
   This category includes techniques to reduce or correct the effects of threats despite an ongoing attack. One type of mitigation would be to attempt to recover true signals that are lost by searching for specific characteristics of the expected signals.

   This category overlaps considerably with techniques in the Verify, Isolate, and Diversify categories, since one way to mitigate an attack that affects one PNT source is to have additional PNT sources providing information for the system PNT solution. In order to successfully implement this broadly applicable threat mitigation, the PNT UE system first would need to detect the effects of the threat on the targeted PNT source, using a technique from the Verify category. The PNT UE system must also have multiple diverse PNT sources to avoid common mode failures. Finally, the PNT UE system would need an architecture that isolates the PNT sources from each other to contain effects caused by threats and prevent cross-contamination between PNT sources when one source is attacked. This approach can build resilience that will be effective against existing as well as new and emergent threats.

6. ***Diversify* technologies to reduce common mode failures.** *(See Appendix A.6)*

   Different types of PNT sources are susceptible to different types of threats and vulnerabilities. Including diverse types of PNT sources and layers of complementary resilience techniques from different categories will enable a resilient PNT UE system to withstand a variety of threats and avoid common mode failures.

   Incorporating diversity throughout the PNT UE system design is a broadly applicable threat mitigation because it enables avoiding common mode failures. For example, when threats target one type of PNT source or PNT service, the PNT UE system can rely on different PNT sources that are not affected by the same attack or disruption. This includes isolated internal PNT sources or other types of PNT sources that receive external input different from the signals under attack. When it is appropriate and safe, the compromised PNT source can be recovered while the other PNT sources allow the continued operation of the PNT UE. Diversity can also include signal diversity from within a PNT service or PNT source type, such as GPS signal diversity from multiple civil bands, multi-GNSS receivers, or multiple GNSS antenna locations.

   In general, these different types of system diversity can increase the complexity and coordination required to launch a successful attack. However, incorporating diverse technology types also increases the complexity of the PNT UE system, since each additional technology requires sufficient development and integration. Each additional PNT source introduces new attack surfaces, requiring complementary defense measures.

7. ***Recover* performance when it is safe to do so.** *(See Appendix A.7)*

   Techniques to recover PNT UE system performance ensure that the system can be returned to a proper working state with typical performance after a threat or disruption has affected the system. Since there are different types of attacks and disruptions, and some may penetrate to different layers of defense, recovery can take a variety of forms. This includes techniques to reset, reload, roll back, reacquire, or restart different elements as needed. Recovery techniques may be used during or after an attack or disruption.

   System performance can be recovered while a threat is present using different resilience techniques, such as mitigating the effects of threats or switching to different PNT sources when threats and disruptions are detected. Different performance parameters may be relevant to defining a good working state for different PNT applications. Relevant performance parameters may include accuracy, availability, integrity, continuity, and/or coverage. Successful recovery of overall system performance is defined by the relevant parameters for the application needs.

   Different techniques for recovery apply to the different aspects of PNT UE systems that may have to be recovered. Individual components can be recovered without requiring full system recovery. Automatic component recovery can be implemented if resilient PNT UE systems have the ability to determine when recovery is safe to initiate. All resilient PNT UE should be capable of full system recovery after the threat or disruption is over.

The last line of defense is manual full system recovery that is initiated by the user based on their situational awareness.

4.0 GRADUATED RESILIENCE LEVEL ARCHITECTURE EXAMPLES

The PNT resilience concepts from Section 3.2 can be implemented using the PNT resilience techniques from the seven categories defined in Section 3.3 to build complete PNT UE system architectures. With a holistic approach, not only which PNT resilience techniques are added, but how the system is integrated affects the overall resilience. This section describes example PNT UE system architecture instances demonstrating each of the resilience levels defined in the CF [1]. Each level of resilience cumulatively builds upon the requirements from the preceding levels and improves on the overall performance capabilities in the presence of threats. In the examples, resilience techniques are added and the architectures are arranged to achieve the required behavior at each level. The evaluated resilience level of any PNT UE implementation depends on the demonstrated overall system performance in the presence of a threat. Specific examples show how different PNT resilience techniques can be integrated using a holistic approach to achieve overall resilient outcomes.

This section includes three subsections and connects to later sections as follows:

- **Section 4.1** starts with a non-resilient, **Level 0** PNT UE timing system example.
- **Section 4.2** provides a **Level 1** resilient PNT UE timing architecture example building from the example in Section 4.1.
- **Section 4.3** provides a **Level 2** resilient PNT UE timing architecture example building from the example in Section 4.2.
- **Section 4.4** provides a **Level 3** or **Level 4** resilient PNT UE timing architecture example building from the example in Section 4.3.
- **Section 4.5** closes with a conceptual framework comprising three subsystems to address the overall objectives of a resilient PNT UE system.
- **Section 5.0** further describes the three subsystems introduced in Section 4.5 and explores their role in meeting the objectives of next generation PNT UE systems.
- **Section 5.3** specifically includes position and navigation system examples from the literature to supplement the timing-only examples provided in this section.

These examples show one way to build resilience within a PNT UE timing system, but other architectures can also achieve resilient outcomes. The guidance provided in this RA can be used to develop different types of resilient PNT UE systems. System designers should not use the examples in this document to constrain how they develop other innovative PNT UE systems.

4.1 Level 0 Non-Resilient Architecture Instance

As a reference, the first example architecture instance given in Figure 7 is a non-resilient GPS receiver providing the system PNT solution to the user. Since this example is for a timing application, the PNT UE system only provides time as the system PNT solution. The GPS receiver may be a GPS chipset or an integrated GPS receiver with no internal resilience functions. Note that while this GPS receiver PNT source depends on the external GPS signal, other external input types are possible, including other types of radiated signals or time over fiber. Appendix C includes a description of different types of PNT sources.

This user equipment is Level 0 because it is essentially an open port, taking in all radio frequency (RF) signals to which it is sensitive and processes them without scrutiny. This example serves as a starting point for showing how to build from no resilience through different grades of resilience and ultimately achieve a system architecture capable of high resilience.

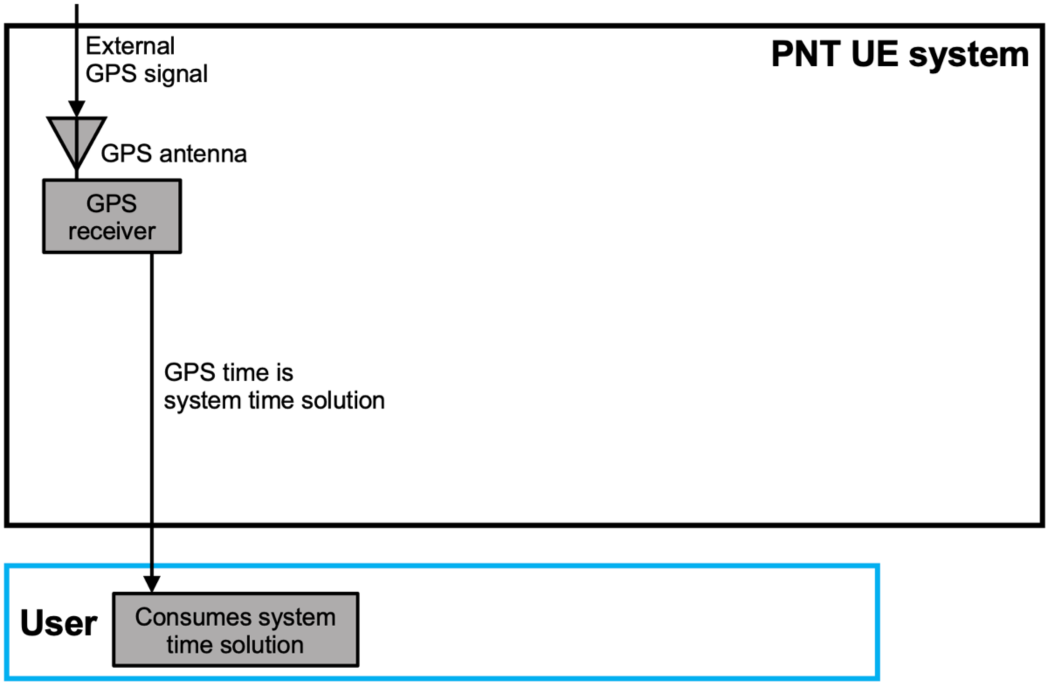


Figure 7. Level 0 timing UE system example architecture.

4.2 Level 1 Resilient Architecture Instance

Level 1 resilience focuses on PNT UE system recovery after a threat or disruption is over, setting the foundation for all remaining resilience levels. It also includes basic verification steps to confirm external inputs adhere to established standards. Figure 8 depicts an example architecture instance. System components added to achieve Level 1 resilience are highlighted in purple.

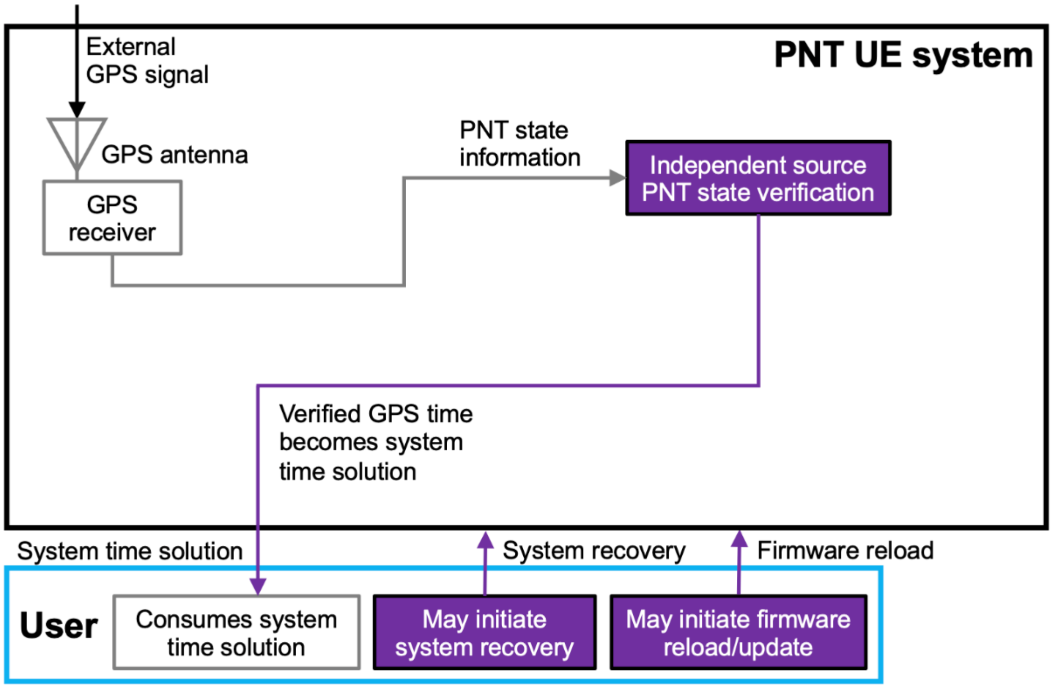


Figure 8. Level 1 timing UE system example architecture.

Instead of passing the system PNT solution directly from the GPS receiver to the user, the Level 1 example architecture instance adds an intermediate verification step to Level 0. The PNT state information passed from the GPS receiver to the verification step includes the PNT solution (time in this case) and any information stored to memory, because Level 1 requires checking stored data from external inputs against the appropriate established standards. An example would be GPS navigation message information, including variables ranging from the week number to satellite ephemeris and almanac information, which can be verified against the standard message formats given in the GPS Interface Specification document (IS-GPS-200M) [16].

The PNT state information can also use position, velocity, and other internal observables as verification resources. For example, if the timing system is known to be stationary, a simple verification would be checking that the position maintains the same location over time using a Stationary Position Monitor algorithm. Other internal observables may include different types of signal measurements such as power, carrier amplitude, beat carrier phase, or code phase. The PNT UE systems may have to incorporate verification algorithms using these additional observables or correlator outputs to meet the requirements to identify and respond to compromised PNT sources and corrupted data at higher levels of resilience.

Level 1 PNT UE systems are not required to continue providing a system PNT solution when a threat is present. However, a Level 1 PNT UE system should at a minimum be able to recover to a proper working state, or typical performance, after the threat or disruption is over. Recovery includes the ability to reset or roll back information stored to memory and the ability to reload or update firmware. At Level 1, users can manually initiate system recovery because they may have to force recovery when the system cannot function correctly. System designers can add other types of recovery as they build more capabilities into the timing UE system. The User box in the Level 1 diagram in Figure 8 shows recovery functions because they are initiated by the user.

The interaction of the user with the PNT UE system is important to achieve resilient outcomes. The user must receive appropriate training to understand the system PNT solution and typical performance characteristics to expect. To know when to trust the system PNT solution and when to initiate recovery functions the user needs timely and accurate information on which to base decisions. The necessary information may include SA about threats or PNT assurance metrics. The PNT UE system or other PNT devices to which the user has access can provide this information.

4.3 Level 2 Resilient Architecture Instance

Level 2 resilience requires the PNT UE system to minimally withstand a threat or disruption by continuing to operate with degraded system performance. At Level 2, the performance degradation can be unbounded in the presence of a threat or disruption, which means it could potentially increase indefinitely. The requirements for Level 2 imply a need for at least two PNT sources so the system can continue to operate if one source is compromised. A protected local source can allow the system to operate in a holdover state, without input from compromised PNT sources, until the threat is over. In addition to all the capabilities from Level 1, a Level 2 system responds to threat detection by temporarily isolating compromised PNT sources from the system PNT solution and initiating their automatic recovery. Figure 9 depicts an example architecture instance, with blocks added to achieve Level 2 behavior shown in green.

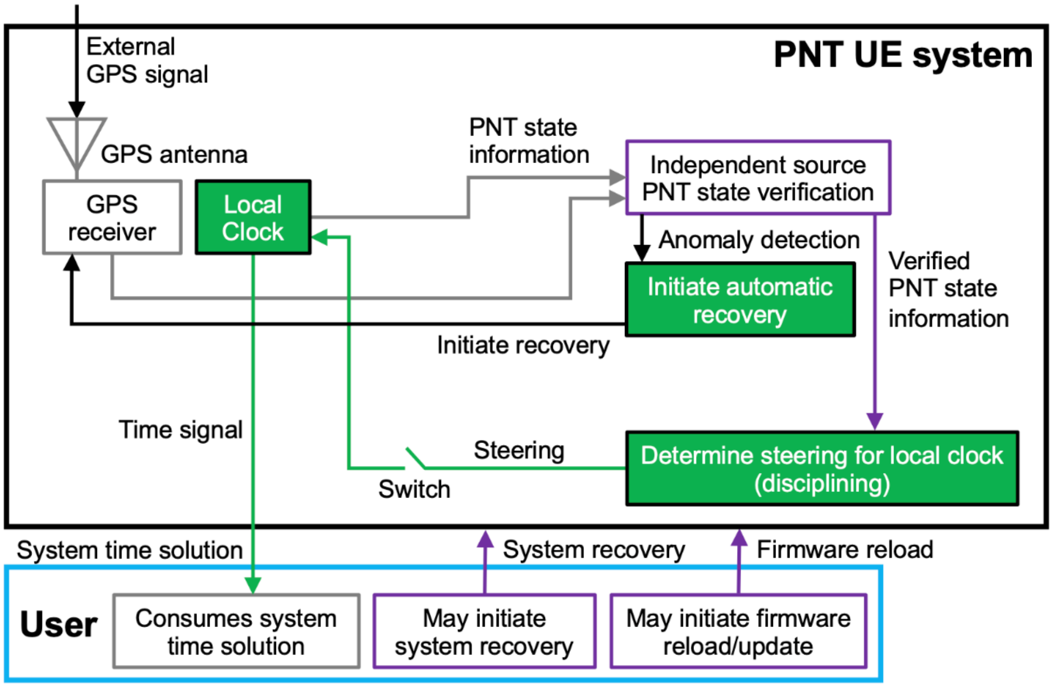

PNT UE system
External GPS signal
GPS antenna
GPS receiver
Local Clock
PNT state information
Independent source PNT state verification
Anomaly detection
Initiate automatic recovery
Verified PNT state information
Initiate recovery
Time signal
Steering
Switch
Determine steering for local clock (disciplining)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

Figure 9. Level 2 timing UE system example architecture.

Since GPS receivers inherently rely on external GPS signals to generate PNT information, a PNT source that does not rely on external input can be used while the GPS receiver is compromised. For example, in the timing UE system in Figure 9, a local clock provides a trusted internal PNT source that provides PNT state information with high intrinsic integrity. When the verification step detects an atypical error in the PNT state information coming out of the GPS receiver, the switch in Figure 9 can be opened to cut off disciplining and protect the local clock from compromised external input. The local clock can free run while the device remains in holdover mode. The verification step continues to monitor the PNT information from the GPS receiver and internal logic can automatically initiate GPS receiver recovery when the monitoring indicates the attack or disruption is over. This ensures the system recovers GPS as soon as possible, without needing the attention of the user. A limitation of this feature is that it must be carefully calibrated to avoid triggering frequent unnecessary recovery sequences due to false positive error detections. When the threat or disruption is over, the switch can be closed, and the local clock can return to disciplining from the GPS receiver.

Alternatively, the PNT UE system can treat the local clock as the primary timing source and the GPS receiver as the secondary source. With this approach, the clock provides a trusted internal state with good short-term stability, which is isolated and allowed to free run as the default. The UE only uses the GPS timing solution to discipline, or steer, the local clock as necessary to maintain the accuracy required by the application of the timing UE. This allows the system time solution to take advantage of the long-term stability of GPS without constantly disciplining the local clock. Limiting the duration when the external input can influence the local clock through GPS disciplining reduces the attack surface of the UE. Variations of the disciplining period, rate, and regularity can be adopted according to the performance needs of the UE application. In some cases, a threat may be able to predict when the local clock is periodically disciplined by the GPS receiver and corrupt or disrupt the external GPS signal when it is being used. To further protect the local clock, the disciplining schedule can be obfuscated by randomizing the durations of the disciplining and free-running intervals.

The resilience techniques included in the Level 2 timing architecture instance in Figure 9 work together to produce overall resilient outcomes. The PNT state information from the GPS receiver is verified before it is used to discipline the local clock, but it is possible for the verification step to fail, so additional techniques that do not rely on the success of the verification step are needed. Limiting the use of external input and obscuring its disciplining schedule are both effective methods that minimize attack surfaces even when verification fails.

Note that a threat may attack the GPS signal for an extended period, beyond the maximum duration the system can maintain the required accuracy without disciplining the clock. In this case, the local clock should be allowed to free run as long as the verification step identifies issues with the GPS receiver, even if it drifts outside the nominal accuracy performance bounds for the PNT UE system. Different types of clocks will have different stability and drift characteristics, so it is important to select a suitable local clock to meet the application's performance requirements and other size, weight, power, and cost (SWAP-C) constraints. Unbounded performance degradation in the presence of a threat is allowed for Level 2 systems. Higher levels of resilience, with bounded degradation or no degradation, require improved isolation of the local clock and additional alternative PNT sources that receive external input to verify and use when GPS is not available.

4.4 Higher Level Resilient Architecture

Higher levels of resiliency, Levels 3 and 4, may have to include additional hardware or rigorous software assurance practices to sufficiently isolate PNT sources from each other. Three or more

PNT sources are necessary to implement the cross-verification required for Level 3 and to prevent local PNT sources from losing verified external input during PNT service attacks and disruptions. Level 4 explicitly requires diverse types of PNT sources that do not share common failure modes. An example architecture instance incorporating all these requirements is shown in Figure 10, where additions to meet the requirements for Level 3 are red and additions for Level 4 are blue. However, note that the numbered requirements are only minimally different for Levels 3 and 4. Most of the differences between these higher levels come from the overall performance requirement: Level 4 demonstrates no performance degradation in the presence of a threat or disruption, whereas Level 3 may have bounded degradation.

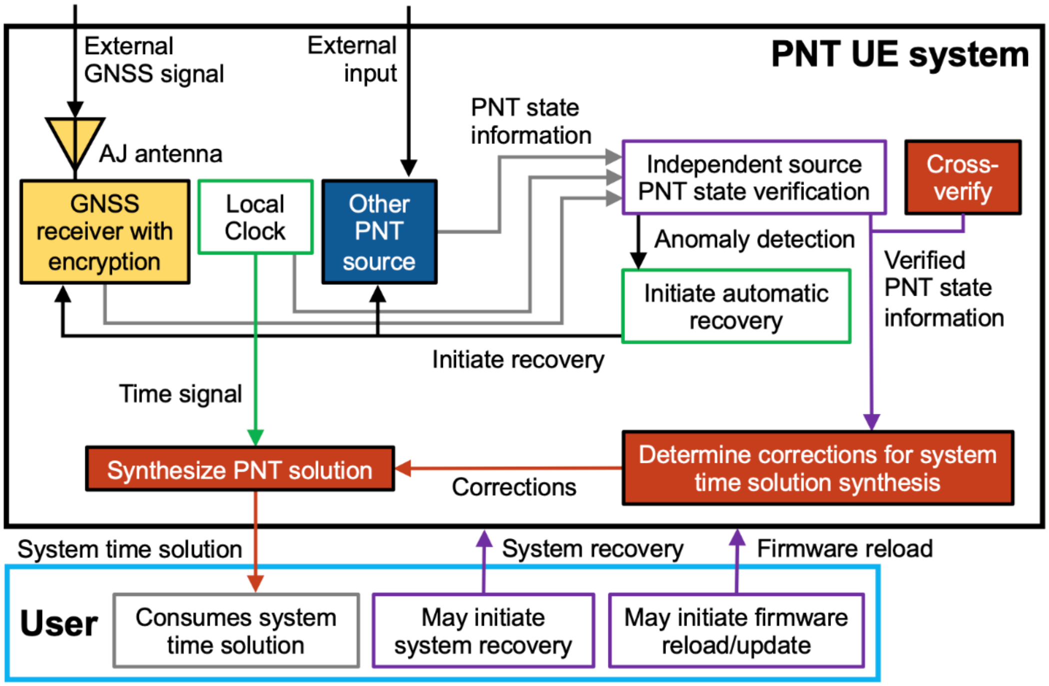

External GNSS signal
External input
PNT UE system
PNT state information
AJ antenna
Independent source PNT state verification
Cross-verify
GNSS receiver with encryption
Local Clock
Other PNT source
Anomaly detection
Verified PNT state information
Initiate automatic recovery
Initiate recovery
Time signal
Synthesize PNT solution
Corrections
Determine corrections for system time solution synthesis
System time solution
System recovery
Firmware reload
User
Consumes system time solution
May initiate system recovery
May initiate firmware reload/update

Figure 10. Level 3 or 4 timing UE system example architecture instance.

In the Level 2 example, the system design placed limits on the time during which external input could influence the internal clock through the disciplining from GPS. Instead of merely limiting the influence of external input, the internal clock can be permanently isolated from the GPS receiver. Adding a synthesizer responsible for forming the system time solution provided to the user achieves this isolation in the Figure 10 example. For a timing UE system, the synthesizer could be a signal generator that is driven by the local clock, as depicted in Figure 10. To obtain the long-term stability benefits of GNSS timing, an algorithm calculates and applies corrections in the form of programmed modifications [17]. Any PNT state information that does not pass the Verification step is ignored when the algorithm calculates the corrections. This arrangement can adapt to changes quickly, including the ability to roll back previous corrections if GPS or other PNT sources are found to be compromised and recent integrity may be uncertain. Preventing PNT information from compromised PNT sources from contributing to the system PNT solution is one way to mitigate the effects of threats and continue providing a system PNT solution to the user.

Increasing the number of PNT sources to include diverse technology types reduces common mode failures. This step can make the system stronger and enable it to withstand disruptions to one PNT source with low or no impact on the performance of the system time solution. Further, with at least three sources of time, PNT UE systems can use cross-verification between sources as an additional check after verifying the PNT state information from each source independently. However, it is important to note that each additional different timing source introduces unique verification challenges, new attack surfaces, and new failure modes. Though this approach generally avoids common mode failures, it introduces new types of issues. Higher resilience comes at the cost of increased complexity. The PNT information from the diverse sources must also be combined into one system PNT solution in a way that considers the different performance capabilities and current verification status of the PNT sources.

To prevent false signals from entering the PNT UE system in the first place, the design can include an anti-jam antenna on the front of the GPS receiver, as shown highlighted in yellow the example in Figure 10. This antenna limits the frequency and direction from which the system will accept incoming signals. The receiver can be further protected from targeted spoofing by consuming messages in PNT signals that are obscured from potential attackers using encryption. For example, PNT UE systems can include GNSS receivers that can utilize available civilian encrypted messages. With Navigation Message Authentication (NMA), the encrypted messages can be authenticated with a key (which is broadcast after some delay) [18].

Given the concept of defense in depth, system designers should not assume that preventive measures suffice on their own. A false signal may still get through defenses, or another type of disruption may occur. An anti-jam antenna is a useful, resilient addition to the system, but it cannot by itself guarantee a high level of resilience. In Figure 10 both the anti-jam antenna and GNSS receiver using encrypted signals were colored yellow because they are not representative of any of the requirements for the different levels of resilience listed in Table 1. However, these elements may be part of an overall design that achieves the performance requirements for one of the levels. Each of the resilience techniques included in the example timing system design work together to provide durable, layered PNT resilience.

In summary, this example architecture instance of a resilient timing UE system incorporates seven categories of resilience techniques:

Obfuscate characteristics to confuse attackers

Example: Use a GNSS receiver that can consume obscured encrypted messages in supported civilian PNT signals. One example would be a GNSS receiver with NMA capabilities.

Limit external input to minimize attack opportunities

Example: An anti-jam antenna prevents the system from processing false signals by limiting the frequency and direction of accepted input.

Verify external input for managed trust

Example: Verify the PNT state information to determine when to use different PNT sources in generating the system time solution. One algorithm for a timing UE system in a static location would be a Stationary Position Monitor.

Isolate components to protect from external influence

Example: Isolate the local clock to make it a protected internal state with no connection to external input.

Mitigate the effects of threats

Example: Mitigate the effects of threats that penetrate the system by eliminating PNT information obtained from compromised PNT sources from the combined system PNT solution.

Diversify technologies to reduce common mode failures

Example: Use multiple different PNT sources with diverse technology to prevent common mode failures.

Recover performance when it is safe to do so

Example: Implement automatic recovery to return to a proper working state as soon as it is safe to do so and maintain the option for manual system recovery when needed.

Appendix A lists many examples of resilience techniques that fit into these seven categories.

4.5 Resilient PNT UE Subsystems

Generalizing the component functions of the system architecture instances in Sections 4.2-4.4 reveals three types of components: PNT sources, resilience functions, and PNT solution synthesis elements. Figure 11 shows how the components from Figure 10 are assigned to these three groups. The components included in each group may differ for each of the different level examples from Sections 4.2-4.4. The Level 1 architecture instance from Section 4.2 would only include one PNT source, the GPS receiver. There may be very few components involved in producing the system PNT solution in lower level PNT UE systems that do not synthesize the system PNT solution using input from multiple PNT sources. For the Level 1 architecture instances from Section 4.2 the PNT solution synthesis component may simply be a formatting step applied to convert a source PNT solution to the system PNT solution (not pictured in the diagrams). For the Level 2 architecture instance in Section 4.3 the steering calculation for the disciplining step may be considered part of the PNT solution synthesis, but a resilience function would make decisions about when to turn disciplining on or off.

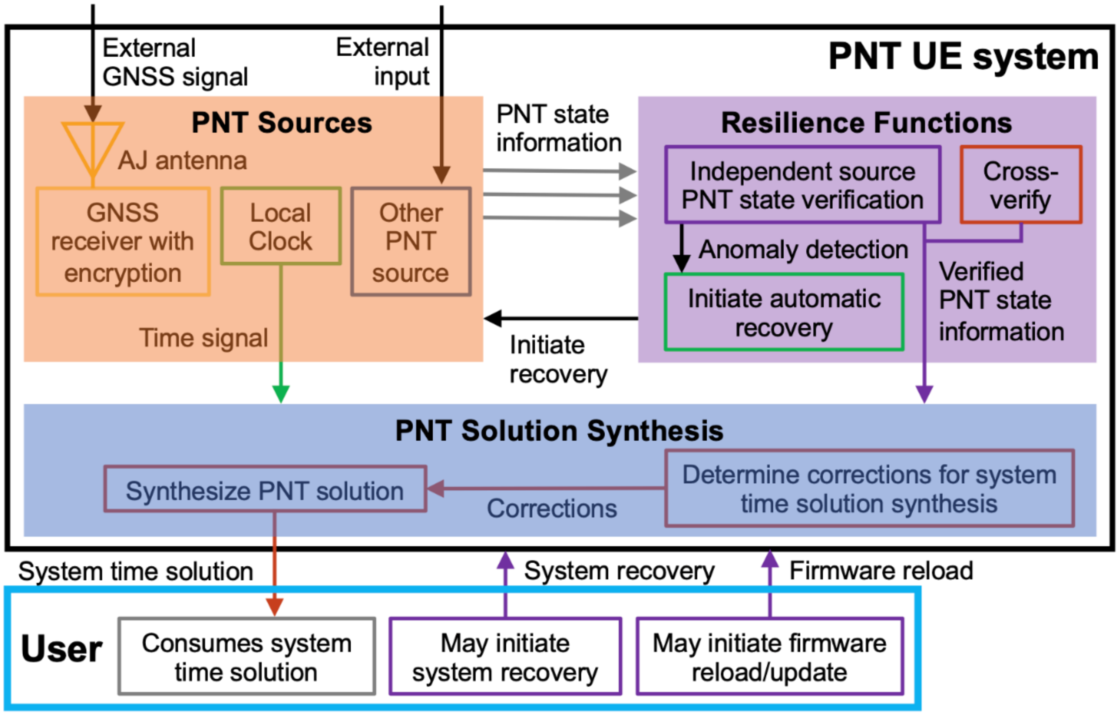


Figure 11. Types of components in a resilient PNT UE system.

The functions of the three types of components can be further generalized to identify three main subsystems of a conceptual PNT UE system architecture:

- **The PNT Source Controller** organizes the input and output from multiple, diverse PNT sources. This includes controlling the external input interfaces and handling the PNT state information from the PNT sources, which comprises PNT solutions and other collected observables and measurements.
- **The Resilience Manager** implements resilient functions, including PNT source recovery. Using different complementary resilience techniques, the Resilience Manager determines which PNT sources should be allowed to contribute PNT state information to the system PNT solution and when it is appropriate to implement mitigations or automatic recovery.
- **The PNT Solution Synthesis Agent** produces the final system PNT solution output to the user. With input from the Resilience Manager, the PNT Solution Synthesis Agent combines the trusted PNT state information from the different PNT sources to form the system PNT solution. As part of this process, the subsystem can apply corrections to drifting PNT state information from physical PNT sources that were isolated to protect them from external influence.

These generalized PNT UE Subsystems can be implemented in very different physical architectures. For example, the GNSS receiver may very tightly integrate some GNSS anti-spoof techniques from the Verify resilience technique category with internal signal processing steps. Although the GNSS receiver hardware may implement these techniques, they can still be considered part of the logical functions satisfying the Resilience Manager objectives.

Figure 12 demonstrates the high-level functionality of the three subsystems and the inherent isolation of system components that is achieved by partitioning resilient PNT UE in this manner. Each subsystem performs its objectives and, to the extent possible, provides a barrier between components to prevent corrupted or untrustworthy data from propagating through the system. Partitioning into subsystems can be one aspect of implementing managed trust architectures by isolating components and subsystems. The subsystem viewpoint is presented here as a suggested implementation of resilient PNT UE and is not meant to constrain the possible resilient PNT UE architectures that system designers can develop.

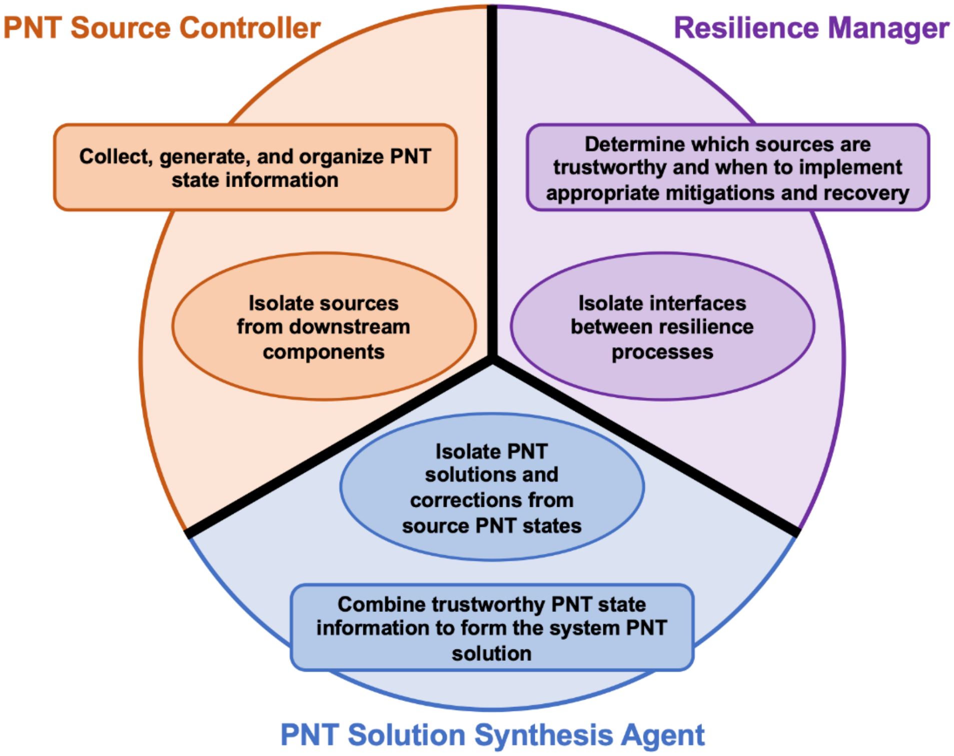

PNT Source Controller
Resilience Manager
Collect, generate, and organize PNT state information
Determine which sources are trustworthy and when to implement appropriate mitigations and recovery
Isolate sources from downstream components
Isolate interfaces between resilience processes
Isolate PNT solutions and corrections from source PNT states
Combine trustworthy PNT state information to form the system PNT solution
PNT Solution Synthesis Agent

Figure 12. PNT UE architecture functions can be partitioned into subsystems to enable isolation.

5.0 INTEGRATION OF RESILIENCE INTO COMPLETE PNT UE SYSTEMS

Resilient PNT UE systems use different combinations of resilience techniques to withstand and recover from threats and other types of disruptions. Section 3.3 introduced seven categories of resilience techniques; Appendix A describes them in more detail, with specific examples. This section further explores the composition of resilient PNT UE systems and includes a detailed discussion of the purpose of each of the three PNT UE Subsystems described in Section 4.5. Figure 13 shows the PNT UE Subsystems overlaid on the conceptual representation of trust from Figure 4 in Section 3.2, which depicted PNT resilience concepts.

The roles of the PNT UE Subsystems related to trust concepts are:

- **The PNT Source Controller** organizes the input and output from multiple, diverse PNT sources. Some PNT sources receive untrusted external input from different signals and services and occupy the untrusted edge of the device. In the protected trusted core, internal PNT sources that do not directly receive external input use physics-based sensors to provide PNT information.

- **The Resilience Manager** implements resilient functions. It brings external input from the untrusted edge to the trusted core through different techniques to build trustworthiness. It identifies untrustworthy PNT information and prevents it from propagating to the trusted core. It also executes mitigation and recovery processes when appropriate.

- **The PNT Solution Synthesis Agent** produces the final system PNT solution. It uses only PNT state information that is accepted into the trusted core to synthesize the system PNT solution made available to the user. Combining PNT information at this stage protects internal PNT sources from external influence.

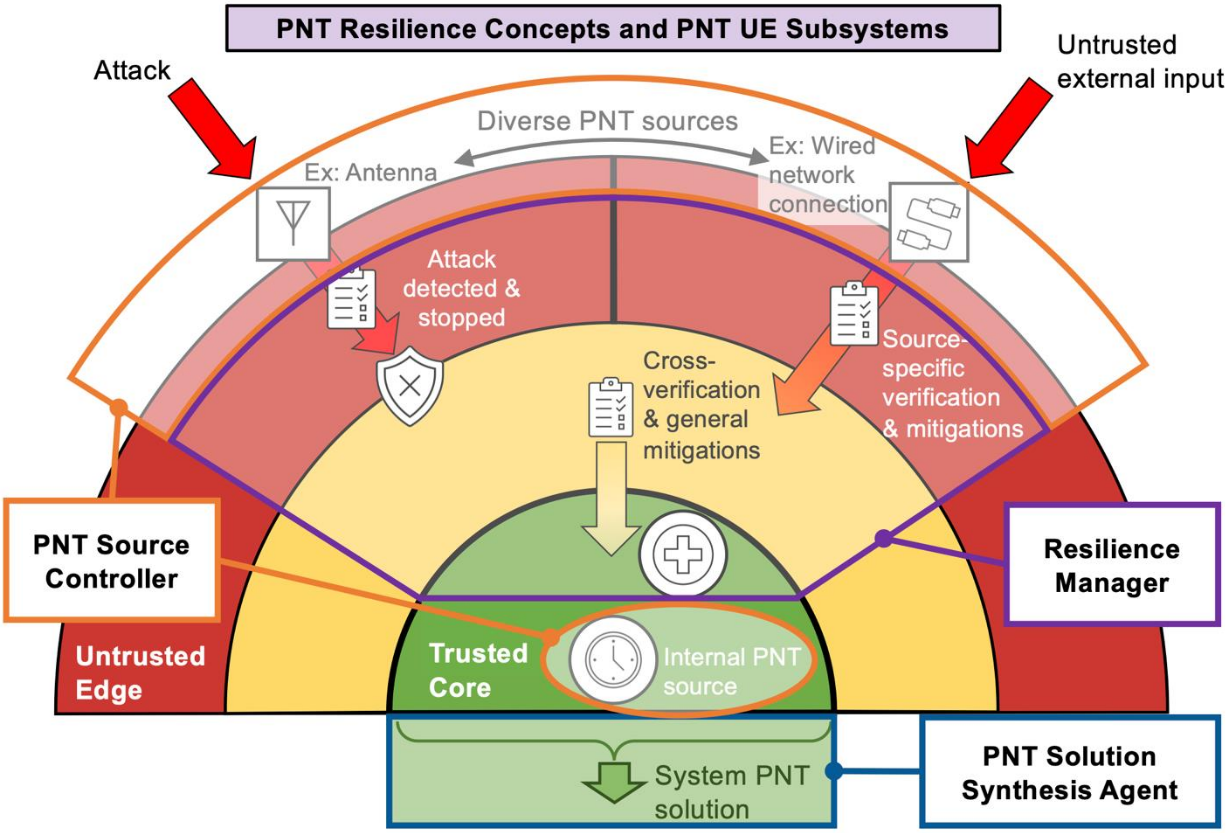

PNT Resilience Concepts and PNT UE Subsystems
Attack
Untrusted external input
Diverse PNT sources
Ex: Antenna
Ex: Wired network connection
Attack detected & stopped
Cross-verification & general mitigations
Source-specific verification & mitigations
PNT Source Controller
Resilience Manager
Untrusted Edge
Trusted Core
Internal PNT source
System PNT solution
PNT Solution Synthesis Agent

Figure 13. Conceptual representation of trust and PNT UE Subsystems.

This section gives an overview of different aspects related to developing complete resilient PNT UE systems and integrating them into the broader PNT user space. Although the concepts of resilience in this document are intended to be agnostic to the type of PNT sources used, many of the specific resilience techniques listed apply to GNSS sources due to this RA's frequent references to GNSS services.

This section includes four subsections:

- **Section 5.1** reviews different types of PNT sources that the PNT Source Controller may include, showing the breadth of options available to complement GNSS or to use as alternative PNT sources in PNT UE systems.

- **Section 5.2** further develops the role of the Resilience Manager by showing how the concept of defense in depth applies to layers of resilience within a PNT UE system.
- **Section 5.3** discusses how the PNT Solution Synthesis Agent can combine PNT state information from different PNT sources and gives examples for position and navigation applications.
- **Section 5.4** explores how resilience fits with the related objectives of PNT assurance and PNT SA in next generation PNT UE system designs.

5.1 PNT Source Controller: Using Diverse PNT Technology

GNSS services provide highly accurate, globally available PNT solutions to any user in possession of the GNSS receivers required to access the service. Due to the widespread use of GNSS receivers and publicly available GNSS signal information, GNSS services are targets of attacks designed to deny or manipulate PNT information. Many of the resilience technique examples in this RA are specific to GNSS receivers because organizations have devoted considerable effort to develop detection and mitigation methods for GNSS threats. PNT UE systems can use other PNT sources in place of GNSS receivers or as a backup when GNSS signals are disrupted or assessed as having low integrity.

PNT UE system designers can use diverse PNT source technologies to produce PNT solutions. Supplementing GNSS receivers with other PNT sources can yield more accurate PNT solutions. By providing diverse options, different PNT sources may also allow PNT UE systems to circumvent threats specific to a particular PNT service or type of PNT technology. However, given the assumption that all PNT services can and will be attacked, users must manage the trustworthiness of all PNT sources by applying appropriate resilience techniques to produce an overall resilient PNT UE system. To use them as a backup to withstand GNSS threats, system designers must consider the performance quality of the alternative PNT sources when incorporating them into a PNT UE system, including their accuracy, availability, stability, continuity, coverage, and integrity. Further, PNT UE system designers must consider the source-specific threats and other vulnerabilities of all PNT sources and include appropriate verification, obfuscation, mitigation, and recovery techniques for each new PNT source that accepts external input. The system architecture should protect any additional local, physical PNT sources by limiting interactions or by completely isolating them from PNT sources with access to external input.

Considerations for selecting and incorporating PNT sources in PNT UE systems

- What are the required **performance parameters** for *accuracy, availability, stability, continuity, coverage,* and *integrity* for the PNT source to execute its role within the PNT UE system?
- Which **PNT resilience techniques** from the *Obfuscate, Limit, Verify, Isolate, Mitigate, Diversify*, and *Recover* categories will be used to defend each PNT source from different types of threats and disruptions?
- How will the *holistic approach* be implemented to integrate the selected PNT source and PNT resilience techniques in the **PNT UE system architecture** and produce overall resilient behavior?

Different types of PNT sources can share or measure PNT information using internal physics-based sensors, external RF signals, optical systems, cables linked to a network, or different types of reflected signals for radar, LiDAR, or sonar systems. Manufactured external RF signals other than GNSS might include navigational signals from stationary terrestrial beacon navigation and timing systems, signals of opportunity originating from 802.11 Wi-Fi routers, or signals from Low Earth Orbit (LEO) satellites. Optical systems may utilize fixed landmarks such as constellations to determine absolute position or estimate the trajectory of an object in motion relative to some starting position. Other naturally occurring physical phenomena can also be input for PNT sources, such as magnetometers sensing crustal variations in the earth's magnetic field. Internal PNT sources include INS and local clocks. Methods to distribute Universal Coordinated Time (UTC) are described in *NIST Technical Note 2187: A Resilient Architecture for the Realization and Distribution of Coordinated Universal Time to Critical Infrastructure Systems in the United States,* include network architectures and protocols [19]. Many other sources in the literature [20] [21] [22] [23] review different kinds of complementary PNT. Appendix C provides a categorization of different types of PNT sources.

Commercial airplanes represent a specific application using many different kinds of navigation aids in addition to GNSS receivers and INS instrumentation to maintain the accuracy and continuity required for different airspaces. Ground-based transmitters include Nondirectional Radio Beacons (NDBs) and VHF Omni−directional Ranges (VORs). Some navigation aids require signals transmitted by the aircraft, including Distance Measuring Equipment (DME) and Doppler radars [24].

Simply adding multiple different types of PNT sources to the PNT UE system does not automatically increase the resilience of the system. System designs should handle each PNT source in a resilient manner to avoid introducing new vulnerabilities to the system.

5.2 Resilience Manager: Applying Defense in Depth for Resilient PNT UE

With a holistic approach to PNT UE system design, complete system architectures should account for the interactions among the individual components to produce resilient outcomes. The defense in depth PNT resilience concept introduced in Section 3.2 incorporates all the PNT resilience technique categories because it applies to the way different techniques are combined. The concept underlying defense in depth is that layers of different complementary protection strategies, which can be implemented by different resilience techniques, will add up to produce strong and durable overall security. The example of a timing UE system architecture given in Section 4.4 includes layered verification of individual PNT sources, cross-verification between sources, synthesis of the system PNT solution while maintaining PNT source isolation, and recovery capabilities. Other system architecture instances also reflect the defense in depth concept.

To implement the defense in depth PNT resilience concept, system designers should consider different dimensions of PNT UE system design, including PNT UE system layers, available observables, and the types of potential threats and disruptions the system may face. PNT UE system layers can include input components, front ends, digital channels, different types of processing layers, synthesis components, and many other types of hardware and software [12]. Specific PNT UE observables are listed in the CF [1]. Some examples are PNT state information, stored data (such as navigation messages), or other types of internal observables from power measurements, raw signal parameters, and signal processing steps. Threats and disruptions can include anything from routine events and hazards to coordinated, targeted attacks that have not yet been demonstrated (see Appendix B for further discussion of threats and disruption types). PNT resilience techniques can be implemented throughout the PNT UE system layers, involve different observables, and defend against a variety of threats and disruptions.

Considerations for implementing defense in depth in PNT UE systems

System designers should consider the following questions when selecting complementary PNT resilience techniques to implement the defense in depth concept:

- **Performance**: What are the important performance parameters for the PNT UE system, and how can they be affected by threats and disruptions?
- **Observables**: What observables are available and how can they be used to verify authentic signals or detect the effects of threats and disruptions on the PNT UE system?
- **Timeframe**: What effects on the PNT UE system can be detected during different phases of an attack or disruption? How long do different threats and disruptions last?
- **Change rate**: Which detection techniques can identify gradual or sudden changes in PNT information and other observables?
- **System layers**: What effects can be measured when threats or other system faults and failures penetrate to each layer of the PNT sources and PNT UE system?
- **Additional features**: What supplemental information or components can be added to the PNT UE system to provide additional references or observables for authentication or detection?

Fernández-Hernández et al. [25] explore countermeasures against interference threats to aviation applications at different layers of a GNSS receiver. At the input to the receiver, anti-jam antennas can prevent spoofing signals from entering the system. Then, system designers can implement filters and Automatic Gain Control (AGC) setpoint power monitors in the front end. In the signal processing layer, the PNT UE system can use C/N_0 monitors, multi-peak monitors, vestigial signal detection, and other methods to detect spoofing and jamming. The system design can implement pulse blanking at this layer to mitigate pulse interference. Consistency checks and Navigation Message Authentication at the navigation layer further verify the external input. The platform layer performs cross-checks comparing the INS and local clock to PNT information from the GNSS receiver.

Selecting complementary resilience techniques that work well together is an important step in designing resilient PNT UE systems. Since resilient PNT UE systems should be broadly applicable to different threats, system designers should consider many different types of threats as an exercise to identify complementary detection strategies. One example would be selecting different techniques from the Verify category to defend against a spoofing attack that attempts to drag off GNSS tracking loops from a true GNSS signal. Complementary resilience techniques detect spoofing at different points in the attack. The drag-off process begins with the spoofed signal copying the true signal with greater power. An Absolute Power Monitor or another type of power monitor sensitive to unexpected changes to signal power could detect this part of the attack. Next, a Distortion Monitor checks the complex autocorrelation function for distortions caused by the interaction between false and true GNSS signals. This interaction occurs when a spoofer attempts to drag off the tracking loops from the true signal in the next phase of a potential attack. If a spoofer successfully deceives the GNSS tracker and drags off the tracking loops without being detected by the previous monitors, a Multi-Peak Monitor may be able to detect the threat by searching for multiple correlation peaks from one satellite [26].

By searching for spoofing characteristics that would manifest during different phases of the attack, these complementary techniques would work together to instantiate defense in depth. Note that each of these monitors would also be effective against other types of threats because they search for different types of effects that could be caused by abnormalities in signal processing. For example, jammers can also cause changes in signal power and multipath can also interfere with signals. These monitors would create a complementary combination of resilience techniques to verify external input because they would detect different types of signal effects, regardless of the cause. This type of complementary protection also makes it more difficult for adversaries to devise new attacks that will evade the combined monitors.

5.3 PNT Solution Synthesis Agent: Position and Navigation Examples

Section 3.2 introduced the PNT resilience concept of protecting internal PNT sources. After initial setup and calibration, internal, physics-based PNT sources do not depend on external input, which can be disrupted or manipulated, so they inherently have a greater degree of integrity and a resilient PNT UE system can rely on them when it must withstand or recover from external threats.

The timing UE system examples given in Section 4.0 showed how a local clock could act as a protected internal PNT source. Limiting the duration when external input was allowed to influence the local clock through GPS steering (Section 4.3 Level 2 example) or completely isolating the clock to protect it from all external influence (Section 4.4 Level 3 and 4 examples) demonstrated two ways to prevent corruption of the local clock when GPS was attacked.

System designers can implement a similar approach for PNT UE systems that provide position and navigation solutions by using an Inertial Measurement Unit (IMU) or INS as the protected internal source. An IMU is a physics-based instrument that reports measurements from internal motion sensors (accelerometers), rotation sensors (gyroscopes), and sometimes heading sensors (magnetometers). INSs are dead reckoning systems that use measurements from physics-based sensors, which may be packaged as IMUs, to calculate the position, orientation, and velocity of motion. Although they have different definitions, both INS and IMU can be used as general terms for physics-based motion sensors in the discussion that follows. Like a local clock, an INS does not require external input after a secure initialization period, so it can be a trusted source of PNT information. Also like a local clock, the PNT solution from an INS can drift over time. PNT sources that receive external input can also use an INS to improve the accuracy of the overall PNT system solution.

The PNT UE design can combine the PNT information from a GNSS receiver and INS using loosely or tightly coupled methods, depending on the depth of access to the GNSS signal processing. In the loosely coupled case, an external Kalman filter integrates the position and velocity solution from the GNSS receiver with the INS. When the GNSS receiver includes an internal Kalman filter in the navigation processor, correlation issues may result that require additional modeling in the external Kalman filter. Tightly coupled GNSS/INS configurations bypass or eliminate the internal GNSS receiver Kalman filter and directly integrate raw measurement data from the GNSS receiver with the INS data in the external Kalman filter [27], which makes it more difficult to completely isolate the INS. System designers can overcome this problem by introducing additional complexity into the PNT UE system [28], which may increase costs, but is necessary for resilient system designs.

There are many different Kalman filter designs for system integration. Appendix A.4 introduces some broad definitions. Ongoing research actively addresses different types of challenges, for example those that arise when multiple GNSS signals are integrated [29] or delays are introduced when the GNSS signals are verified (for example, through authentication [25] [30]).

Considerations for incorporating complementary PNT and Kalman filtering

Combining internal physics based PNT source state information with that of externally generated PNT sources can improve accuracy, enable holdovers, and add diversity to the system. However, some configurations, such as tightly coupled Kalman filters inhibit the ability for system designers to truly isolate PNT sources. PNT UE systems designers must keep resilience in mind while trying to balance factors such as:

- Improved accuracy and resistance to jamming
- Isolation of sources and holdover capability
- Redundant PNT solutions vs system complexity and cost

Many other types of PNT sources can be integrated with GNSS and INS sources in position and navigation systems. For example, [31] describes a PNT UE system that uses a local clock and an IMU as the internal physical sources in addition to GPS and a system utilizing a LiDAR [Light Detection and Ranging] sensor as a visual aid when GPS is unavailable.

5.4 Next Generation PNT Objectives

As PNT UE is incorporated into more consumer products and instrumentation for critical infrastructure, the growing user space will introduce new challenges and provide new opportunities for integration, data collection, and scalability. Next-generation PNT UE systems should be designed for resilience to prevent widespread failures in dependent systems across the civilian user space. In addition to PNT resilience, system designers should consider PNT SA and PNT assurance as two related objectives to incorporate into next generation PNT UE.

PNT UE systems can use SA techniques to collect information about threats and anomalies, which may be used to reduce or eliminate negative effects on the system. SA information can originate from measurements inside the PNT UE system or be received from other instruments external to the system. SA information can also be passed to the user along with the PNT solution. PNT assurance quantifies the degree of confidence that PNT information has integrity and can be used to establish a level of trustworthiness. PNT assurance can also help to manage algorithms for automatic integration of PNT sources.

Figure 14 illustrates how SA and PNT assurance relate to the subsystem view of PNT UE systems. PNT assurance quantifies confidence in the integrity of PNT information and components internal to the PNT UE system. In a managed trust architecture, the PNT UE subsystems are connected through controlled access to PNT information across boundaries, which can be enabled by assessing trustworthiness using PNT assurance. SA involves knowledge of external threats and hazards. Whether SA originates outside the PNT UE system or is generated by internal functions, SA is intended to be reported to external users for their awareness.

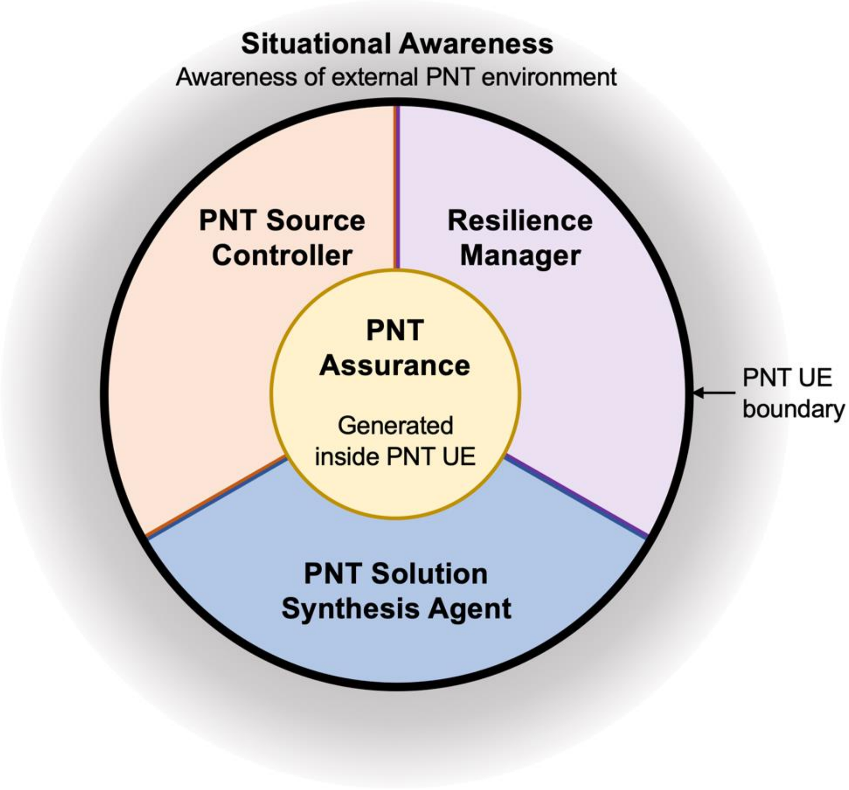


Figure 14. Relationship between resilient PNT UE subsystems and next generation PNT objectives.

5.4.1 PNT Situational Awareness

PNT SA encompasses ***detection***, ***characterization***, and ***geolocation*** of threats that may jeopardize the accurate or uninterrupted delivery of PNT solutions to the user. In the context of GNSS receivers, PNT SA includes detection of different types of interference with satellite signals, characterization of the type and possible intent of the interference, and geolocation of its source. Within the PNT UE system, PNT SA can be used to determine when to respond with resilient functions, including when to stop using PNT information from compromised PNT sources and when it is safe to initiate recovery. PNT SA information can be generated within the PNT UE system and reported to the user. PNT UE systems may also be capable of accepting supplementary PNT SA information from external devices, including dedicated SA UE.

Some of the resilience techniques from the Verify category can also be labelled ***detection*** techniques to achieve SA. Detecting interference for SA purposes requires recording, reporting, and/or further characterizing the threats. Methods to detect threats to improve resilience use the information for managed trust, to mitigate the effects of the threats, and to protect the system PNT solution from corruption.

Threats can be ***characterized*** to enable activities to counter them. Sufficient characterization allows systems to manage threats appropriately, including responses that enable the systems to ignore, deceive, and/or remove them. Characterization may involve measurements of the spectrum, signal data, and/or the direction of the threat. Different forms of analysis can attempt to infer the type and intent of interference. PNT UE systems can record data to analyze later or evaluate as it is collected and report to the user. For resilience, PNT UE systems can use SA threat characterization to respond with resilient behaviors, such as mitigating or protecting against attacks. For SA, the objective is to increase awareness, so next-generation PNT UE systems instrumented for SA should record or report threat characterization information.

Geolocating threats enables activities to counter them, which include antenna nulling in the direction of interference, or countermeasures to remove the threat. As with detection and characterization, responding to the location information is resilient behavior, whereas recording or reporting the threat location information provides SA.

System designers have many ways to implement PNT SA capabilities, which include utilizing existing hardware and measurements to integrate PNT SA into existing UE, or employing independent sensors optimized specifically to report PNT SA in the local environment. Successful implementation ensures awareness of interference and threats for UE relying on PNT services. Whereas the resilience of a particular system PNT solution may reflect the equipment’s endurance and ability to recover from attacks, PNT SA applies to knowledge of the overall environment in which the UE operates.

5.4.2 PNT Assurance

PNT assurance is a way to quantify the integrity of PNT information and establish a level of trustworthiness. One computable definition of PNT assurance is the users’ level of confidence that information (especially pertaining to the position, velocity, and time) output by PNT UE conforms to a specific set of models of the expected accuracy [32] [33]. With this definition, assessing PNT assurance requires knowledge of the PNT UE system model, the use cases, the threat model, the implemented defense techniques, and the accuracy model. PNT resilience and PNT assurance are related, but separate concepts. PNT assurance information can inform resilient behaviors, and some of the Verify category techniques discussed in this RA can act as integrity checks that overlap with PNT assurance assessment methods. However, PNT resilience also includes functions beyond the scope of PNT assurance, including withstanding threats and disruptions through prevention and response techniques and recovering to normal performance after a threat has affected the system.

PNT assurance assessment depends on the context in which to define the different models. During the development or planning process, systems engineers can use assurance assessments to decide whether a system design is sufficiently secure against expected threats. In this situation, the engineers can compare the modelled system PNT solution to the ground truth PNT information input to the model and can easily calculate errors. In the context of real-world applications, the PNT UE system may not recognize specific threats and will lack access to ground truth for error calculations. In this case, PNT assurance calculations involve inferring the likelihood that system PNT solutions conform to a given set of accuracy models based on observations, threat assumptions, and representative models.

Resilient PNT UE systems must have some information, whether generated internally or externally, to inform automatic or user decisions about which resilient actions to take at any given time. For example, PNT UE systems should only initiate recovery functions when they have evidence that the threat or disruption is no longer active. The systems can conduct PNT assurance assessments periodically to identify any changes in integrity and inform resilient behaviors. However, other metrics, which may not rise to the level of rigor provided by PNT assurance calculations, may satisfy this requirement, depending on the PNT UE system design, performance requirements, and target resilience level.

6.0 SUMMARY: NEXT GENERATION RESILIENT PNT ARCHITECTURES

To be resilient, a PNT UE system must demonstrate the ability to withstand and recover from threats and disruptions. The CF [1], introduced in Section 2.0, defined four levels of resilience, starting with basic recovery at Level 1 and, with increasing capabilities to withstand and recover, building up to Level 4, where the system experiences no performance degradation in the presence of a threat. This RA supports the CF by providing examples of architectures that can be used to develop implementations that can meet the requirements for the different resilience levels.

PNT UE Subsystems Summary

- The **PNT Source Controller** gathers PNT information from different PNT sources and controls external input interfaces.
- The **Resilience Manager** implements resilient functions to determine what PNT state information is suitable for the system PNT solution and when it is appropriate to implement mitigations or automatic recovery.
- The **PNT Solution Synthesis Agent** produces the system PNT solution delivered to the user by combining verified PNT state information from different PNT sources.

The architecture instances described In Section 4.0 show that a resilient PNT UE system has three main objectives, which may be organized under three architecture components known as PNT UE Subsystems: the PNT Source Controller (for gathering PNT information), the Resilience Manager (for implementing resilient functions), and the PNT Solution Synthesis Agent (for producing the system PNT solution delivered to the user). Figure 13 in Section 5.0 depicts how the three subsystems handle trust within the PNT UE system. Section 5.0 further explored the objectives and challenges that each of the PNT UE Subsystems may encounter in integrating resilience techniques to implement managed trust and produce resilient outcomes.

PNT Resilience Concepts Summary

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

A ***holistic*** approach to PNT UE system architecture design considers the resilient behaviors of individual elements, their interactions with each other, and how they are integrated as a whole into the overall system to produce resilient outcomes, which include the ability to withstand and recover from threats and disruptions.

The CF also identified three core functions of resilience: *Prevent, Respond,* and *Recover*. Section 3.0 of this RA showed how the core functions of resilience and trust concepts used to implement cybersecurity and cyber resiliency can be applied to PNT UE systems to develop a set of PNT resilience concepts adapted to the unique characteristics of PNT UE systems. Different resilience techniques can implement each of the PNT resilience concepts; these PNT resilience techniques fall into seven categories: *Obfuscate, Limit, Verify, Isolate, Mitigate, Diversify*, and *Recover*. Appendix A lists specific resilience techniques for each category.

PNT Resilience Technique Categories

Obfuscate characteristics to confuse attackers.

Limit external input to minimize attack opportunities.

Verify external input for managed trust.

Isolate components to protect from external influence.

Mitigate the effects of threats.

Diversify technologies to reduce common mode failures.

Recover performance when it is safe to do so.

In general, a single PNT resilience technique will not produce overall resilience for a PNT UE system. However, system designers can use a holistic approach to develop combinations of techniques which can be integrated into architectures to execute the objectives of the PNT UE Subsystems and generate overall resilient outcomes. Developing resilient combinations of techniques requires knowledge of the user's PNT performance needs, expected threats and disruption types, and the overall PNT environment the PNT UE system will occupy. This RA provides specific examples and overall concepts and considerations to enable these design objectives.

REFERENCES

[1] Department of Homeland Security (DHS) Science and Technology Directorate (S&T), "Resilient PNT Conformance Framework, Version 2.0," May 2022. https://www.dhs.gov/publication/st-resilient-pnt-conformance-framework.

[2] The White House, Office of the Press Secretary, "Presidential Policy Directive -- Critical Infrastructure Security and Resilience/PPD-21," 12 February 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[3] M. Lombardi, "NIST Technical Note 2189, An Evaluation of Dependencies of Critical Infrastructure Timing Systems on the Global Positioning System (GPS)," November 2021. DOI: 10.6028/NIST.TN.2189.

[4] National Security of the National Science & Technology Council, "Positioning, Navigation, and Timing Research and Development Interagency Working Group Subcommittee on Resilience Science and Technology Committee on Homeland and National Research and Development Plan for Position, Navigation, and Timing Resilience," August 2021. https://www.whitehouse.gov/wp-content/uploads/2021/08/Position_Navigation_Timing_RD_Plan-August-2021-1.pdf.

[5] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau and R. McQuaid, "NIST SP 800-160 Volume 2, Revision 1, Developing Cyber Resilient Systems: A Systems Security Engineering Approach," December 2021. DOI: 10.6028/NIST.SP.800-160v2r1.

[6] National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity," 16 April 2018. DOI: 10.6028/NIST.CSWP.04162018.

[7] M. Bartock, J. Brule, Y.-S. Li-Baboud, S. Lightman, J. McCarthy, K. Reczek, D. Northrip, A. Scholz and T. Suloway, "Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services (NISTIR 8323)," February 2021. DOI: 10.6028/NIST.IR.8323.

[8] National Institute of Standards and Technology (NIST), "NIST PNT Profile: A Quick Guide," February 2021. https://www.nist.gov/system/files/documents/2021/02/11/PNT%20Services_%20A%20Quick%20Guide%20Final.pdf.

[9] K. M. Skey, "Responsible use of GPS for critical infrastrucure," in *Critical Infrastructure Protection and Resilience North America*, Merritt Island, Florida, 2017. https://www.gps.gov/multimedia/presentations/2017/12/CIPRNA/skey.pdf.

[10] E. Wong, "A Cybersecurity-based Vision for NextGen Resilient PNT," in *61st Meeting of the Civil GPS Service Interface Committee*, St. Louis, Missouri, 2021. https://www.gps.gov/cgsic/meetings/2021/wong.pdf.

[11] P. W. Ward, "GNSS Receivers," in *Understanding GPS/GNSS: Principles and Applications*, 3rd ed., E. D. Kaplan and C. J. Hegarty, Eds., Boston/London, Artech House, 2017, pp. 339-548.

[12] J. W. Betz, *Engineering Satellite-Based Navigation and Timing: Global Navigation Satellite Systems, Signals, and Receivers*, IEEE, 2016. https://ieeexplore.ieee.org/servlet/opac?bknumber=7394655.

[13] "ISO/IEC/IEEE International Standard - Systems and software engineering--Systems and software assurance --Part 1:Concepts and vocabulary," in *ISO/IEC/IEEE 15026-1:2019(E)*, pp.1-38, 1 March 2019, DOI: 10.1109/IEEESTD.2019.8657410.

[14] National Cybersecurity & Communications Integration Center (NCCIC) and National Coordinating Center for Communcations (NCC), "Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure." https://us-cert.cisa.gov/sites/default/files/documents/Improving_the_Operation_and_Development_of_Global_Positioning_System_%28GPS%29_Equipment_Used_by_Critical_Infrastructure_S508C.pdf.

[15] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "NIST SP 800-207 Zero Trust Architecture," August 2020. DOI: 10.6028/NIST.SP.800-207.

[16] Global Positioning Systems Directorate Systems Engineering & Integration, "Interface Specification IS-GPS-200M," 13 April 2021. https://www.gps.gov/technical/icwg/IS-GPS-200M.pdf.

[17] M. A. Lombardi, "The Use of GPS Disciplined Oscillators as Primary Frequency Standards for Calibration and Metrology Laboratories," *Measure: The Journal of Measurement Science,* vol. 3, no. 3, 2008. https://tf.nist.gov/general/pdf/2297.pdf.

[18] I. Fernández-Hernández, V. Rijmen, G. Seco-Granados, J. Simon, I. Rodríguez and J. D. Calle, "A Navigation Message Authentication Proposal for the Galileo Open Service," *NAVIGATION, Journal of the Institute of Navigation,* vol. 63, no. 1, pp. 85 - 102, 2016. https://www.ion.org/publications/pdf.cfm?articleID=102667.

[19] J. Sherman, L. Arissian, R. Brown, M. Deutch, E. Donley, V. Gerginov, J. Levine, G. Nelson, A. Novick, B. Patla, T. Parker, B. Stuhl, D. Sutton, J. Yao, W. Yates, V. Zhang and M. Lombardi, "NIST Technical Note 2187 A Resilient Architecture for the Realization and Distribution of Coordinated Universal Time to Critical Infrastructure Systems in the United States," November 2021. DOI: 10.6028/NIST.TN.2187.

[20] D. A. Grejner-Brzezinska, C. K. Toth, T. Moore, J. F. Raquet, M. M. Miller and A. Kealy, "Multisensor Navigation Systems: A Remedy for GNSS Vulnerabilities?," *Proceedings of the IEEE,* vol. 104, no. 6, pp. 1339-1353, 2016. DOI: 10.1109/JPROC.2016.2528538.

[21] A. Hansen, S. Mackey, H. Wassaf, V. Shah, E. Wallischeck, C. Scarpone, M. Barzach and E. Baskerville, "Complementary PNT and GPS Backup Technologies Demonstration Report: Sections 1 through 10," U.S. Department of Transportation Volpe Center, 14 January 2021. https://www.transportation.gov/sites/dot.gov/files/2021-01/FY%2718%20NDAA%20Section%201606%20DOT%20Report%20to%20Congress_Combinedv2_January%202021.pdf.

[22] A. Hansen, S. Mackey, H. Wassaf and K. V. Dyke, "Complementary PNT Technology Demonstration," in *Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021)*, St. Louis, Missouri, 2021. DOI: 10.33012/2021.18075.

[23] R. Mason, J. Bonomo, T. Conley, R. Consaul, D. R. Frelinger, D. A. Galvan, D. A. Goldfeld, S. A. Grossman, B. A. Jackson, M. Kennedy and e. al., "Analyzing a More Resilient National Positioning, Navigation, and Timing Capability," Homeland Security

Operational Analysis Center operated by the RAND Corporation, RR-2970-DHS, 2021. https://www.rand.org/pubs/research_reports/RR2970.html.

[24] U.S. Department of Transportation Federal Aviation Administration, "Aeronautical Information Manual: Official Guide to Basic Flight Information and ATC Procedures," 17 June 2021. https://www.faa.gov/air_traffic/publications/media/aim_basic_6_17_21.pdf.

[25] I. Fernández-Hernández, T. Walter, K. Alexander, B. Clark, E. Châtre, C. Hegarty, M. Appel and M. Meurer, "Increasing International Civil Aviation Resilience: A Proposal for Nomenclature, Categorization and Treatment of New Interference Threats," *Proceedings of the 2019 International Technical Meeting of The Institute of Navigation*, Reston, Virginia, January 2019, pp. 389-407. DOI: 10.33012/2019.16699.

[26] M. L. Psiaki and T. E. Humphreys, "GNSS Spoofing and Detection," *Proceedings of the IEEE,* vol. 104, no. 6, pp. 1258 - 1270, 2016. DOI: 10.1109/JPROC.2016.2526658.

[27] J. B. Bullock and M. King, "Integration of GNSS with Other Sensors and Network Assistance," in *Understanding GPS/GNSS Principles and Applications*, 3rd ed., E. D. Kaplan and C. J. Hegarty, Eds., Boston/London, Artech House, 2017, pp. 789-914.

[28] G. T. Schmidt and R. E. Philips, "INS/GPS integration architectures," Massachusetts Institute of Technology, Lexington, MA, 2010.

[29] B. Reuper, M. Becker and S. Leinen, "Benefits of Multi-Constellation/Multi-Frequency GNSS in a Tightly Coupled GNSS/IMU/Odometry Integration Algorithm," *Sensors,* vol. 18, no. 3052, 2018. DOI: 10.3390/s18093052.

[30] M. C. Esswein and M. L. Psiaki, "GPS Spoofing Resilience via NMA/Watermarks Authentication and IMU Prediction," in *34th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2021)*, September 20-24, 2021. DOI: 10.33012/2021.17997.

[31] S. Moafipoor, L. Bock and J. A. Fayman, "Resilient Sensor Management for Dismounted Assured-PNT," in *Proceedings of the 2020 International Technical Meeting, ION ITM 2020*, San Diego, 2020. DOI: 10.33012/2020.17202.

[32] S. Römisch and B. Patla, "Towards Metrics for Assured Time: a Report," in *Workshop on Synchronization and Timing Systems*, San Jose, 2019. https://wsts.atis.org/presentation/towards-metrics-for-assured-time-a-report/.

[33] A. Molina-Markham and J. J. Rushanan, "Positioning, Navigation, and Timing Trust Inference Engine," 20 May 2020. https://insidegnss.com/positioning-navigation-and-timing-trust-inference-engine/.

[34] C. Günther, "A Survey of Spoofing and Counter-Measures," *Navigaion,* vol. 61, no. 3, pp. 159-177, 2014. https://www.ion.org/publications/pdf.cfm?articleID=102624.

[35] F. Naeem, M. Mohsin, U. Rauf and L. A. Khan, "Formal approach to thwart against drone discovery attacks: A taxonomy of novel 3D obfuscation mechanisms," *Future Generation Computer Systems,* vol. 115, pp. 374-386, 2021. DOI: 10.1016/j.future.2020.09.001.

[36] R. Paulet, M. G. Kaosar, X. Yi and E. Bertino, "Privacy-Preserving and Content-Protecting Location Based Queries," *IEEE Transactions on Knowledge and Data Engineering,* vol. 26, no. 5, pp. 1200-1210, May 2014. DOI: 10.1109/TKDE.2013.87.

[37] A. Albelaihy and J. Cazalas, "A survey of the current trends of privacy techniques employed in protecting the Location privacy of users in LBSs," in *2nd International Conference on Anti-Cyber Crimes (ICACC)*, 2017. DOI: 10.1109/Anti-Cybercrime.2017.7905256.

[38] D. L. Adamy, "Radar Decoys," in *EW 104: Against a new generation of threats*, Norwood, MA, Artech House, 2015, pp. 379-402.

[39] J. M. Anderson, K. L. Carroll, N. P. DeVilbiss, J. T. Gillis, J. C. Hinks, B. W. O'Hanlon, J. J. Rushanan, L. Scott and R. A. Yazdi, "Chips-Message Robust Authentication (Chimera) for GPS Civilian Signals," in *Proceedings of the 30th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2017)*, Portland, OR, 2017. DOI: 10.33012/2017.15206.

[40] L. Perdue, J. Fischer and R. Dries, "Signals of Opportunity as an Augmentation or Alternative to GNSS for Critical Timing Applications," in *Proceedings of the 2017 Precise Time and Time Interval Meeting*, Monteray, CA, 2017. DOI: 10.33012/2017.14988.

[41] N. Francis, B. Breitsch, J. Morton and J. Hinks, "Ionospheric Effects on Future Navigation Signals: Frequency Hopping Modulation," in *Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation*, St. Louis, MO, 2021. DOI: 10.33012/2021.18009.

[42] "3GPP TS 38.305; 5G; NG Radio Access Network (NG-RAN); Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN," January 2022. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3310.

[43] A. K. Scholz, "The Flip: More Robust Timing Applications using GPS," in *24th Meeting of the Space-Based Positioning Navigation and Timing National Advisory Board*, Cocoa Beach, FL, 2019. https://www.gps.gov/governance/advisory/meetings/2019-11/scholz.pdf.

[44] I. J. Gupta, I. M. Weiss and A. W. Morrison, "Desired Features of Adaptive Antenna Arrays for GNSS Receivers," *Proceedings of the IEEE,* vol. 104, no. 6, pp. 1195-1206, 2016. DOI: 10.1109/JPROC.2016.2524416.

[45] R. Morales-Ferre, P. Richter, E. Falletti, A. d. l. Fuente and E. S. Lohan, "A Survey on Coping With Intentional Interference in Satellite Navigation for Manned and Unmanned Aircraft," *IEEE Communications Surveys & Tutorials,* vol. 22, no. 1, pp. 249-291, 2020. DOI: 10.1109/COMST.2019.2949178.

[46] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen and G. Lachapelle, "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques," *International Journal of Navigation and Observation,* vol. 2012, no. 127072, pp. 1-16, 2012. DOI: 10.1155/2012/127072.

[47] W. Wang, I. A. Sanchez, G. Caparra, A. McKeown, T. Whitworth and E. S. Lohan, "A Survey of Spoofer Detection Techniques via Radio Frequency Fingerprinting with Focus on the GNSS Pre-Correlation Sampled Data," *Sensors,* vol. 21, no. 3012, 2021. DOI: 10.3390/s21093012.

[48] Z. Wu, Y. Zhang, Y. Yang, C. Liang and R. Liu, "Spoofing and Anti-Spoofing Technologies of Global Navigation Satellite System: A Survey," *IEEE Access*, vol. 8, pp. 165444-165496. DOI: 10.1109/ACCESS.2020.3022294.

[49] Department of Homeland Security (DHS) Science and Technology Directorate (DHS), "GPS Receiver Whitelist Development Guide," 12 July 2021. https://www.dhs.gov/publication/gps-receiver-whitelist-development-guide.

[50] Department of Homeland Security (DHS) Science and Technology Directorate (S&T), "Epsilon Algorithm Suite," February 2021. https://github.com/cisagov/Epsilon.

[51] Department of Homeland Security (DHS) Science and Technology Directorate (S&T), "PNT Integrity Library," February 2021. https://github.com/cisagov/PNT-Integrity.

[52] L. Scott, "Spoofing Incident Report: An Illustration of Cascading Security Failure," 9 October 2017. https://insidegnss.com/spoofing-incident-report-an-illustration-of-cascading-security-failure/.

[53] Zhang, V., Weiss, M., Powers, E., Loiler, R., "GPS Week Rollover & Y2K Compliance for NBS-Type Receivers," *Proceedings of the 30th Annual Precise Time and Time Interval Systems and Applications Meeting*, Reston, Virginia, December 1998, pp. 11-18. https://www.ion.org/publications/abstract.cfm?articleID=14119.

[54] C. Hegarty, B. O’Hanlon, A. Odeh, K. Shallberg, and J. Flake, “Spoofing Detection in GNSS Receivers through Cross-Ambiguity Function Monitoring,” *Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)*, Miami, FL, September 2019. DOI: 10.33012/2019.16986.

[55] A. G. Dempster and E. Cetin, "Interference Localization for Satellite Navigation Systems," *Proceedings of the IEEE,* vol. 104, no. 6, 2016. DOI: 10.1109/JPROC.2016.2530814.

[56] L. Scott, "Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems," in *Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003)*, Portland, OR, 2003. https://www.ion.org/publications/abstract.cfm?articleID=5339.

[57] J. D. Jurado, "Autonomous and Resilient Management of All-Source Sensors for Navigation Assurance" (2019). Air Force Institute of Technology, PhD dissertation, 2361. https://scholar.afit.edu/etd/2361.

[58] J. Jurado, J. Raquet, C. M. S. Kabban and J. Gipson, "Residual-based multi-filter methodology for all-source fault detection, exclusion, and performance monitoring," *NAVIGATION, Journal of the Institute of Navigation,* vol. 67, no. 3, pp. 493 - 510, 2020. DOI: 10.1002/navi.384.

[59] C. Tanil, S. Khanafseh, M. Joerger and B. Pervan, "An INS Monitor to Detect GNSS Spoofers Capable of Tracking Vehicle Position," *IEEE Transactions on Aerospace and Electronic Systems,* vol. 54, no. 1, pp. 131-143, 2018. DOI: 10.1109/TAES.2017.2739924.

[60] J. D. Quartararo and S. E. Langel, "Detecting Slowly Accumulating Faults Using a Bank of Cumulative Innovations Monitors in Kalman Filters," *NAVIGATION: Journal of the Institute of Navigation*, vol. 69, no. 1, navi.507, March 2022. DOI: 10.33012/navi.507.

[61] The MITRE Corporation, "D3fend, A knowledge graph of cybersecurity countermeasures, 0.10.0-BETA-2," https://d3fend.mitre.org.

[62] K. Kauffman, D. Marietta, J. Raquet, D. Carson, R. C. Leishman, A. Canciani, A. Schofield, M. Caporellie, "Scorpion: A Modular Sensor Fusion Approach for Complementary Navigation Sensors," *2020 IEEE/ION Position, Location and*

Navigation Symposium (PLANS), 2020, pp. 156-167, DOI: 10.1109/PLANS46316.2020.9110165.

[63] M. J. Coleman and R. L. Beard, "Autonomous clock ensemble algorithm for GNSS applications," *NAVIGATION, Journal of the Institute of Navigation,* vol. 67, no. 2, pp. 333-346. DOI: 10.1002/navi.366.

[64] T. Kraus, F. Ribbehege and B. Eissfeller, "Use of the Signal Polarization for Anti-jamming and Anti-spoofing with a Single Antenna," in *Proceedings of the 27th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2014)*, Tampa, Florida, 2014. https://www.ion.org/publications/abstract.cfm?articleID=12336.

[65] C. Yang and A. Soloviev, "All Signal Acquisition Processing for Spoofing Detection, Estimation, Mitigation and Intent Analysis," in *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)*, 2020. DOI: 10.33012/2020.17566.

[66] F. Rothmaier, Y.-H. Chen, S. Lo and T. Walter, "GNSS Spoofing Mitigation in the Position Domain," in *Proceedings of the 2021 International Technical Meeting of The Institute of Navigation*, 2021. DOI: 10.33012/2021.17824.

[67] F. Rothmaier, Y.-H. Chen, S. Lo, J. Blanch and T. Walter, "Providing Continuity and Integrity in the Presence of GNSS Spoofing," in *Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021)*, St. Louis, Missouri, 2021. DOI: 10.33012/2021.17984.

[68] J. Wen, H. Li, Z. Wang and M. Lu, "Spoofing Discrimination Using Multiple Independent Receivers Based on Code-based Pseudorange Measurements," in *Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)*, Miami, Florida, 2019. DOI: 10.33012/2019.17075.

[69] N. Stenberg, E. Axell, J. Rantakokko and G. Hendeby, "GNSS Spoofing Mitigation Using Multiple Receivers," in *2020 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, Portland, Oregon, 2020, pp. 555-565. https://www.ion.org/publications/abstract.cfm?articleID=17484.

[70] O. Montenbruck, P. Steigenberger, L. Prange, Z. Deng, Q. Zhao, F. Perosanz, I. Romero, C. Noll, A. Stürze, G. Weber, R. Schmid, K. MacLeod and S. Schaer, "The Multi-GNSS Experiment (MGEX) of the International GNSS Service (IGS) – Achievements, prospects and challenges," *Advances in Space Research,* vol. 59, no. 7, pp. 1671-1697, 2017. DOI: 10.1016/j.asr.2017.01.011.

[71] P. W. Ward, "GPS Receiver RF Interference Monitoring, Mitigation, and Analysis Techniques," *NAVIGATION, Journal of the Institute of Navigation, Volume 41, Number 4,* vol. 41, no. 4, pp. 367-392, 1994. DOI: 10.1002/j.2161-4296.1994.tb01886.x.

[72] S. Lo, Y. H. Chen, T. Reid, A. Perkins, T. Walter and P. Enge, "Keynote: The Benefits of Low Cost Accelerometers for GNSS Anti-Spoofing," in *Proceedings of the ION 2017 Pacific PNT Meeting*, Honolulu, Hawaii, 2017. DOI: 10.33012/2017.15109.

[73] R. Da, "Investigation of a Low-Cost and High-Accuracy GPS/IMU System," in *Proceedings of the 1997 National Technical Meeting of The Institute of Navigation*,

Santa Monica, CA, 1997, pp. 955-963. https://www.ion.org/publications/abstract.cfm?articleID=557.

[74] G. Vyasaraj, B. Raghothama and J. Ray, "Cost Effective & Innovative Approach to Recover from Data Corruptions Due to Radiation Effects in GPS Receivers in Leo-Orbits," in *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008)*, Savannah, GA, 2008, pp. 795-801. https://www.ion.org/publications/abstract.cfm?articleID=8000.

[75] W. Torres-Pomales, "Software Fault Tolerance: A Tutorial," National Aeronautics and Space Administration, Hampton, VA, 2000. https://ntrs.nasa.gov/api/citations/20000120144/downloads/20000120144.pdf.

[76] B. Kujur, S. Khanafseh and B. Pervan, "A Solution Separation Monitor using INS for Detecting GNSS Spoofing," in *Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020)*, 2020. DOI: 10.33012/2020.17535.

[77] M. J. Murrian, L. Narula, P. A. Iannucci, S. Budzien, B. W. O'Hanlon, M. L. Psiaki, T. E. Humphreys, "First results from three years of GNSS interference monitoring from low Earth orbit," *NAVIGATION, Journal of the Institute of Navigation*, vol. 68, no. 4, pp. 673-685, 2021. DOI: 10.1002/navi.449.

[78] K. Kovach, P. J. Mendicki, E. D. Powers and B. Renfro, "GPS Receiver Impact from the UTC Offset (UTCO) Anomaly of 25-26 January 2016," in *Proceedings of the 29th International Technical Meeting of the ION Satellite 2887 Division, ION GNSS+ 2016*, Portland, OR, 2016. DOI: 10.33012/2016.14767.

[79] C. Curry, "The Impact of the GPS UTC Anomaly Event of 26 January 2016 on the Global Timing Community," *Proceedings of the 48th Annual Precise Time and Time Interval Systems and Applications Meeting*, Monterey, California, January 2017, pp. 164-170. DOI: 10.33012/2017.14986.

[80] J. Betz, “Navwar Compliance Methodology—An Initial Discussion,” MITRE PowerPoint Presentation to Navwar Working Group, 2 December 2021.

[81] "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems," in *IEEE Standard 1588-2019 (Revision of IEEE Standard 1588-2008)*, pp.1-499, June 2020. DOI: 10.1109/IEEESTD.2020.9120376.

APPENDIX A: RESILIENCE TECHNIQUE EXAMPLES

Section 3.0 introduced seven resilience technique categories, supported by the PNT resilience concepts from a holistic approach. The high-level resilient timing UE system architecture examples in Section 4.0 showed how system designers can combine specific resilience techniques from these categories to form resilient architectures. This appendix provides more details about each of the resilience technique categories, as well as select examples for each one. Table 2 summarizes the resilience technique categories and gives the numbers of the subsection that describe each.

Table 2. Resilience technique categories and sections.

PNT Resilience Technique Categories	Section
Obfuscate characteristics to confuse attackers	A.1
Limit external input to minimize attack opportunities	A.2
Verify external input to implement managed trust	A.3
Isolate components to protect from external influence	A.4
Mitigate the effects of threats	A.5
Diversify technologies to reduce common mode failures	A.6
Recover performance when it is safe to do so	A.7
PNT Resilience techniques that fit multiple categories	A.8

The techniques included in each category section show the breadth of possible methods to implement resilience and provide a selection of examples. Specific examples help clarify the broad PNT resilience concepts and the generalized PNT resilience technique categories introduced in Section 3.0, as well as the requirements for the different resilience levels outlined in the CF [1] and summarized in Section 2.0. The categorization facilitates the selection of different techniques to build durable, layered PNT UE systems that conform to the defense in depth concept for resilient system architectures. Examples demonstrating the integration of different resilience techniques are given in Sections 4.0 and 5.0. Recognizing the overall methods for resilient behavior may motivate the development of new resilience techniques for each category, or the identification of new categories.

Note that this document does not include all possible resilience techniques and is not meant to be an exhaustive list. It includes each specific technique as an example to support the resilient behavior for each category. Inclusion in this document should not be interpreted as a DHS preference or recommendation. The specific implementation, the overall performance of the PNT UE system, and the characteristics of the threats or disruptions that are encountered determine effectiveness of each technique.

Several resilience technique categories address ways to implement resilience while using external input. External input includes any signal or information coming into the PNT UE system.

This may include radiated signals, such as GNSS signals, or information provided over a physical connection, such as timing services supported over fiber or Ethernet connections. External input is an important way to deliver PNT information over large areas and to coordinate PNT information over connected or networked devices. However, it also introduces an opportunity for attackers to deny or degrade the information, or tamper with it to deceive the receiver.

A.1 Obfuscate Characteristics

Adversaries with specific knowledge of PNT UE systems can employ sophisticated techniques to target known attack surfaces and degrade or deny PNT solutions to the user. Responding to these threats by concealing or obfuscating system characteristics can minimize the attack surface and reduce the likelihood of a successful attack. Several examples of resilience techniques in the Obfuscate category are included in Table 3 and described below.

Some attack techniques, such as spoofing, rely on knowledge of the position of the target receiving antenna. Obfuscating the actual antenna position from the external threat can make spoofing more difficult to accomplish and easier to detect. Attackers can employ spoofing to attempt to trick PNT UE systems into providing false PNT solutions to users. Internal system models can check PNT state information against prior states and derive reasonable estimates of how much the observables should change in time. Effective spoofing must not deviate too much from actual PNT observables to avoid being detected by anti-spoof algorithms (some examples are given in the Verify resilience category in Appendix A.2). Therefore, successful spoofing attacks require accurate position estimates for the targeted user. Obfuscating the user's position makes spoofing less effective for threats employing spoofing by coherent superposition [34].

Different position obfuscation techniques are effective against different methods used by attackers to estimate the PNT UE system's location. For example, an unmanned aerial vehicle (UAV) may broadcast its position to the UAV's base station over ad-hoc networks. Eavesdroppers on the network may be able to obtain the UAV position and use it to effectively spoof the onboard PNT UE systems. System designers have developed multiple obfuscation algorithms to counter this scenario [35]. Additionally, system designs can use cryptographic methods to prevent location data from being shared with anyone who does not have the correct key. Researchers have explored this form of obfuscation for general privacy in location-based services [36] [37], but the principles apply to specific threats such as spoofing.

If attackers estimate the PNT UE position by other means, such as radar or optical sensors, PNT UE systems can employ other obfuscation methods. The use of active or passive decoys as radar countermeasures can obfuscate the true position of moving objects [38]. Similarly, decoy antennas can be placed near fixed installations [9].

PNT UE systems can employ a broadband receiver to further confuse a would-be spoofer and frustrate their efforts through spectrum usage obfuscation. Including PNT sources that receive signals from multiple different GNSS constellations or (potentially encrypted) signals of opportunity forces spoofers to cover a larger frequency band and range of signals. This can be considered obfuscation if the spoofer is aware of the receiver's capability but not the specific signals being used. Additionally, frequency hopping falls into this category, as the spoofer must also know which frequencies to use at any given time.

Table 3. Example resilience techniques to obfuscate PNT characteristics from potential attackers.

Technique	Description	References
Encrypt Transmitted Position Data	Render position data unreadable to eavesdroppers on location-based services.	[36]
Navigation Message Authentication	Authenticate encrypted navigation messages using a key that is obtained separately, such as through a delayed broadcast. PNT information from signals with authenticated navigation messages have higher integrity.	[18] [39]
Obfuscate Transmitted Position Data	Alter position data transmitted over network to prevent eavesdroppers from leveraging precise position for spoofing.	[35]
Spectrum Usage Obfuscation	Use a greater portion of the frequency spectrum through multi-GNSS, dedicated terrestrial beacon systems (TBS), signals of opportunity, or develop new positioning signals that employ techniques such as frequency hopping.	[40] [41] [42]
Obfuscate Position with Decoys	Deploy decoy antennas to deflect adversarial attempts to spoof GNSS position solutions.	[9] [38]
Randomize Holdover Periods	Use GNSS signals to discipline internal clock at random intervals to limit vulnerability to external threats and obfuscate time interval in which spoofing should occur.	[43]

A.2 Limit Untrusted External Input

Many PNT sources rely on external input, such as GNSS signals, to produce PNT solutions. However, this creates a potential attack surface that adversaries may exploit through threat methods such as jamming or spoofing. PNT UE systems that rely on external input are also vulnerable to accidental outages and other events that can disrupt the delivery of external information. The Limit resilience technique category includes different methods to limit the dependence on and influence of untrusted external input in the PNT UE system. A few examples of resilience techniques from the Limit category are listed in Table 4.

One method to limit untrusted external input is to use internal physical PNT sources as the primary source of PNT information in the PNT UE system. For example, one type of internal physical PNT source would be a local clock with good short-term stability. To improve the long-term stability of the PNT solution, a local clock can be disciplined by a PNT source that receives external input. By disciplining occasionally, rather than constantly, this resilience technique limits the timeframe during which spurious input can influence a PNT UE system [1].

A PNT source that receives external input has many options for the timescale to occasionally discipline a primary, internal PNT source. Disciplining can be implemented at periodic intervals with a duty cycle that minimizes the total disciplining time while maintaining the accuracy required by the application using the PNT UE system. Alternatively, updates can be made after resilience techniques from the Verify category have established that the external input is trustworthy. Randomized disciplining episodes, which do not occur at regular, predictable intervals, are an option that can also obfuscate the disciplining schedule from attackers.

External input from RF sources can be limited directionally through the use of antennas with desirable radiation pattern characteristics. The antenna for semi-permanent installations can be designed to have a fixed radiation pattern appropriate to the application and assumed threats. For example, a horizon nulling antenna for GNSS will maintain high gain in the direction of overhead satellites while limiting the received power from terrestrial interference sources.

More complex antennas can dynamically alter their radiation patterns to limit external radiation in a changing environment. For these designs, input received on multiple antenna elements is combined coherently so that signals originating from some directions are cancelled or nulled out. These controlled reception pattern antennas add functionality at the expense of increasing system complexity and cost.

PNT UE systems can also use frequency selective notch filters to reduce the impact of unintentional interference.

Table 4. Example resilience techniques to limit untrusted external input.

Technique	Description	References
Directional Limits	Prevent undesired RF signals from entering the receiver by limiting the allowed directions of arriving signals through the antenna reception pattern. Includes horizon nulling fixed-reception pattern antennas and controlled reception pattern antennas with adaptive nulling.	[14] [44]
Frequency Limits	Excise narrowband RF interference with notch filters.	[45]
Temporal Limits	Limit the period of time during which an internal PNT source can be influenced by external input. For example, cycle between GNSS-controlled and free-running periods with a local clock to minimize the total disciplining time while still achieving the necessary accuracy.	[43]

A.3 Verify External Input

GNSS receivers and many other types of PNT source technologies depend on external input to generate source PNT solutions. External input includes any signal or information coming into the PNT UE system through radiated signals or physical connections. Threats can deny, degrade, or manipulate the information, so external input should not be inherently trusted. However, different techniques that verify the external input when it is received can establish a degree of trustworthiness. Many of the resilience techniques in the Verify category are termed “anti-spoof” techniques because they were developed to detect different characteristics of spoofing attacks. When resilience techniques from the Verify category indicate that external input is untrustworthy, the PNT UE architecture can prevent the untrusted information from propagating in the system and respond with different techniques from the Isolate, Mitigate, Diversify, and Recover categories.

Resilience techniques that fall into the Verify category can be grouped into approaches to show how common strategies emerge. Individual verification techniques can be viewed as different ways to execute an overall strategy. Some verification approaches try to detect different characteristics of atypical performance that can indicate attack or malfunction. If the verification step detects no issues, a degree of confidence in the integrity of the information can be established. With the concept of defense in depth, it is important to implement complementary layers of detection algorithms. Researchers have developed many different techniques to detect jamming and spoofing threats. Survey articles [26] [34] [46] [47] [48] review spoofing threats and anti-spoof countermeasures. Subsections A.3.1-A.3.6 group a selection of examples by the type of characteristics they are meant to detect, to show the breadth of different techniques available to system designers.

Verification also includes approaches to confirm information through authentication or cross-verification. PNT information can be authenticated using trusted information, which may be encrypted, to verify its integrity, as described in Section A.3.7. Examples of cross-verification include comparing the information received from different GNSS satellites or comparing the PNT solutions provided by different PNT sources. Resilient PNT UE systems must verify the PNT information from each PNT source before comparing across sources so that more trustworthy information is prioritized. Section A.3.8 describes different approaches to cross-verify PNT information, along with specific techniques and references that provide examples.

Applying the defense-in-depth concept improves resilience when techniques to verify external input are layered to create complementary combinations. Each technique in the Verify category may only be designed to detect a specific effect within the PNT UE system that may be caused by a threat or malfunction. Some techniques may also depend on specific observables that may not always be available. System designers must have a thorough understanding of the limitations of the verification techniques, the applications that use the system PNT solution, and expected potential threats when selecting methods to implement in resilient PNT UE systems. To respond to a broad range of threats, verification techniques that monitor for different types of effects in different ways should be layered on one another. Some threats may not be detected by some techniques, but together, the different techniques should produce a resilient defense. Section 5.2 describes some specific examples of effective combinations of resilience techniques from the Verify category.

A.3.1 Monitor for Consistency with Known Standards, Formats, and Patterns

This approach searches for spoofing characteristics by monitoring external input for consistency with known standards, formats, and patterns. These include known physical parameters, standardized bounds, normalized formats, and scheduled changes. PNT UE systems should only accept external input if it conforms to the expected standards, formats, and patterns.

Table 5 provides several examples of this approach, along with references that discuss them in more detail. These examples apply to GNSS input, but similar checks are possible for any external input that is expected to conform to a known standard, format, or pattern. System designers can develop a conformance verification algorithm for any set of standardized parameters. DHS S&T has provided a GPS Receiver Whitelist Development Guide [46] online.

Table 5. Example resilience techniques to detect spoofing by monitoring for consistency with known standards, formats, and patterns.

Technique	Description	References
Conformance Verification Algorithm	Check the value, range, and state information of data against the relevant interface specification or standard. For example, a whitelist algorithm to check GPS navigation data is consistent with the IS-GPS-200M [16] specification.	[14] [46]
GNSS Schedule Monitor	Check for unscheduled navigation message updates that do not follow the usual update pattern and are unlikely to be from the GNSS satellite.	[34]
GNSS Satellite ephemeris consistency check	Identify incorrect satellite ephemeris information compared to the expected values provided by either (1) other satellites or (2) an online database of satellite locations.	[26] [46]

A.3.2 Monitor for Physical Consistency

PNT sources can output observables to check for physical consistency. For example, the position, velocity, and time (PVT) information in the PNT solution output from a PNT source should be physically consistent and adhere to the known physical limitations of the PNT UE system. Other observables may include intermediate parameters calculated in the process of forming the PNT solution and measurements of internal states. Consistency means that the UE system detects no unexpected jumps, no physically impossible values, and passes basic checks comparing across different observables. These checks are only effective when the monitored observables are available and relevant. For example, techniques that depend on antenna motion would not function when the UE is stationary.

Table 6 gives a few example techniques to monitor PVT information and other observables for consistency, along with references. DHS S&T has provided sample code implementations for a variety of verification methods from this approach on Github: *Epsilon Algorithms* [50] and *PNT Integrity Library* [51]. Since these checks compare observables from GNSS receivers to expected physical behavior, the *PNT Integrity Library* refers to the techniques in this approach as “model-based consistency checks”.

Table 6. Example resilience techniques to detect spoofing by monitoring PNT solutions and other internal observables for physical consistency.

Technique	Description	References
Stationary Position Monitor/ Static-Position Check	Monitor position solutions for abnormal behavior. Stationary equipment will have a constant position solution, with some deviation due to noise.	[50] [51]
Stationary Velocity Monitor	Monitor velocity solutions for abnormal behavior. Stationary equipment will have a constant zero velocity solution, with some deviation due to noise.	[50]
Position-Velocity Consistency Check	Estimate the velocity from the position solution and compare it to the velocity solution.	[51]
Clock Rate Monitor/ Clock-Jump Check	Compare the measured clock drift with the expected drift from a model and check if it is within reasonable bounds.	[50] [51]
Clock Consistency Divergence (CCD) Monitor	Over a period of time, monitor the change in clock bias and compare the findings to the integral of the clock bias rate. A large difference between the two values may indicate a spoofer is pulling away the timing solution.	[50]
Look for unexpected changes in signal observables	Look for jumps in signal observables such as the carrier amplitude, beat carrier phase, or code phase.	[26]
Linear time check	Check that absolute time increments linearly. For example, if the date moves backwards, it can indicate a GNSS data spoofing attack or a GNSS receiver software fault during a routine week number rollover.	[52] [53]

A.3.3 Monitor Power Measurements

This approach attempts to detect spoofing or jamming by monitoring the power at different points in the system. Changes in power can indicate jamming or spoofing. For example, a power increase in one channel in a GNSS receiver while all other channels had consistent power may indicate a spoofer. If all channels measure a power increase, jamming is likely occurring. The examples in Table 6 apply to different power measurements within a GNSS receiver. However, similar methods can be developed for any type of PNT technology that transmits, receives, and processes RF signals.

Table 7. Example resilience techniques to detect jamming and/or spoofing by monitoring power measurements.

Technique	Description	References
Received Power Monitor (RPM) / AGC monitor	Look for changes in the total power input to the receiver using the AGC setpoint.	[26] [51]
C/N_0 monitor	Look for changes to the ratio of the carrier power to the noise floor (C/N_0).	[46] [50]
Absolute Power Monitor (APM)	Determine if a monitor finds signals that are too strong to have come from a GNSS constellation.	[46]
L1/L2 Power Comparison	Measure and compare the L1 and L2 band power. A spoofer may not cover both signals.	[46]
Power variation vs. receiver movement	Look for changes in received power that correlate with receiver movement due to proximity to spoofer.	[46]

A.3.4 Monitor the Direction of Arrival of Signals

PNT UE systems that can measure the direction of arrival of different signals can use this information to infer which signals may be untrustworthy. Multiple signals arriving from the same direction may be manipulated signals form a spoofer with a single transmitter. Precise spatial discrimination can be used to verify that signals are coming from an expected direction, such as known GNSS satellite locations. Table 8 gives one example technique for this approach.

Table 8. Example resilience techniques to detect spoofing by monitoring the direction of incoming signals.

Technique	Description	References
Angle of Arrival (AOA) or **Direction of Arrival (DOA)**	Find the phase difference of arrival between different elements to find the direction of the received signal -- essentially beam-steering in reverse. Compare the direction of arrival of each signal. Multiple signals coming from the same direction could indicate a spoofer with a single transmitter.	[26] [34] [46] [51] [55]

A.3.5 Monitor for Duplicate or Extra Signals

Duplicate or extra signals may indicate a spoofer is attempting to deceive a GNSS receiver using false signals. Typically, false signals have slightly higher power than true signals to draw the GNSS receiver tracking loops away. Table 9 gives two example techniques to find the vestigial signals. Similar methods to search for duplicate or extra signals may apply to different PNT technology types that process RF transmissions.

Table 9. Example resilience techniques to detect spoofing by searching for duplicate or extra signals.

Technique	Description	References
Multiple Peak Monitor or **Vestigial Signal Detection** or **Acquisition Check**	Search for multiple signal peaks in a single Cross-Ambiguity Function (CAF) and compare the peak power to a threshold to assess the likelihood of jamming or spoofing.	[46] [51] [54]
Re-acquisition Search Sequence	Perform a brute-force acquisition search for new peaks. Even after satellites have been acquired, they may find authentic peaks if tracking loops have been dragged off.	[26]

A.3.6 Monitor for Interactions Between Signals

Systems can detect similar signals by searching for characteristics of interference. When GNSS receivers are spoofed, the false signal may be very close to or identical to the true signal for a certain period as the spoofer captures the receiver tracking loops and smoothly drags them off to a false position and/or time fix. Table 10 gives a few examples of resilience techniques to detect spoofing characteristics during drag-off.

Table 10. Example resilience techniques to detect spoofing by looking for interactions between the true and spoofed signals.

Technique	Description	References
Distortion monitor	Look for distortions in the complex autocorrelation function caused by interaction between false and authentic signals. These distortions can be observed in a plot of code offset, in-phase accumulation, and quadrature accumulation.	[26]
Signal Quality Monitor (SQM)	For tracking receivers working in the line-of-sight condition, use the ratio and delta SQM tests to detect abnormalities in GPS correlation peaks caused by spoofing.	[46]
Distribution analysis of correlator output	In line-of-sight conditions, the correlator output power for a tracking receiver approximately follows a Chi-squared distribution. Analyze the distribution for perturbations that may indicate fluctuations caused by the interaction between the fake and authentic signals during drag-off.	[46]

A.3.7 Authenticate External Input to Verify Integrity

PNT UE systems with an authentication capability can verify the authenticity of the input information to ensure that it comes from a trusted source. In GNSS, while system designers can consider a number of authentication techniques [56], major operational systems such as GPS and Galileo are developing authentication capabilities that involve Navigation Message Authentication (NMA).

Galileo uses Open Service Navigation Message Authentication (OSNMA) based on the Timed Efficient Stream Loss-Tolerant Authentication (TESLA) protocol [18]. It digitally signs the Open

Service Navigation message in the E1 band, making use of 40 reserved bits (“Reserved 1”) in the Galileo E1B data message (I/NAV).

GPS adopts Chips-Message Robust Authentication (Chimera), a hybrid NMA and spreading code authentication technique proposed for use with the GPS L1C signal [39]. The NMA portion of this scheme is based on a well-established standard, and therefore simplifies the integration of the scheme into existing GNSS receivers.

Table 11. Example resilience techniques to authenticate external input.

Technique	Description	References
Navigation Message Authentication	Authenticate encrypted navigation messages using a key that is obtained separately, such as through a delayed broadcast. PNT information from signals with authenticated navigation messages has higher integrity.	[18] [39]

A.3.8 Cross-Verify Between PNT Sources

PNT UE systems should verify each PNT source they use independently. They can also compare PNT state information from each PNT source to the others and to the combined system PNT solution to find outlier sources, which may indicate interference. However, this process requires PNT state information from a sufficient number of sources to successfully identify incorrect PNT information when findings disagree.

Table 12. Example resilience techniques to cross-verify between PNT sources.

Technique	Description	References
Receiver Autonomous Integrity Monitoring (RAIM) and variants	Detect and reject outliers by identifying large residuals between individual measurements and the combined solution from all measurements. This is commonly used with measurements from redundant GNSS satellites. The RAIM concept has many variants.	[34] [46] [57]
Sensor-Agnostic All-source Residual Monitoring (SAARM)	For an all-source sensor management system, determine when corruption is present by detecting any general mismatches between the model and measurements associated with a particular sensor.	[57] [58]
Cumulative Innovations Monitor	Detect measurement faults, which may indicate GNSS receiver spoofing, using Extended Kalman filters (EKFs) that monitor innovations over time in tightly coupled multisensor navigation systems, such as INS/GNSS. A bank of cumulative innovations monitors can be used to improve detection of slowly accumulating measurement faults compared to a single cumulative monitor.	[59] [60]

A.4 Isolate Components

Many PNT UE system architectures use multiple PNT sources; for example, the Level 2 PNT UE system architecture instance in Figure 9 of Section 4.3 uses a GNSS receiver to steer a local clock. This arrangement gives a time solution that takes advantage of both the good short-term stability from the local clock and the good long-term stability of GNSS. However, attackers can spoof GNSS receivers by transmitting fake signals that are manipulated to provide false information, and the manipulated information can propagate to steer the local clock incorrectly. When the PNT UE system detects atypical errors in the GNSS signal, which can indicate spoofing, it can cut off the steering to contain the corruption, but manipulated information may have had the opportunity to propagate and contribute to steering the local clock before it was detected. Isolating PNT sources from each other prevents atypical errors in one PNT source from affecting the others. Protecting the local clock from the effects of external input by isolating it completely produces greater resilience. One way to completely isolate the local clock or other internal physical PNT source is to allow it to free run indefinitely after a secure initialization period.

Table 13. Example resilience techniques to implement isolation in PNT UE systems.

Technique	Description	References
Dynamic PNT solution isolation	Isolate PNT solutions when atypical errors are detected to contain the effects of threats and disruptions. For example, stop disciplining internal physical PNT sources using GNSS PNT information if a GNSS threat is detected.	[5] [17]
Predefined PNT solution isolation	Isolate PNT solutions from different PNT sources from each other to prevent atypical errors from spreading regardless of detection capabilities. For example, allow internal physical PNT sources to free run after initial calibration, without disciplining, to prevent corruption from untrusted external influence. Drift can be corrected by different methods to synthesize PNT information from different PNT sources (see Table 14).	[5] [17]
Lateral isolation	Implement lateral isolation to prevent attacks and disruptions that affect one PNT source from corrupting other PNT sources. For example, threats that affect internal stored data, such as data spoofing, should be blocked from lateral movement that would allow them to affect other PNT sources, such as through shared memory allocation. M	[15] [52] [61]

PNT UE systems can use a synthesizer to take advantage of the combined solution from both an isolated local clock and GNSS, while keeping both PNT sources isolated. For example, a free-running local clock can drive a signal generator and receive corrections for the drift from the GNSS time solution, as discussed with the Level 3 or 4 architecture instance example in Figure 10 from Section 4.4.

More complex systems may incorporate multiple PNT sources for positioning and navigation solutions in addition to the timing-only solution from the examples in Section 4.0. A common technique is to utilize INSs in conjunction with GNSS to improve performance in contested environments [27]. The sources can be fully isolated or can provide input to one another in loosely coupled or tightly coupled configurations or even be deeply integrated with one another. The benefits and tradeoffs between these architectures [28] are briefly summarized below.

Loosely coupled systems incorporate an external Kalman filter that integrates the output of the GNSS receiver with data from the INS. This level of coupling reduces GNSS acquisition times and enables continued operations in the event that GNSS signals become unavailable. At the same time, this configuration maintains separate systems that can be used to produce isolated and independent PNT solutions. Tightly coupled systems utilize the raw GNSS measurements in conjunction with output from the INS to produce system PNT solutions. This introduces additional performance benefits such as reducing the bandwidth of GNSS tracking loops and maintaining PNT services under high dynamics. System designers can build tightly coupled systems that maintain separate independent sources by introducing more complexity into the system [62]. Under certain use cases it may be worthwhile to increase system cost and complexity to achieve source isolation for more resilient UE.

Many other methods can keep multiple PNT sources isolated while combining their solutions to produce the system PNT solution. Table 14 gives several examples. Note that system designers should implement techniques from the Verify resilience technique category (Appendix A.3) on source PNT solutions before using them to synthesize the system PNT solution.

Table 14. Example resilience techniques to synthesize system PNT solutions by combining the PNT solutions from different PNT sources.

Technique	Description	References
Use a Hardware Synthesizer	Drive a signal generator using an isolated free-running local clock. Apply corrections to the synthesized signal using input from other PNT sources that receive external input.	[17]
Kalman Filter Ensemble	Use a Kalman filter to recursively cycle state prediction and correction and form a weighted average ensemble solution.	[63]
Real-time Validation for Plug-and-play Sensors (RVPS)	Use the Kalman-Schmidt filter formulation to execute a “partial update” and provide sensitive fault detection for sensor model validation while protecting the ongoing navigation solution by using a single-filter architecture.	[57]
Modular Sensor Fusion	Use tightly coupled sensor fusion algorithms with different isolated sensor modules that have independent mathematical models.	[62]

A.5 Mitigate the Effects of Threats

PNT UE systems can respond in several ways when they detect threats and other anomalies using resilience techniques from the Verify category such as the examples given in Section A.3. One appropriate response is to stop relying on any output from the compromised PNT source. If the PNT UE system includes other PNT sources, it can use them to provide the system PNT solution to the user during the period when the PNT source with the detected threat remains compromised. The PNT UE system can include control logic to automatically recover the performance of the compromised PNT source when it is safe to do so.

Another way to respond to threat detection is to mitigate the effects of the threat and recover true PNT information. For example, when a GNSS receiver is spoofed, the PNT UE system can use different techniques to separate the true GNSS signals from the false signals and continue tracking the true signals to produce a PNT solution. Table 15 lists example resilience techniques and associated references. Note that these mitigations can be considered broadly applicable because they focus on finding and tracking the true signals, which have specific, recognizable characteristics, regardless of any false signals that are present.

Mitigations, like the techniques in the Verify category, have limitations that must be well understood when designing resilient PNT UE systems. Coordinated attackers may find ways to better mimic the characteristics of the true signals. Although true signals may be present, they may not be detected or correctly identified. Due to these limitations, PNT UE systems should not rely solely on resilience techniques from the Mitigate category to produce resilient behaviors. Instead, system designers should layer mitigations along with other resilience techniques to produce overall resilient PNT UE systems.

Table 15. Example resilience techniques to mitigate the effects of threats by recovering true signals.

Technique	Description	References
Signal Polarization Separation	Measure the polarization of incoming signals to separate true GNSS signals, which have right-hand circular polarization, from spoofed signals, which are typically linearly polarized. Even spoofed signals with circular polarization can be excluded because the low elevation angle of the spoofer deforms the polarization.	[64]
Track Multiple Correlation Peaks	When spoofing is detected, use auxiliary tracking channels to search for secondary correlation peaks in the time-frequency domain and track the true signals.	[65] [66] [67]
Mitigate using Multiple Receivers	Spoofed signals from a single transmitter propagate along an identical path, whereas true GNSS signals from different satellites propagate along different paths. With multiple receiver locations, the PNT UE system can use these path differences to identify and eliminate information from spoofed signals.	[68] [69]

A.6 Diversify Technologies

System designers can increase the number of PNT sources with diverse technology types to reduce common mode failures in the PNT UE system. Resilience techniques from the Diversify category can make it possible to withstand disruptions to one PNT source with low impact or no impact on system performance. Further, PNT UE systems can use cross-verification between multiple sources as an additional check after the PNT state information from each source is verified independently. Table 16 gives some example resilience techniques from the Diversify category. However, it is important to note that each additional PNT source introduces unique verification challenges and new failure modes and therefore requires additional verification, isolation, mitigation, etc. In addition to increasing the system complexity for each new technology type added, system designers face the overall problem of how to combine the PNT information from the different PNT sources to produce a unified system PNT solution. Section A.4 described techniques to address this.

Table 16. Example resilience techniques to diversify PNT sources to reduce common mode failures.

Technique	Description	References
Spatial Diversity of Antenna Elements	Use multiple distinct antennas (spatial diversity) to identify the direction of incoming external signals (spatial processing) from interferometric methods, such as Angle of Arrival (AOA) techniques.	[26] [34] [46] [51] [55]
Diversify GPS signals	Use GPS signal diversity to increase the reliability of the GPS PNT solution.	[9]
Multi-GNSS	Use PNT solutions from different kinds of GNSS systems.	[70]
Diversify PNT sources	Use different types of PNT sources to avoid common mode failures.	[71] [72] [73]

A.7 Recover Performance

Ideally, resilient PNT UE could withstand threats, disruptions, or other types of interference by continuing to provide the system PNT solution with no or with only minimal performance degradation. However, this is not always possible. Whether or not the PNT UE system can withstand the threat or disruption, it should at a minimum be able to recover to a proper working state, or typical performance, after the disruption has passed. Therefore, system recovery serves as the foundation of resilient behavior.

Recovery incorporates the different processes needed to return to a proper working state, or typical PNT UE system performance, regardless of the effects on the system caused by threats and other disruptions. Specific examples of these processes include re-acquiring signals, the ability to reset, or roll back information stored to memory, and the ability to reload or update firmware. The user can initiate recovery manually or the internal logic of the PNT UE system can instigate it automatically. System designers can add other types of recovery as they build more capabilities into the PNT UE system. Table 17 gives some example resilience techniques from the Recovery category.

PNT UE systems can employ mitigation techniques from Section A.5 to recover true signals in the presence of a threat. Some degree of performance may also be recovered during a threat or disruption by using the unaffected PNT sources to generate the system PNT solution if the system includes multiple PNT sources. However, PNT UE systems may need to delay other types of recovery to typical system routines until the threat or disruption is no longer in effect.

Recovery processes can be initiated in different ways. The user may recognize a problem when the system is incapable of functioning or may receive PNT SA about threats from separate user devices or communication channels. Some PNT UE systems may be designed to report the outcomes from different techniques in the Verify category to the user to support recovery decisions. The system may also use outcomes from verification techniques to initiate automatic recovery processes.

Table 17. Example resilience techniques for recovery.

Technique	Description	References
Manual Recovery by Reset or Reload	Perform a reset to roll back to or restore a previous good state, to re-initialize with "factory settings", to clear memory with stored information from external input, reload firmware, etc.	[5]
Automatic Recovery	Automatically recover from data corruptions or other error states.	[74]
Fault-Tolerant Concepts	Apply methods to detect and recover from a fault that is happening or has already happened in the software or hardware in the system to provide service in accordance with the specification.	[75]

A.8 Resilience techniques That Fit Multiple Categories

The seven categories discussed in this appendix provide a framework for exploring methods that system designers can implement to achieve resilient behavior in PNT UE systems. This categorization borrows from other resilience frameworks and suggests new avenues for innovation. However, these techniques should not constrain innovation by prescribing categories into which a new method must fit. The categories presented in this appendix do not represent canned solutions to achieve resilience and are not necessarily mutually exclusive. Some techniques defy simple categorization, and some techniques are only enabled by the implementation of other techniques. To demonstrate the overlapping nature of some resilience technique categories, this section presents techniques that fit into multiple categories and includes a list of examples in Table 18.

Section A.2 described processes for limiting the time during which a PNT UE system is vulnerable to threats through external input by using a local timing source that operates in holdover mode between GNSS disciplining periods. The system is not susceptible to jamming or spoofing during intervals between disciplining periods, when the clock is allowed to free run. If disciplining occurs at predictable intervals, an adversary may choose an optimal time to spoof the PNT UE system. Randomizing the holdover period is a form of obfuscation made possible by the implementation of other resilience technique principles. It forces the attacker to operate constantly, which increases the probability of detection. Similarly, NMA methods for Galileo (TESLA, implemented) and GPS (Chimera, proposed) use encryption to obfuscate the navigation message in the GNSS signal. The navigation message can be authenticated using the appropriate key as a way to verify the integrity of the signal.

Additionally, using a diverse set of isolated PNT sources allows monitoring and detection of threats. Disagreement between PNT solutions may indicate the presence of a spoofer when the system architecture implements a solution separation monitor. A PNT Solution Synthesis Agent can then mitigate the impact of spoofing on the system by removing the corrupted output of the GNSS receiver from the overall PNT solution and relying only on verified sources until the threat is removed.

Table 18. Example resilience techniques that fit multiple categories.

Technique	Description	Categories	References
Randomize Holdover Periods	Use GNSS signals to discipline the internal clock at random intervals to limit vulnerability to external threats and obfuscate time interval in which spoofing should occur.	Limit and Obfuscate	[43]
Navigation Message Authentication (NMA)	Authenticate encrypted navigation messages using a key that is obtained separately, such as through a delayed broadcast. PNT information from signals with authenticated navigation messages has higher integrity.	Verify and Obfuscate	[18] [39]
Solution Separation Monitor	Compare information coupled to GNSS to information from an isolated physical source, such as an INS or local clock, to detect spoofing.	Diversify, Isolate, Verify, and Mitigate	[76]
Spatial Processing	For radiated signals, spatial diversity of receiver elements can be used with interferometry to determine the direction of incoming radiation. Signals coming from expected directions can be verified using this method (example: AOA). Signals that are not coming from expected directions can be limited using beam steering (example: anti-jam antennas)	Verify, Diversify, Limit	[14] [26] [34] [44] [46] [51] [55]

APPENDIX B: PNT THREATS AND DISRUPTIONS

There are many kinds of threats and disruptions that can affect the transmission of PNT signals. Interference may be caused by malicious attacks, unintentional RF transmissions and reflections, and natural events. The impact on the PNT UE depends on the power, proximity, and type of interference transmitter. Legitimate signals can be blocked by buildings or natural structures or can include errors when incorrect information is uploaded from control segments. Signals carried on RF transmissions or wired connections can be manipulated, degraded, or blocked before they reach the PNT UE.

Figure 15 shows a diagram of some of the threats and disruptions that can affect GNSS signals. Other satellite-based systems will face similar threats and disruptions. In the diagram, a GNSS satellite transmits a legitimate GNSS signal, which is received by the antenna of a GNSS receiver. The legitimate GNSS signal may be degraded or entirely denied by targeted jamming, or unintentional interference from adjacent band or accidental in-band RF transmission. Buildings, trees, and other structures can also block GNSS signals from reaching the GNSS receiver, or reflect legitimate signals, causing multipath. Attackers can also use different kinds of measurement and data spoofing to generate manipulated GNSS signals meant to deceive targeted receivers [52] [77]. The quality of the manipulated GNSS signal depends on the attacker's equipment complexity and knowledge of the target receiver, including the antenna location and the type and quality of mitigations. Spoofing attacks can range from simple repeaters of genuine GNSS signals, called meaconers, to sophisticated coordinated attacks that produce false signals targeted to a specific receiver [26] [34] [46] [47] [48]. Natural events can also degrade GNSS signals, such as solar activity that affects the ionosphere, which the signals travel through. An unprepared GNSS receiver may even be disrupted by a routine, scheduled event, such as a leap second, or week number rollover. There can also be errors in the PNT information uploaded to the GNSS satellite by the GNSS ground control station [78] [79].

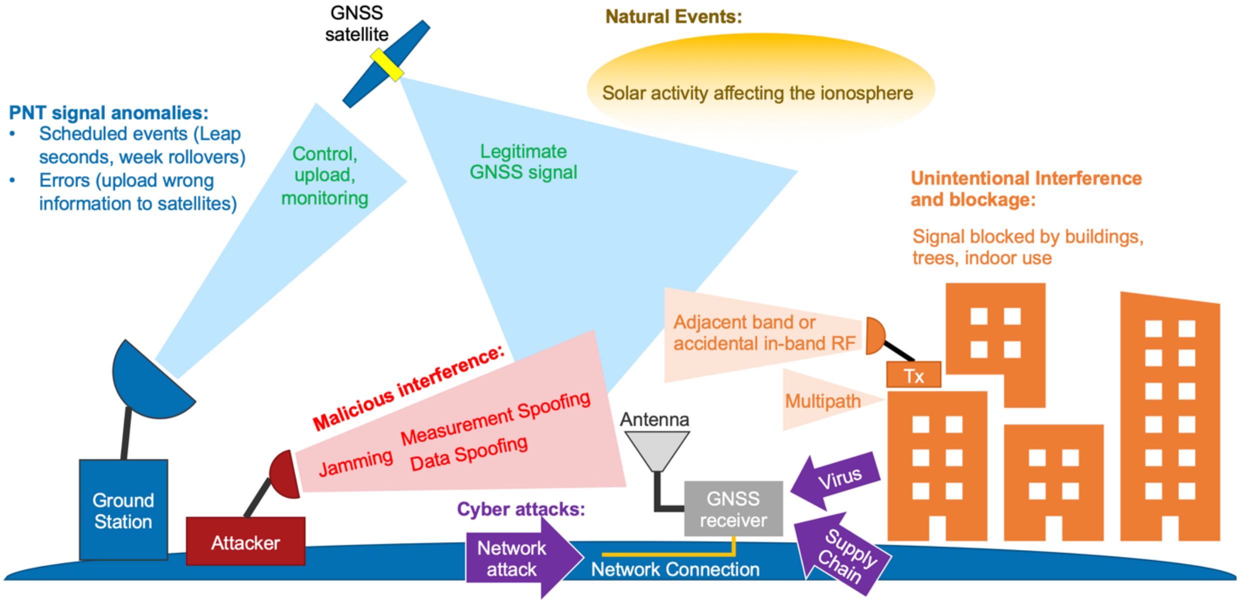

GNSS satellite
Natural Events:
Solar activity affecting the ionosphere
PNT signal anomalies:
• Scheduled events (Leap seconds, week rollovers)
• Errors (upload wrong information to satellites)
Control, upload, monitoring
Legitimate GNSS signal
Unintentional Interference and blockage:
Signal blocked by buildings, trees, indoor use
Adjacent band or accidental in-band RF
Tx
Multipath
Malicious interference:
Measurement Spoofing
Jamming
Data Spoofing
Antenna
GNSS receiver
Virus
Supply Chain
Cyber attacks:
Network attack
Network Connection
Ground Station
Attacker

Figure 15. Diagram of threats and disruptions for GNSS signals [10].

Signals radiated by terrestrial sources can encounter many of the same sources of interference and disruption, including blockage or reflection from buildings, intentional jamming or spoofing, and unintentional interference from other transmitters. Signals transmitted through wired connections, communication networks such as cellular 4G/5G, or other physical links can be disrupted if the transmission medium is cut or interfered with, either by a natural disaster, accidental incursion, or intentional sabotage. Terrestrial beacons or wired networks that rely on PNT sources to provide the PNT information distributed on the network are also still susceptible to the threats and hazards that can disrupt those sources at their dispersed locations. While threats local to the PNT UE system can be mitigated by the network, threats that affect the distributed PNT sources must be addressed appropriately.

In addition to PNT-specific threats and disruptions, system designers should also consider general problems associated with electronic and manufactured UE. This includes supply chain issues, power supply disruptions, and the potential for user error. Cyber-attacks, including viruses and other types of cyber threats, may access the PNT UE system through a network connection or the manufacturing supply chain. Different types of weather or other use cases that can affect the physical security of the PNT UE can also be hazards.

APPENDIX C: PNT UE BOUNDARIES

The object of PNT UE is to provide a PNT solution output to the user. In this context, it is important to understand the outer boundary of PNT UE that defines the equipment for which resilience behaviors are evaluated. A user can be a person, an application, or another component in a system. The CF [1] defined three recursive PNT UE boundaries over which PNT resilience can be evaluated to determine if it meets different types of user needs.

The three recursive PNT UE boundaries defined in the CF [1] are:

- **Fundamental PNT measurements** (for example, a GNSS chipset or an atomic clock).
- **PNT integrated receiver** (for example, an integrated GNSS receiver that includes a GNSS chipset, PNT processor, and local clock or oscillator).
- **PNT system of systems** (for example, a system that includes an integrated GNSS receiver, an anti-jamming antenna, and any other connected devices used to deliver PNT data).

As indicated by the examples, each successive boundary can be a user of the PNT UE defined by the previous boundary. Figure 16 shows each of the boundaries from Figure 1 in the CF [1] together on one diagram. Different types of PNT resilience techniques may be more applicable for PNT UE with different boundaries [5].

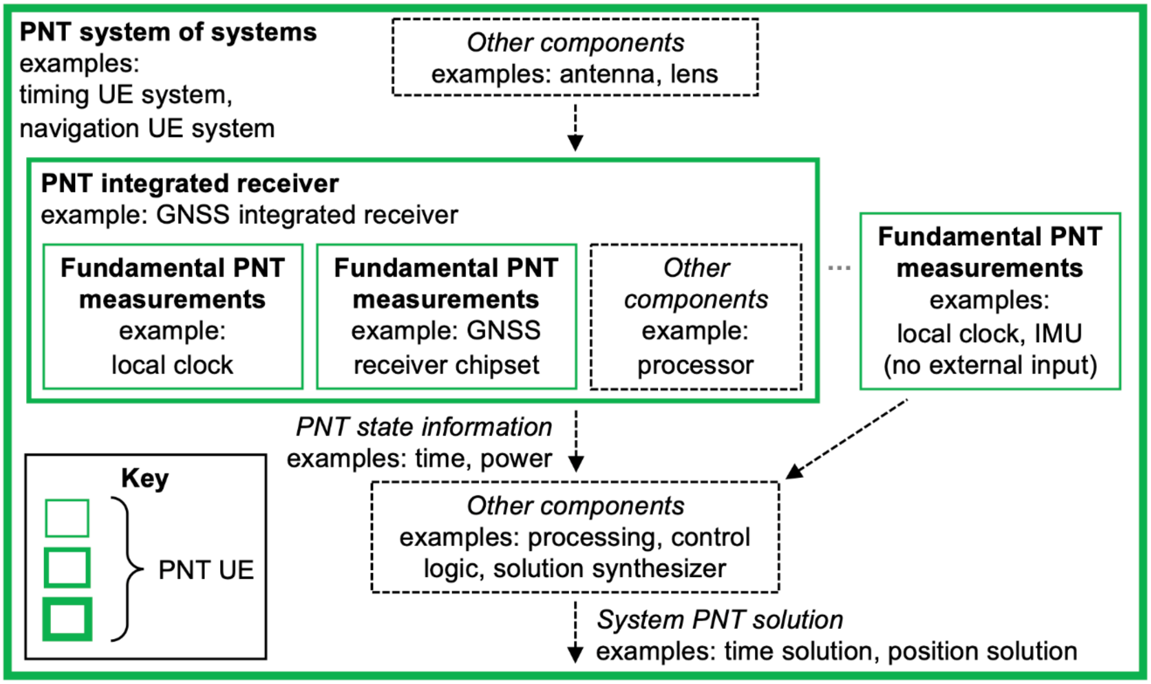


Figure 16. Recursive PNT UE boundaries for fundamental PNT measurements, integrated PNT receivers, and PNT system of systems.

The CF [1] defined a PNT source as a PNT UE system component that is used to produce a PNT solution. This definition was reviewed in Section 2.1 and three PNT sources were included in the diagram of a generic PNT UE system in Figure 2. In Figure 16, fundamental PNT measurements from a GNSS receiver chipset and a local clock are PNT sources for a GNSS integrated receiver. In turn, the GNSS integrated receiver becomes a PNT source for the PNT system of systems, along with other fundamental PNT measurements or other PNT integrated receivers.

The resilience level can be evaluated over each green PNT UE boundary in Figure 16. PNT UE systems may contain subcomponents that are PNT UE with different resilience levels than the overall system. One possible arrangement of resilience levels would be:

1. **Level 1** resilience provided by a *fundamental PNT measurement,* such as a GNSS chipset that can be recovered when commanded by a higher-level system user.
2. **Level 2** resilience from a *PNT integrated receiver* that contains a Level 1 GNSS chipset and a local clock. When a threat impacts the GNSS chipset, this GNSS integrated receiver can use the local clock for holdover with unbounded degradation due to drift.
3. **Level 3** resilience for a *PNT system of systems* that combines a Level 2 PNT integrated receiver and at least one other PNT source to provide corrections for the clock drift during holdover. For the Level 3 performance requirement, the system PNT solution with the clock drift corrections may be degraded compared to typical performance when the GNSS chipset PNT information is used.
4. **Level 4** resilience achieved by a *PNT system of systems* with sufficient PNT source technology diversity and quality to maintain typical performance in the presence of a threat. This may be realized by a PNT UE system that includes Level 3, Level 2, and Level 1 PNT sources, which may be fundamental PNT measurements or PNT integrated receivers.

A PNT source is contained within the boundary of PNT UE, while PNT infrastructure and external input are outside the boundary. There are a large variety of PNT sources that can be included in a PNT UE system. Some PNT sources require external input, which may be manufactured signals provided by PNT infrastructure or naturally occurring physical phenomena. External input can be received as radiated signals or phenomena or over a wired connection. Some PNT sources even transmit information, so the external interface passes information both in and out. Each of these PNT source types may also utilized additional supporting information shared through a different method. The boundary around a PNT source is important for defining external input and the boundary over which PNT UE resilience is evaluated.

This appendix summarizes different kinds of PNT sources and corresponding important boundaries by identifying five general examples of different PNT source types. Each type of PNT source is described below with a figure that shows some general components which may be included in the PNT source. A boundary in each figure shows the separation between the PNT source and any external elements that it relies on, such as external input generated by PNT infrastructure or external physical phenomena.

PNT source types:

1. **Internal physical PNT source**
   An internal physical PNT source uses a sensor to measure local physical phenomena, as shown in Figure 17 [81]. Since the physical phenomena is occurring inside the PNT source, it is internal to the PNT UE system and does not require external input.

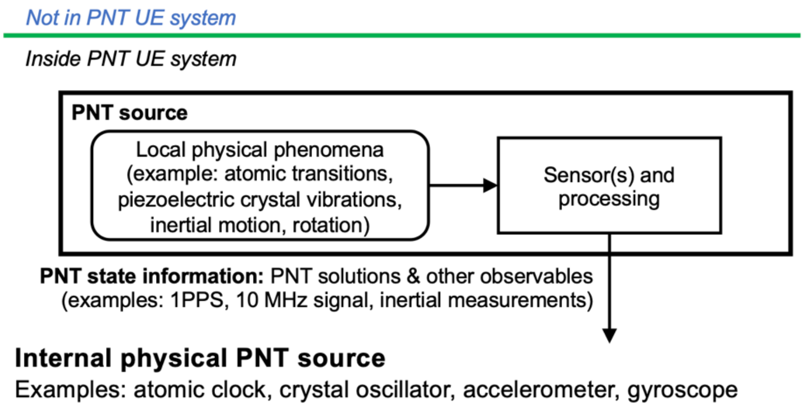

Not in PNT UE system
Inside PNT UE system
PNT source
Local physical phenomena (example: atomic transitions, piezoelectric crystal vibrations, inertial motion, rotation)
Sensor(s) and processing
PNT state information: PNT solutions & other observables (examples: 1PPS, 10 MHz signal, inertial measurements)
Internal physical PNT source
Examples: atomic clock, crystal oscillator, accelerometer, gyroscope

Figure 17. General components of an internal physical PNT source.

Examples of internal physical PNT sources include different types of local clocks, such as rubidium or cesium atomic clocks and crystal oscillators. The physical phenomenon measured in a crystal oscillator is the resonant vibration of a piece of piezoelectric material. In rubidium or cesium atomic clocks, the measured physical phenomenon is the hyperfine atomic transition frequency. For position and navigation, the sensors in INS and IMU systems include accelerometers, to measure inertial motion, and gyroscopes, to measure rotation. With these measurements, the system can calculate the current position, velocity, and orientation based on a known starting point through dead reckoning.

Although internal physical PNT sources do not require external input during typical operation, they do need an initial setup and calibration. For example, frequencies must be tuned and stabilized. Absolute position and time can be calculated from relative position and time measurements if there is a known starting point.

2. **PNT source using external physical phenomena**
   Instead of measuring internal physical phenomena, PNT sources can measure the effects of external physical phenomena that propagate to the system and can be received as external input, as shown in Figure 18 [81]. For example, a compass can use the Earth’s magnetic field to determine the direction of the north magnetic pole. Since this type of PNT source receives natural external input, it doesn’t necessarily require PNT infrastructure. However, the natural external input can still be denied, degraded, or manipulated by attacks or natural hazards, so this type of PNT source does not have the same inherent integrity as internal physical PNT sources.

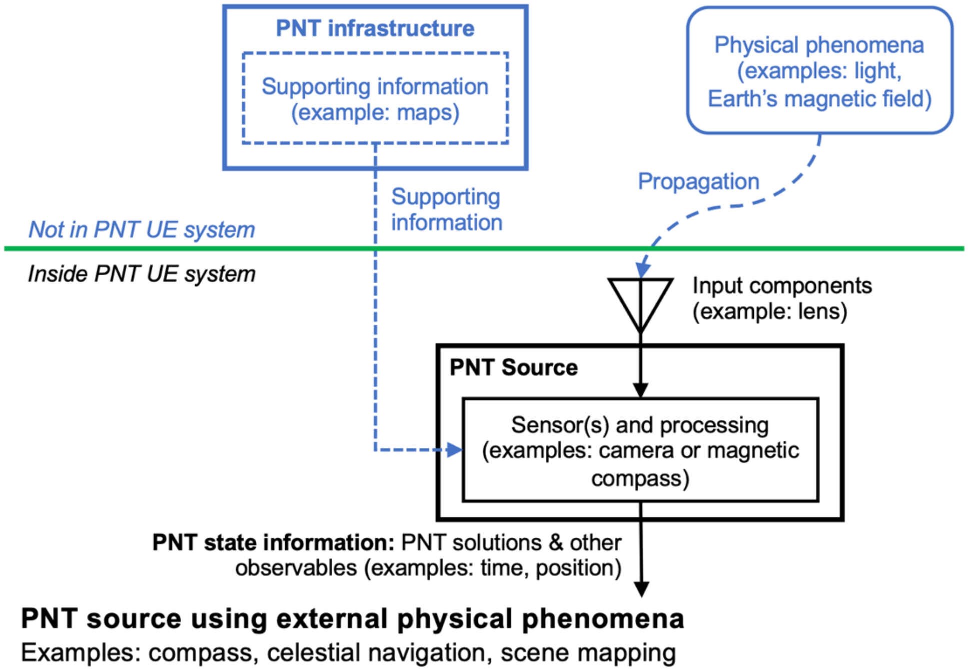

PNT infrastructure
Supporting information (example: maps)
Physical phenomena (examples: light, Earth's magnetic field)
Propagation
Supporting information
Not in PNT UE system
Inside PNT UE system
Input components (example: lens)
PNT Source
Sensor(s) and processing (examples: camera or magnetic compass)
PNT state information: PNT solutions & other observables (examples: time, position)
PNT source using external physical phenomena
Examples: compass, celestial navigation, scene mapping

Figure 18. General components of a PNT source that uses external physical phenomena.

Supporting information may be supplied by PNT infrastructure to aid in the setup or calibration of PNT information coming from PNT sources using external physical phenomena. For example, star maps can be downloaded and used to orient the system using image recognition algorithms and the collected starlight from a camera. Some PNT sources of this type will rely on supporting information more than others.

3. **PNT signal receiver**
   A PNT signal receiver collects PNT signals manufactured by PNT infrastructure and processes them to produce PNT information. Manufactured signals can carry several layers of information that are deciphered by signal processing in the PNT source. Producing the manufactured PNT signals and distributing them over a designated area can required substantial PNT infrastructure. Figure 19 shows some general components that can be included in the PNT infrastructure outside the PNT UE and the PNT source inside the PNT UE [81]. GNSS and other types of space based PNT systems have satellites to transmit signals towards the Earth and ground stations to monitor and control the satellites [12]. Ground-based PNT systems can use beacons to transmit manufactured signals, also supported by monitoring and control components. Each of these types of PNT infrastructure may also have different ways to distribute supporting information, such as satellite ephemeris information or encryption keys.

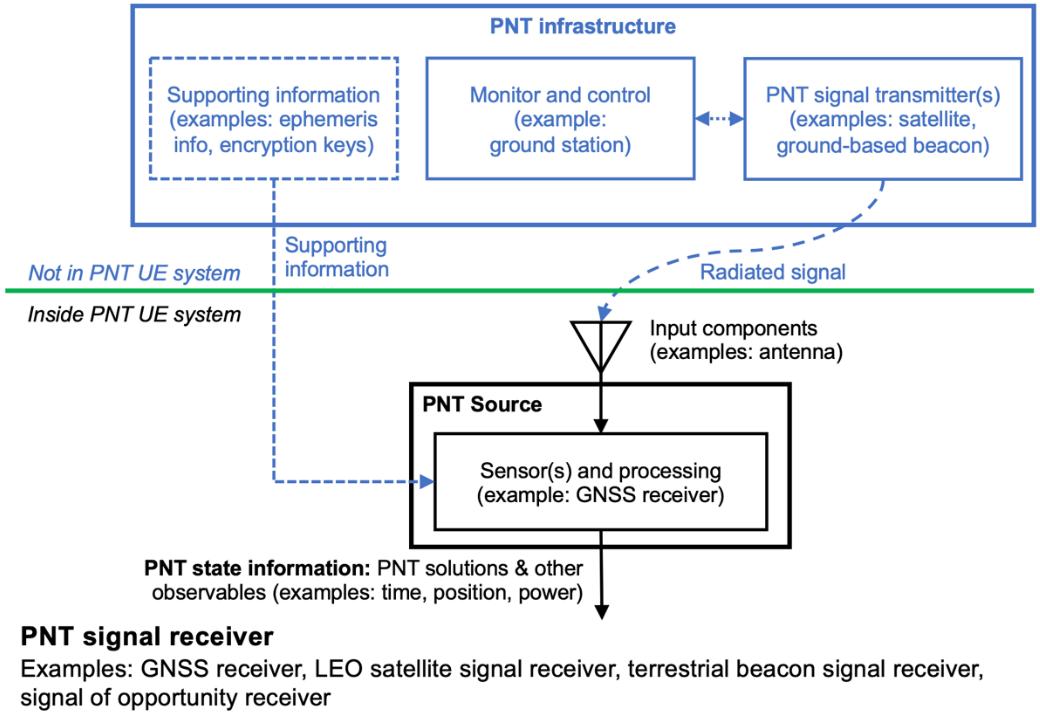

PNT infrastructure
Supporting information (examples: ephemeris info, encryption keys)
Monitor and control (example: ground station)
PNT signal transmitter(s) (examples: satellite, ground-based beacon)
Supporting information
Radiated signal
Not in PNT UE system
Inside PNT UE system
Input components (examples: antenna)
PNT Source
Sensor(s) and processing (example: GNSS receiver)
PNT state information: PNT solutions & other observables (examples: time, position, power)
PNT signal receiver
Examples: GNSS receiver, LEO satellite signal receiver, terrestrial beacon signal receiver, signal of opportunity receiver

Figure 19. General components of a PNT source that receives radiated PNT signals.

PNT signal receivers depend on received external input to produce PNT information. Manufactured PNT signals can be fabricated with false information to attempt to deceive PNT signal receivers. Threats and hazards can also deny or degrade the radiated PNT signal before it reaches the receiver in the PNT source.

4. **Wired network timing service customer**
Instead of receiving radiated PNT signals, a PNT source can receive PNT information through a physical link connected to a network. This type of PNT source is likely to only be used for stationary timing applications since it is impractical for moving PNT UE systems to be attached to cables. Different types of cable materials, network protocols, and reference clocks can be used for the PNT infrastructure to support this type of PNT source. Figure 20 shows a general diagram of this PNT source type and the PNT infrastructure network that supports it from outside the PNT UE system. One example would be the time over optical fiber method, which can use White Rabbit protocols to provide calibrated links to UTC(NIST) over long distance optical fiber cables [19]. Different types of networks could use ethernet or other wire cables for the physical link or different types of protocols, such as Network Time Protocol (NTP) or Precision Time Protocol (PTP) [80].

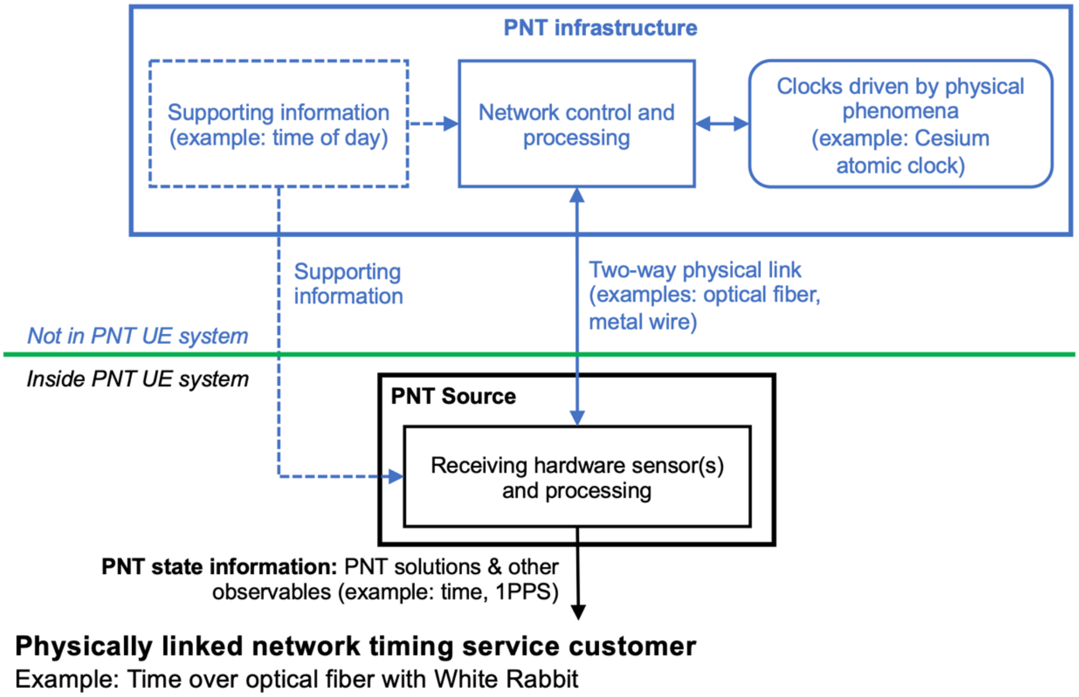

PNT infrastructure
Supporting information (example: time of day)
Network control and processing
Clocks driven by physical phenomena (example: Cesium atomic clock)
Supporting information
Two-way physical link (examples: optical fiber, metal wire)
Not in PNT UE system
Inside PNT UE system
PNT Source
Receiving hardware sensor(s) and processing
PNT state information: PNT solutions & other observables (example: time, 1PPS)
Physically linked network timing service customer
Example: Time over optical fiber with White Rabbit

Figure 20. General components of a PNT source that uses a physically linked network timing service.

PNT sources that use a physical link to connect to external input are unaffected by RF interference, but they are susceptible to damage to the transmission medium, which can be cut by accidental incursion or intentional sabotage. Installing and maintaining the physical link is an important cost and convenience consideration for this type of PNT source. Further, the quality of the time servers within the network, cable calibrations, cable materials, and protocol precision affects the accuracy of the PNT information that this type of PNT source can provide.

5. PNT source with a transmitter

Another type of PNT source both transmits and receives PNT signals. This type of PNT source controls a transmitted signal and can use the reflected and received signal to determine the range to the reflection point. Examples of this type of PNT source include radar [24], LiDAR [31], and sonar devices. Radar uses RF signals, LiDAR uses laser light, and sonar uses sound to find the range to reflecting surfaces. Sonar signals are usually transmitted in water and are useful in maritime applications. Figure 21 shows the general components for this type of PNT source and the supporting elements located outside the PNT UE.

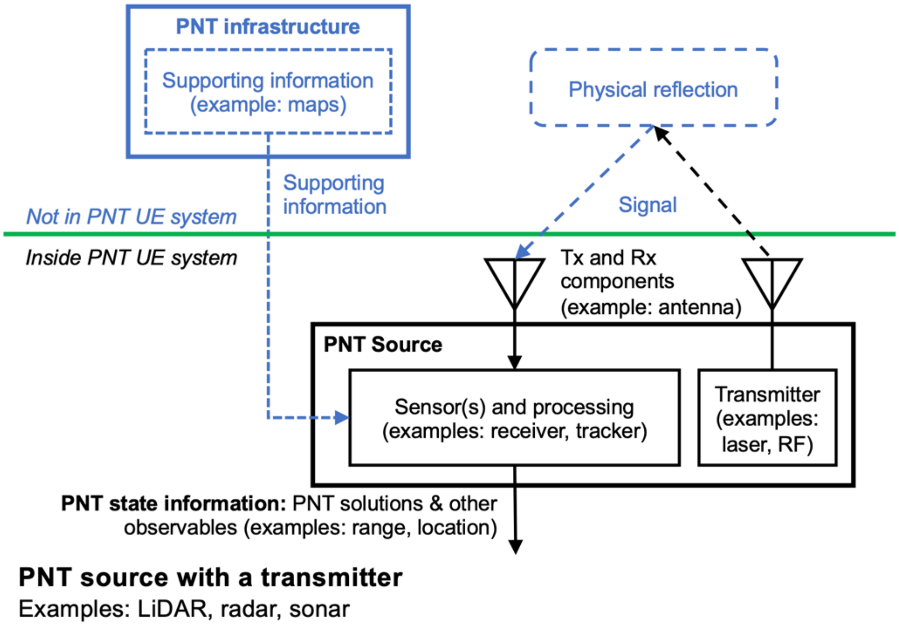

PNT infrastructure
Supporting information (example: maps)
Physical reflection
Supporting information
Signal
Not in PNT UE system
Inside PNT UE system
Tx and Rx components (example: antenna)
PNT Source
Sensor(s) and processing (examples: receiver, tracker)
Transmitter (examples: laser, RF)
PNT state information: PNT solutions & other observables (examples: range, location)
PNT source with a transmitter
Examples: LiDAR, radar, sonar

Figure 21. General components of a PNT source that includes a transmitter.

The transmitters in these PNT sources add complexity and require power. Transmitted signals can also be disrupted, degraded, or manipulated, so the received signal should still be treated as external input, even though it originated from inside the PNT UE. Range information is relative to the PNT source, so maps, other supporting information, or other types of PNT sources are needed to supplement PNT sources with transmitters to find absolute position information.

APPENDIX D: DEFINITIONS

atypical error

Error outside of the calibrated uncertainty bounds of the system within a specified confidence interval. This could include the case where the error is less than the expected performance error due to manipulation.

common mode

Common mode threat/failure refers to the case in which two or more PNT UE systems (or PNT sources), while appearing independent, in fact have a common dependence that makes them susceptible (vulnerable) to the same threat or failure.

component

A part or element of a larger PNT UE system with well-defined inputs and outputs and a specific function. Examples may include individual PNT sources or subsystems of PNT sources, discrete software functions that implement resilient PNT processing algorithms, or hardware modules providing a supporting function internal to the PNT UE system.

compromised PNT source

A PNT source that generates untrustworthy PNT solutions. The source may contain corrupt data or contamination of the normal data processing and storage capabilities. Note that untrustworthy does not always mean the current solution is incorrect.

ephemeris

Parameters relating to the position and trajectory of satellite vehicles.

Integrity

The property of conforming to expected behaviors, preserving quality, and avoiding manipulation.

navigation message

A message included in GNSS signals that provides all the information needed to calculate the PNT solution with the signal measurements.

observables

Measured quantities or calculated values used during the internal signal processing of a system that, when exposed on an interface, could contribute to demonstrating and/or verifying resiliency level claims.

PNT assurance

A process to quantify the confidence that PNT information has integrity, which can be used to establish a level of trust.

PNT resilience

From PPD-21 [2]: *"… 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."*

PNT resilience concepts

Behavior models that describe how to impede attacks and minimize performance degradation due to threats and disruptions in a PNT UE system.

PNT resilience technique

A specific method for implementing a particular aspect of PNT resilience.

PNT resilience technique categories

Groupings of PNT resilience techniques using a common strategy for implementing resilient behaviors.

PNT source

A PNT UE system component that produces a PNT solution. Examples include GNSS receivers, local clocks, inertial measurement units (IMUs), and/or timing services provided over a wired or wireless connection.

PNT UE system

The components, processes, and parameters that collectively produce the final PNT solution for the user.

proper working state

A condition in which the device or system contains no compromised internal components and data fields (e.g., data stored to memory), and from which the device or system can recognize and process valid input signals and output valid PNT solutions. An initial pre-deployment configuration is a basic example. The accuracy of the immediate PNT solution is not specified in this definition, as it will depend on the specifics of the device or system's performance and the degradation allowed by different resilience levels.

PNT situational awareness

The detection, characterization, and geolocation of threats that may jeopardize the accurate or uninterrupted delivery of PNT solutions to the user.

PNT solution

The full navigation solution provided by a PNT UE system or PNT source, including time, position, velocity, and/or navigation information. A PNT UE system or source may provide a full PNT solution or a part of it.

PNT state information

PNT solution information as well as any other types of observables collected from PNT sources, such as power measurements, internal raw signal observables, and data messages. Different types of PNT sources have different types of PNT state information. For a GNSS receiver, the PNT state information includes the pseudorange and other GNSS signal observables as well as information from the navigation message.

resilience

The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions, such as deliberate attacks, accidents, or naturally occurring threats or incidents.

resilience technique

A specific method for implementing a characteristic of resilience.

threat agnostic

An approach to resilience that does not prescribe a specific threat to overcome. Threat-agnostic system architectures should respond to a broad range of existing threats and be capable of withstanding emerging threats not yet imagined.

trustworthiness

The degree to which an element can reasonably be relied on to have integrity.

typical error

An error within the operating bounds of the user equipment.

user equipment

Equipment that outputs PNT solutions, including PNT systems of systems, integrated PNT receivers, and PNT source components (such as GNSS chipsets).

APPENDIX E: ACRONYMS

AGC	Automatic Gain Control
AOA	Angle of Arrival
APM	Absolute Power Monitor
CAF	Cross-Ambiguity Function
CCD	Clock Consistency Divergence
CF	Conformance Framework
CI	Critical Infrastructure
CISA	Cybersecurity and Infrastructure Security Agency
C/N_0	Carrier to Noise Density
DHS	Department of Homeland Security
DME	Distance Measuring Equipment
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
I/Q	In-phase/Quadrature
IMU	Inertial Measurement Unit
INS	Inertial Navigation System
LEO	Low Earth Orbit
OSNMA	Open Service Navigation Message Authentication
NMA	Navigation Message Authentication
PNT	Positioning, Navigation, and Timing
PPD	Presidential Policy Directive
PVT	Position, Velocity, and Time
RA	Reference Architecture
RAIM	Receiver Autonomous Integrity Monitoring
RF	Radio Frequency
RPM	Received Power Monitor
RVPS	Real-time Validation for Plug-and-play Sensors
SA	Situational Awareness

SAARM	Sensor-Agnostic All-source Residual Monitoring
SDR	Software Defined Radio
SQM	Signal Quality Monitor
S&T	Science and Technology
SV	Space Vehicle
TESLA	Timed Efficient Stream Loss-Tolerant Authentication
UAV	Unmanned Aereal Vehicle
UE	User Equipment
VHF	Very High Frequency (30-300 Megahertz)
VORs	VHF Omni−directional Ranges