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

Version 1.0

Homeland Security

Science and Technology

ACKNOWLEDGEMENTS

This document was developed with significant input and collaboration from industry and government stakeholders. The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) acknowledges and thanks all those who have contributed to this framework.

Version 1.0 of this document was developed from July 2019 through August 2020, with contributions from the following people:

Name	Organization/Affiliation
Ernest Wong	U.S. Department of Homeland Security
Benjamin Salazar	U.S. Department of Homeland Security
William Jackson	U.S. Department of Homeland Security
Dr. Arthur Scholz	MITRE
Dr. Patricia Larkoski	MITRE
Dr. William Young	MITRE
Dr. Bradley Moran	MITRE
Brian Callahan	MITRE
Dr. Steven W. Lewis	The Aerospace Corporation
Dr. Sai Kalyanaraman	Collins Aerospace
Helmut Imlau	Deutsche Telekom
Lannie Herlihy	Federal Aviation Administration
Andrew F. Bach	Financial services technology consultant
Victor Yodaiken	FSMLabs Inc.
Dr. Steve Guendert	IBM Corporation
Leigh Whitcomb	Imagine Communications
Lee Cosart	Microchip
Rich Foster	Microchip
Greg Wolff	Microchip
Dr. Paul E. Black	The National Institute of Standards and Technology
Ya-Shian Li-Baboud	The National Institute of Standards and Technology
Magnus Danielson	Net Insight AB
Dr. Deepak Maragal	New York Power Authority
Dr. Cristina Seibert	NextNav
Dr. Stefania Römisch	Northrop Grumman Mission Systems
Charles Swain	Johns Hopkins University – Applied Physics Lab
Monty Johnson	OPNT
John Fischer	Orolia
David Sohn	Orolia
Jeff Dagle	Pacific Northwest National Laboratory
Lori Ross O'Neil	Pacific Northwest National Laboratory
Dr. Michael O'Connor	Satelles
Christina Riley	Satelles
Dan Rippon	Schweitzer Engineering Laboratories
Francisco Girela Lopez	Seven Solutions
Marc Weiss	Spirent Consultant
Mitch Narins	Strategic Synergies, LLC.
Haroon Muhammad	Trimble

Jeffery Sanders	UHU Technologies
Dave Howard	U.S. Department of Energy
Dr. Hadi Wassaf	U.S. Department of Transportation Volpe Center

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/publication/st-resilient-pnt-conformance-framework

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, precision agriculture, financial services, and emergency services. Other GNSS have also joined GPS in providing precise location-based services and precise timing to global infrastructure. Therefore, disruption of or interference with PNT systems (whether GNSS-dependent or otherwise) has the potential to have adverse impacts on individuals, businesses, and the nation's economic and national security. The existence and nature of threats to PNT services are well known and both government and industry have recognized the need for resilient PNT equipment that is capable of withstanding and recovering from such threats.

This Resilient PNT Conformance Framework was sponsored by U.S. Department of Homeland Security Science and Technology Directorate and developed in coordination with industry and federal agency partners. It provides guidance for defining expected behaviors in resilient PNT user equipment (UE), with the goal of facilitating development and adoption of those behaviors through a common framework that enables improved risk management, determination of appropriate mitigations, and decision making by PNT end-users. To encourage industry innovation, this framework is PNT source agnostic and outcome based. It also contains four levels of resilience so that end-users can select a level that is appropriate based on their risk tolerance, budget, and application criticality. Therefore, a lower level receiver is not necessarily better or worse; instead, it simply reflects a level that meets the user's particular needs.

This framework focuses on resilience and applies to UE that outputs PNT solutions, including PNT systems of systems, integrated PNT receivers, and PNT source components (such as GNSS chipsets). While the framework does not cover downstream systems that consume PNT solutions, it remains important to examine downstream systems to reduce PNT risks in operations. Executive Order 13905, Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services, emphasizes the importance of a risk-based approach to identify where PNT services are required and how they are used to limit the impact of PNT disruptions on critical operations and services.

Recognizing that requirements will vary by sector and application, this framework is limited to broad outcome-based capabilities and behaviors for resilient PNT equipment. It is intended to serve as guidance documentation that can be used by standards development organizations to develop voluntary standards with specific requirements tailored to different PNT sources based on sector and application needs.

The conformance framework's four levels of resilience are based around the core functions of Prevent, Respond, and Recovery. Additionally, the levels are cumulative, with requirements in each level carrying over into the next. This results in higher levels corresponding with greater resilience. PNT resilience arises not just from individual component capabilities (such as holdover devices or new PNT sources), but also how they are architected within PNT systems. The vision for the conformance framework is that it acts as a bridge, with Levels 1 and 2 addressing critical legacy issues and Levels 3 and 4 paving the way for future PNT equipment.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1.0 INTRODUCTION AND BACKGROUND

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, precision agriculture, financial services, and emergency services. Other GNSS have also joined GPS in providing precise location-based services and precise timing to global infrastructure. Therefore, disruption of or interference with PNT systems (whether GNSS-dependent or otherwise) has the potential to have adverse impacts on individuals, businesses, and the nation's economic and national security. The existence and nature of threats to PNT services are well known and both government and industry have recognized the need for resilient PNT equipment that is capable of withstanding and recovering from such threats.

This Resilient PNT Conformance Framework was sponsored by U.S. Department of Homeland Security Science and Technology Directorate (DHS S&T) and developed in coordination with industry and federal agency partners. It provides guidance for defining expected behaviors in resilient PNT equipment, with the goal of facilitating development and adoption of those behaviors through a common framework that enables improved risk management, determination of appropriate mitigations, and decision making by PNT end-users. To encourage industry innovation, this framework is PNT source agnostic and outcome based. It also contains four levels of resilience so that end-users can select a level that is appropriate based on their risk tolerance, budget, and application criticality. Therefore, a lower level receiver is not necessarily better or worse; it simply reflects a level that meets the user's particular needs.

This framework focuses on resilience and applies to user equipment (UE) that outputs PNT solutions, including PNT systems of systems, integrated PNT receivers, and PNT source components (such as GNSS chipsets).[1] While the framework does not cover systems that consume PNT solutions, it remains important to examine the systems that consume PNT solutions to reduce PNT risks in operations. Executive Order 13905 Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services emphasizes the importance of a risk-based approach to identify where PNT services are required and how they are used to limit the impact of PNT disruptions on critical operations and services.

2.0 FRAMEWORK OBJECTIVES

The PNT Conformance Framework provides guidance for defining expected behaviors in resilient PNT UE. The intended audience consists of public and private sector users, manufacturers of PNT UE, and providers of PNT services focused on Critical Infrastructure (CI) some of which may not be readily known, or the depth of support well understood.

The objectives of the PNT Conformance Framework include:

---

[1] The distinctions between PNT sources, systems, and solutions are further discussed in Section 4.

- Facilitating the development and adoption of resilient PNT UE, from the underlying chipsets, to integrated receivers, to systems of systems approaches.
- Encouraging industry innovation in resilient PNT UE.
- Providing guidance to Standards Development Organizations (SDOs) in the development of standards tailored to their specific CI sectors.
- Serving as a bridge that addresses legacy resiliency issues at lower levels while paving the way for future UE at the higher resilience levels.

The framework focuses on achieving resilience of PNT UE and services and seeks to ensure alignment to a clear definition of resilience. To that end, it is developed around the Presidential Policy Directive - *Critical Infrastructure Security and Resilience (PPD)-21* definition of resilience the relevant portion of which states:

> The term "resilience" means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. [1]

Assessment of the specific PNT performance requirements of individual sectors or users (i.e., accuracy, availability, integrity, continuity, and/or coverage) is outside the scope of this document.

Finally, although the framework mainly uses GNSS-dependent timing sources as examples, the concepts are intended to be applicable to non-GNSS PNT sources and applications including GNSS and non-GNSS-based position and navigation receivers. GNSS-dependent time and frequency sources are specifically used as examples, because they are currently the most predominant and most at risk timing and frequency sources in CI [2]. For an overview of data and measurement spoofing related to GPS-dependent systems, along with some mitigation strategies, see [3].

3.0 EXPECTED USAGE

The conformance framework is structured for flexibility and is expected to be used in several ways by different groups and individuals. These include Standards Development Organizations (SDOs) that can work with stakeholders to develop performance requirements and facilitate communication regarding resilience between stakeholders. In practice, CI use cases are anticipated to include a mix of PNT systems and services with different resilience level requirements. For example, a timing device at a main site synchronizing many systems and serving a range of performance requirements may require a higher resilience level than a single timing device at a remote location providing time to a single system.

DHS S&T intends to transition the PNT Conformance Framework to CI users, vendors, and industry-supported bodies for adoption and sustainment. Part of the transition should occur via engagement with the appropriate SDOs. The intention is that industry/SDOs would continue the evolution and refinement of the concepts in this document within CI sectors to address the specific needs of those sectors. Stakeholders focused on particular industries would develop additional performance and assurance requirements and refine evaluation processes and metrics. For example, aviation requirements are best developed by the aviation sector, power grid requirements by the power sector, telecommunications by the telecom sector, and so on.

3.1 Guidance and Standards

This PNT framework is agnostic with regards to applications or sectors of use. DHS S&T expects that each CI sector will develop its own set of standards and requirements as needed for that sector and the applications suitable to the sector, with this framework as a common foundation. The framework is also source agnostic, and thus its concepts can be extended for developing guidance documents pertaining to specific PNT sources or services.

3.2. Stakeholder Communication

Another important use of the framework is fostering communication of both the user needs for, and the resilience capability of, a solution. For example, the conformance framework should aid in making the following type of statement:

> For application {X}, subject to threat {Y}, technology/solution {Z} can provide timing at **Resilience Level 3** with an accuracy threshold of 1.8 microseconds 99.9% of the time, and a post-threat recovery time of 80 seconds 95% of the time.

Note that the above statement separates the quantitative performance numbers and other parameters (such as accuracy, availability, integrity, type/magnitude of threat, etc.) from the resilience level. Specific parameters, threats, and threat durations should be consistent with industry use cases and requirements.

4.0 SCOPE OF APPLICABILITY

The scope of applicability covered by the conformance framework includes three general stages in the generation of a PNT solution:

1. Fundamental PNT measurements (e.g., GNSS chipset).
2. Use of an integrated receiver (e.g., includes a GNSS chipset, PNT processor, and clock/oscillator).
3. Use of a system of systems (e.g., includes an integrated receiver, an anti-jamming antenna, and any other connected devices used to deliver PNT data).

These three scopes of applicability illustrate opportunities to increase resilience along the signal processing and solution generation chain. This enables system integrators to use a non-resilient chipset (a chipset that does not meet any resilience level as defined in this document) but integrate it in a receiver in a way that that will ultimately result in its resilience. Similarly, end-users may operate “systems-of-systems” to increase resilience levels through the design, integration, configuration, and deployment of their systems. While the conformance framework makes it possible for an equipment manufacturer to develop a resilient receiver using a non-resilient chipset, utilizing a resilient chipset in a system will mitigate threats earlier in the signal processing chain.

The scope of applicability can be further described using the following definitions, which are used throughout the conformance framework.

> **PNT System:**
>
> The components, processes, and parameters that collectively produce the final PNT solution for the consumer.

PNT Source:

A PNT system component that is used to produce a PNT solution. Examples include GNSS receivers, networked and local clocks, inertial navigation systems (INS), and/or timing services provided over a wired or wireless connection.

PNT Solution:[2]

The full solution provided by a PNT system or source, including time, position, and velocity. A PNT system or source may provide a full PNT solution or a part of it. For example, a GNSS receiver provides a full PNT solution, while a local clock provides only a timing/frequency solution.

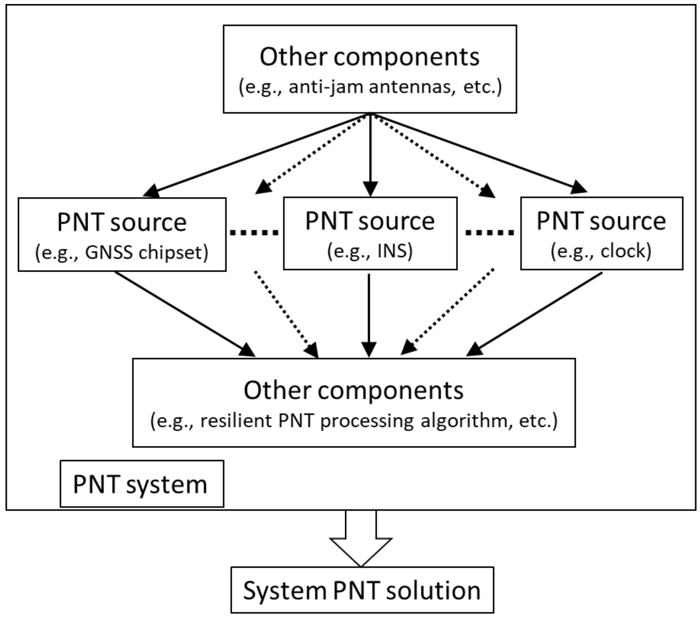

Figure 1. Relationship between PNT source, PNT system, and PNT solution.

Component:

A part or element of a larger PNT 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, hardware modules providing a supporting function internal to the PNT system, antennas, firewalls (between antenna and receiver), and external detectors such as software defined radio (SDR) detectors.

The relationship between a PNT system, PNT source, and a PNT solution in the context of the framework is depicted in Figure 1. The dashed lines indicate that a PNT source may include a variety of inputs from other elements of the system. In addition, the distinction between whether the form of PNT information generation (e.g., chipset, integrated receiver, or system of systems) should be considered a PNT source or PNT system, lies in its relationship to the PNT solution for the overall system. For example, a chipset could contain sufficient internal signal processing to provide a system PNT solution if connected to a wireless timing source.

5.0 KEY CONCEPTS OF THE FRAMEWORK

The framework is built upon three key concepts –defense in depth, core functions, and resilience levels − and adheres to three guiding principles:

[2] Historically, the output of a “PNT source” includes measurements that alone may not provide positioning, navigation, or timing solutions (e.g., altitude). The usage here refers to solutions that generate one or more of the three measurements: positioning, navigation, or timing.

- It should be **outcome-based** (and therefore industry is free to be innovative in how to meet different levels of resilience).
- It should be **cumulative** (where successive levels build upon previous levels).
- It should be **generalized** (remaining technology and source agnostic).

Keeping these guiding principles in mind, the subsections below describe the key concepts of defense in depth, core functions, and resilience levels.

5.1. Defense in Depth

Defense in depth has two dimensions.

- Resilience should be designed and incorporated throughout the entire processing chain and system (via the core functions).
    - The system's required performance and subsequent design requirements should directly address the desired resilience capabilities.
    - Access to observables will support methods to elevate the resilience level.
    - Observables are defined as measured quantities (or calculated values) that:
        - are used by a system during its internal signal processing.
        - could contribute to demonstrating and/or verifying claimed resilience levels when exposed to an interface.
- Diversity of both PNT sources and resilience mechanisms will increase the robustness of the implementation.

Recovery is a critical component of resilience, but it cannot be the first action taken on PNT systems in an operational environment, as it can cause disruptions. Instead it should be treated as the last line of defense, so additional layers of defense are needed. Section 5.2 describes the critical functions that should occur in addition to the last resort of recovery.

5.2 Core Functions

Prevention is the first layer of defense. Ideally threats are prevented from entering a device or system, however, it must be assumed that it will not be possible to stop all threats. Therefore, it is imperative to identify how failure modes occur, understand how a device or system responds to specific threats, and how the device or system recovers. Recovery is an essential element of the definition of resilience in Section 2. These core functions shown in Figure 2, as applied to the PNT Conformance Framework, are described further as follows:

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

- Prevention is preferred: There is no need to execute lower-level functions (i.e., Respond and Recover) if prevention is successful.
- Atypical errors are defined as errors outside of the expected performance bounds. This could include the case where the error appears to be less than the expected performance error due to manipulation. Manipulation can also result in biased or ramping errors within the expected performance bounds that are erroneous and misleading.

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

- The system should ensure an adequate response to externally induced, atypical errors before recovery is needed.

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

- Recovery is required.
- It serves as the last line of defense.

Figure 2. Core functions with embedded detection functionality.

While in practice detection is a key aspect that can permeate all the core functions, some prevention techniques may not directly require detection (or reporting) to be successful; in such cases they would be optional. For example, every filter that blocks bad signals does not necessarily also detect the bad signals and report them (e.g., a directional anti-spoof antenna pointing at the sky, excluding ground signals, does not perform this function). Another example prevention technique might be anti-spoof algorithms that are based on historical data and consistency models and therefore rely only on internal observables.

The intent of the framework is to remain source agnostic to support innovation in industry, however programs and users should understand two underlying factors. First, that all the resilience levels involve some level of detection of anomalous behavior, whether due to intentional or unintentional causes, but the most basic type of detection allowed may be that a human detects a problem through some means. This is may be all that is required for some applications, particularly where Level 1 resilience is acceptable. Second, detection of a problem is generally probabilistic. There is always the potential of either generating false positives (i.e., a problem is detected when one does not actually exist) and not detecting actual problems. It may be necessary to choose a threshold that balances the false-positive and non-detection rates. User training and experience may be necessary for timely recognition of and response to observed and reported anomalies.

5.3 Resilience Levels

The descriptions below cover key features of resilience levels 0 through 4. The capabilities associated with each of the resilience levels are generally increasingly sophisticated and leverage deeper architectural access. The benefits are cumulative with increasing resilience levels; that is, Level 2 is more resilient than Level 1, etc. Finally, descriptions also indicate the depth of architecture access necessary to achieve the resilience levels.

User applications are anticipated to include a mix of PNT systems with different resilience level requirements. The framework provides the flexibility to meet the range of needs by defining hierarchal resilience levels. For example, in a CI timing application, the main site of a distributed timing system may require Level 2 resilience, while Level 1 may be sufficient at remote sites.

In the resilience levels below, “proper working state” is defined as:

> 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.

The descriptions include the desired outcome behaviors and key features of each level, indicating which ones satisfy the core functions of Prevent (P), Respond (RS) and Recover (RC). Some behaviors or features can satisfy more than one of the core functions.

Level 0

A source or system that does not meet Level 1 (or higher) requirements is considered non-resilient. The inability to meet Level 1 requirements may include the following behaviors:

- The possible acceptance and/or usage of unverified input.
- A recovery process that may require manual intervention up to and including replacement of the device (i.e., after the device becomes permanently damaged).

Level 1

Level 1 is the first level of resilience, where a “full recovery” is the critical desired behavior. This recovery process is the last line of defense when all other prevention, response, or recovery behaviors are ineffective or unavailable against threats such as data spoofing. During the recovery process, the PNT solution may be unavailable for some time. Other key features of Level 1 include:

1. Must verify that stored data from external sources adheres to values and formats of established standards. For example, for a GPS-dependent system, this includes compliance with the IS-GPS-200 standard. (P)
2. Must support full system recovery by manual means, making all memory clearable or resettable, enabling return to a proper working state, and returning the system to the defined performance after removal of the threat. (RS, RC)
3. Must include the ability to securely reload or update firmware. (RC)

The necessary architecture depth of access (i.e., what is accessible within the device or system) may be quite minimal (e.g., verify the PNT solution output using basic consistency checks for a simple GNSS-dependent user equipment).

Level 2

Level 2 requires all the resilience behaviors of Level 1 and, in addition, must meet additional requirements in response to compromised PNT sources. A compromised PNT source is defined as 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.

Level 2 requires the ability to continue providing a PNT solution in the presence of the threat while also responding to the threat. However, the PNT solution may be degraded by an unbounded[3] amount. Continuing the enumeration in Level 1, other key features of Level 2 include:

4. Must identify compromised PNT sources and prevent them from contributing to erroneous PNT solutions. (P, RS)
5. Must support automatic recovery of individual PNT sources, without disrupting system PNT output. (RS, RC)

The depth of architectural access (i.e., access to internal processing) necessary to achieve Level 2 resilience is likely at the level of components and their connections. For example, a GNSS-dependent system might verify internal observables from PNT sources and correct the system PNT solution after detecting compromised PNT sources.

Level 3

Level 3 entails a contained and controlled response to the threat. Thus, while in the presence of a threat, a solution must be provided but may be degraded by only a bounded amount. Bounded degradation means that the performance may be reduced compared to nominal operation within well-characterized tolerance limits throughout the degraded period. Adding to the enumeration in Levels 1 and 2, Level 3 includes:

6. Must ensure that corrupted data from one PNT source cannot corrupt data from another PNT source. (P)
7. Must cross-verify between PNT solutions from all sources. (P)

To achieve Level 3, architectural access is likely needed to the internal signal processing steps, and this level of resilience may require hardware, software, and/or system architecture changes.

Level 4

As the highest level of resilience, Level 4 ensures the ability to operate through any compromising events without degradation to the PNT solution. The "No Degradation to Performance" criterion is assumed relative to nominal operations as defined by industry or appropriate SDOs. Level 4 features include:

8. Must have diversity of PNT source technology to mitigate common mode threats. (P, RS, RC)

Beyond source diversity, verification techniques that are fully integrated into the processing of a PNT source might be necessary to achieve Level 4 resilience. For a GNSS-dependent

[3] The output can deviate within a manufacturer defined envelope.

system, this could include validation techniques that are fully integrated into the processing of a PNT source to recover individual PNT sources while a threat persists.

In addition to the features listed for each level, two other important general resilience considerations are:

- Simply adding PNT sources is not a substitute for a secure radio frequency (RF) processing chain and does not necessarily lead to an increase in resilience.
- Additional PNT sources must be handled in a way that ensures each source meets equivalent resilience criteria and does not introduce new vulnerabilities / attack surfaces to the PNT UE.

5.4 Minimum Requirements for Resilience Levels

Table 1 captures the minimum requirements for each resilience level. The descriptions represent minimum behaviors (either allowable or resulting) that must occur to achieve that resilience level. Note that the resilience levels build upon each other, that is, Level 2 includes all enumerated behaviors in Level 1, and so forth. The final PNT output solution behavior for each level is specified as well.

Vendors or test certification bodies could use the table to assert a device is at Resilience Level {X}, and/or is compliant with a regulation or standard. Note that each resilience level comes with an understanding that the provided PNT solution is within the performance indicated in the system's datasheet (e.g., traceability and/or uncertainty to a stated reference) once the threat is removed (Levels 1,2 and 3) or in the presence of the threat (Level 4). Level 2 allows for an unbounded degradation in performance while the threat is present, while Level 3 reduces the allowance to a bounded degradation. Level 1 does not require a viable PNT solution while in the presence of a threat.

Table 1. Minimum requirements for each resilience level.

Level*	Minimum Requirements
Level 1	**Ensures recoverability after removal of the threat**. 1. Must verify that stored data from external inputs adheres to values and formats of established standards. 2. Must support full system recovery by manual means, making all memory clearable or resettable, enabling return to a proper working state, and returning the system to the defined performance after removal of the threat. 3. Must include the ability to securely reload or update firmware.
Level 2	**Provides a solution (possibly with unbounded** degradation) during threat**. Includes capabilities enumerated in Level 1 plus: 4. Must identify compromised PNT sources and prevent them from contributing to erroneous PNT solutions. 5. Must support automatic recovery of individual PNT sources and system, without disrupting system PNT output.
Level 3	**Provides a solution (with bounded degradation) during threat.** Includes capabilities enumerated in Levels 1 and 2 plus: 6. Must ensure that corrupted data from one PNT source cannot corrupt data from another PNT source. 7. Must cross-verify between PNT solutions from all PNT sources.
Level 4	**Provides a solution without degradation during threat.** Includes capabilities enumerated in Levels 1, 2 and 3 plus: 8. Must have diversity of PNT source technology to mitigate common mode threats.
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. ** The output can deviate within a manufacturer defined envelope.

5.5 Common Mode

The conformance framework focuses primarily on resilience behaviors rather than the specific threats a CI sector may face. However, “common mode” threats are an important consideration (e.g., multiple GNSS constellations may be susceptible to the same jamming or spoofing threat). Different mechanisms designed to improve resilience should not be susceptible to the same class of threats (i.e., “common mode” threats). For example, resilience behavior that relies on source diversity assumes that the sources are resilient to common mode threats.

As an example of common mode, consider a receiver able to receive the GPS L2 band or the L5 band. A jammer operating on the GPS L1 signal will not affect the GPS L2 or L5, thus avoiding common mode for that scenario. However, if the bandwidth of the jammer covers both bands or has multiple frequency jamming capability, this jamming scenario would represent a common mode failure.

Another example would be incorrect metadata in the signal broadcast from the GPS system that would cause issues regardless of whether the system uses GPS L1, L2 and L5 signals. A proper analysis of different common mode failures helps to illustrate how different redundancy and resilience mechanisms solve some, but not all, of the common mode issues. Different mechanisms often increase resilience when combined.

6.0 REFERENCE ARCHITECTURE EXAMPLES

Figure 3 provides a high-level view of reference architecture examples associated with the resilience levels. Key differentiators include the depth of architectural access (i.e., access to internal processing) to achieve resilience and the number of PNT sources in the system. Note that simply adding more PNT sources is not enough to increase the resilience level of the PNT system: the sources must be implemented without introducing additional vulnerabilities and must improve the resilient behavior of the system. It is assumed that higher levels of resilience will need to draw on multiple sources, implementing resilience through diversity and advanced resilience processing. In general, the sophistication in resilience processing increases as the resilience level increases.

The diagrams in Figure 3 may apply to PNT systems at different scales. In Figure 3, the "User" is the consumer of the output from the PNT system. A PNT system may be a system of systems or a compact integrated system. The PNT sources may be integrated systems themselves with built-in resilient processing, or minimal versions that will require additional system infrastructure to execute the resilient behavior. For example, for GNSS-dependent systems, the PNT sources may include a chipset or integrated receiver. At each level, the PNT system may be an integrated receiver or a system of systems. In the case of multiple PNT sources as shown in Level 2 and higher, the PNT sources may include non-GNSS-dependent sources, such as clocks, network sources, non-GNSS space-based PNT signals, or ground-based location

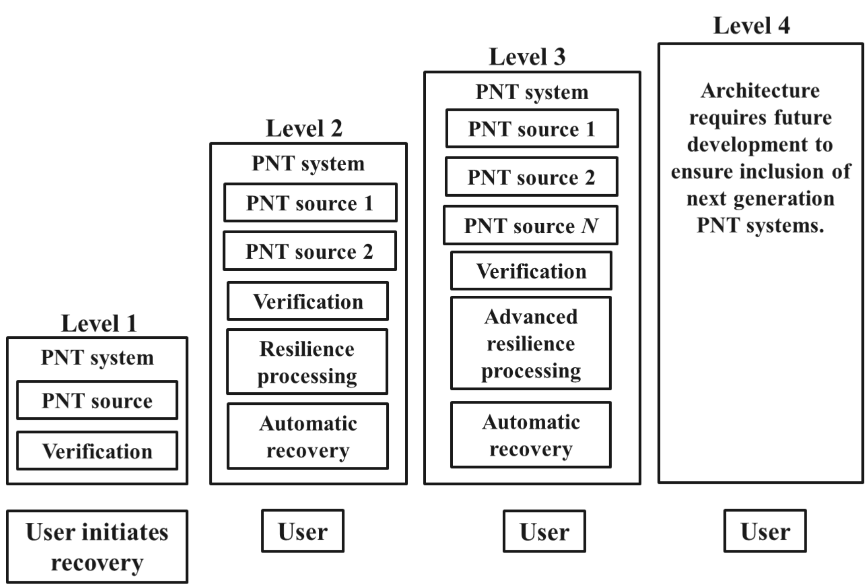

Figure 3. High-level system architectures corresponding to the resilience levels.

systems. Note that Resilience Level 2 does not explicitly require multiple sources. Sections 6.1 and 6.2 contain more details on reference architectures for Levels 1 and 2. Section 6.3 covers some general architecture considerations for Levels 3 and 4.

6.1 Architecture for Level 1

Figure 4 depicts a basic reference architecture example for Resilience Level 1. The key functionality at Resilience Level 1 is represented by the "recovery message," which is used to set the PNT source to a proper working state. The base requirement is the ability for the "user" (whether a person or a system) to initiate the recovery process that sets the PNT source to a proper working state. Verification should occur on the PNT solution and stored data; the required verification processes are not specified.

Example observables for Level 1 include:

- Stored data (any data that is stored to memory, such as state information)
- National Marine Electronics Association (NMEA) messages
- PNT solution, which may include any or all of the position, velocity, and timing solutions depending on the purpose of the system.

Observables are important to inform decisions on response behaviors, such as when to isolate a compromised source. However, resilience levels are not determined by the specific observables that are used or available in the source or system. Simply adding more observables to a source or system does not improve the resilience.

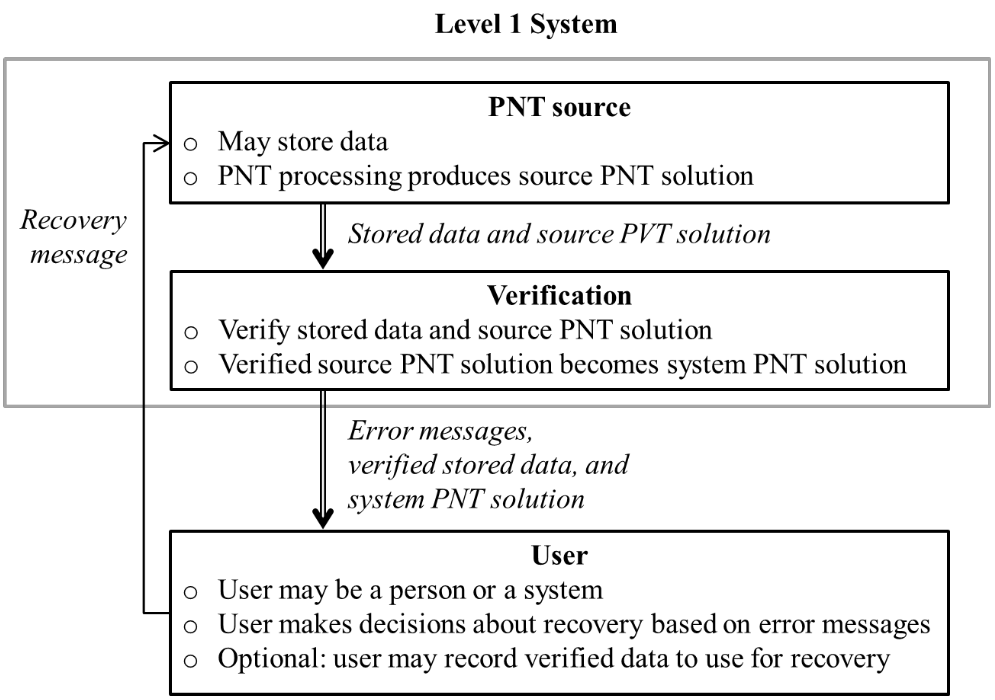

Figure 4. Example reference architecture for Level 1 resilience.

6.2 Architecture for Level 2

Figure 5 depicts a basic reference architecture example for Resilience Level 2. Key features of the architecture (beyond the Resilience Level 1 architecture) include an additional PNT source, verification of internal observables, and the ability to reset individual components. The secondary PNT source must increase the resilience behavior of the PNT system to a higher level than is possible with the primary source alone (i.e., it should be resilient to common mode threats and it should not introduce additional vulnerabilities). Not all features of the architecture, such as verification of internal observables, may be required for a specific implementation.

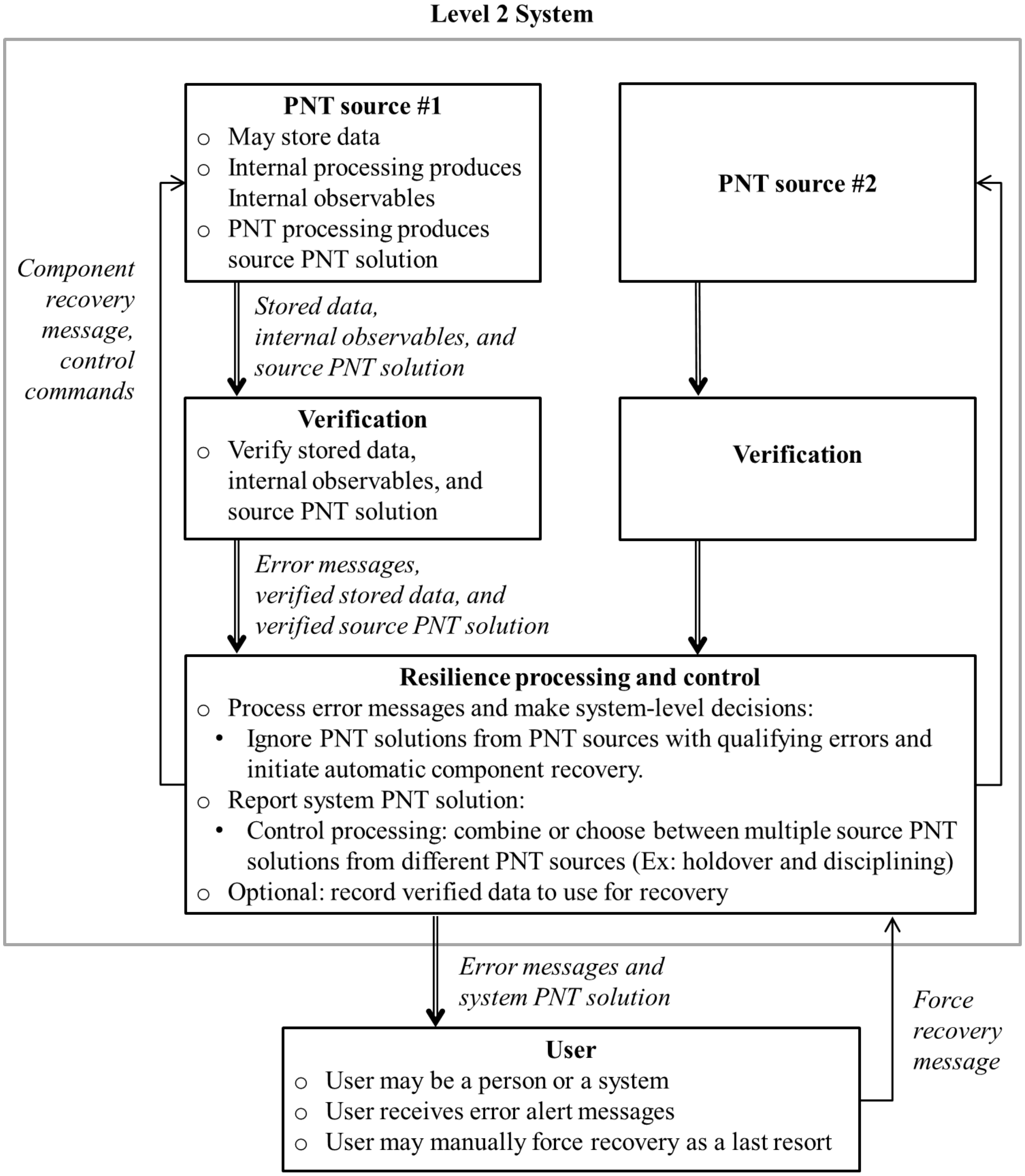

Figure 5. Example reference architecture for Level 2 resilience.

Example observables for Level 2 include:

- Level 1 observables
- Internal observables for GNSS PNT sources
    - Power observables: Automatic Gain Control (AGC), power, or Carrier-to-Noise Density ratio (C/N_0)
    - Raw signal observables: replica code phase, carrier Doppler frequency, phase, and amplitude
    - Solution observables: pseudorange, delta pseudorange, and integrated carrier Doppler phase measurements.

6.3 Architectural Considerations for Levels 3 and 4

Level 3 resilient PNT systems are expected to operate through threats with an allowed bounded degradation to performance. Suitable reference architectures may include access to PNT processing steps internal to the PNT sources to enable advanced mitigation and detection techniques that will likely increase processing complexity. The result of the mitigation or detection techniques employed by the system to withstand the threat can cause performance degradation. For example, the advanced mitigation techniques in a Level 3 PNT system for a timing application may cause delays due to the increase in the processing load, and force the clock locking loop to update at a lower rate, causing in turn the bounded degradation of the overall system performance.

Level 4 resilient PNT systems operate through threats without degradation in performance. These systems will depend on multiple independent PNT sources (possibly different technologies) to achieve this performance. In addition, PNT sources that accept external inputs must perform integrated resilience processing directly in the path of the external input. For example, a GNSS receiver at Level 4 is expected to be able to distinguish the true GNSS signals from false signals, even if the true signals are intermixed with adversarial waveforms.

6.4 Additional Observables

The number and nature of observables play a critical role in achieving resilience. While listing a comprehensive set of observables is beyond the scope of this document, some observables besides those identified in the example Level 1 and Level 2 architectures above include:

- Clock correction – bias, frequency
- Filter specifics
- Tracking loop parameters
- Complete or partial In-phase/Quadrature (I/Q) data
- Outputs from correlators
- Cross-ambiguity Function (CAF).

7.0 SOFTWARE ASSURANCE

While not focused on software assurance (SA), the conformance framework seeks to ensure that SA is incorporated in resilience solutions as appropriate. As pointed out in [4], a “GPS receiver is more computer than radio...”, which serves as a reminder of the need to address SA within PNT sources and systems more generally.

To ensure proper consideration and implementation of SA in achieving resilience solutions, this section provides a non-exhaustive list of SA methods and techniques. Depending on the PNT source or system, not all the listed techniques and methods may apply. For example, a starting point for a GPS-dependent source should ensure that the firmware conforms to the GPS IS-200 standard.

Examples of suggested SA techniques to achieve various levels of resilience include:

- Failsafe firmware upgrade, dual-booting, or recovery image
- Secure firmware loader (Level 0 or 1)
- Dual booting of firmware (Level 1 or 2)
- Error-correcting code on all memory: flash, RAM, processor cache
- Error checking of filesystem and memory – checksums of files, check for stuck bits, etc.
- Sandboxing (Level 3 or 4)
- System design to handle power up and power down scenarios (e.g., what happens if power is cut in the middle of writing data to memory?).

Once a resilient PNT solution is established, maintaining SA to ensure the resilience level over time may include:

- End-user notification of defects, security vulnerabilities, product changes, etc.
- Continuous monitoring of in-process and field failures
- Signed firmware updates
- Third-party software monitoring.

For additional justification of the need for SA in CI timing applications, see the cyber security challenges and potential mitigations with timing in the power grid as discussed in [5], Sections 6 and 7, respectively.

8.0 EVALUATION

Programs can evaluate systems against the resilience levels using multiple methods (or a combination of them), such as static analysis and the application of test vectors. When applying test vectors, the relevant observables should be identified and tracked. CI requirements will determine the appropriate evaluation process as well as the required reporting and supporting documentation.

Testing should include validation and verification of manufacturer specifications and end-user requirements. Manufacturers should test against their product's specifications, while end-users should test against their application requirements. For example, after a firmware upgrade, tests should verify that the device(s) continue to meet the application requirements and defined system performance. The testing can include "negative testing" of high-level processes to account for key failure modes of concern.

The subsections below highlight attributes of several evaluation methods for determining system resilience levels. These descriptions are not comprehensive but provide a starting point for entities such as SDOs and industry stakeholders to define their specific evaluation processes.

8.1 Static Analysis

Static analysis may include a review of the system architecture, engineering designs, and processing code. The key characteristic of this method is that the system is not actively exposed to a threat to determine its response, as occurs when applying test vectors. Due to constantly evolving threats, static analysis is useful to ensure good resilient design and initial implementation practices are followed. For example, Level 1 includes the ability to manually reset a device after an attack, which might be demonstrated by static analysis of the architecture. In Level 4, a requirement for source diversity is clearly an architecture statement that can be verified without testing.

8.2 Test Vectors

A test vector is a surrogate for a threat condition(s) and may represent a specific or generic threat. Individual SDOs will need to determine the test vectors that are appropriate for their certification/acceptance process(es). Development of test vectors that provide clear delineation between resilience levels requires careful consideration to establish clear distinctions between the different resilience levels. Threat modeling plays a key role in developing the appropriate test vectors.

General classes of problems to test for to establish the resilience level are:

- Failures in the source of the timing signal, whether a satellite system or a clock of some kind
- Problems in the transmission of signals, such as jamming, spoofing, or multipath interference
- Problems in the PNT system itself, such as a software bug, oscillator failure, or other hardware failure.

Testing methods include (but are certainly not limited to) the use of simulators (e.g., GNSS simulators) to generate jamming or spoofing signals, signal generators to produce signals that simulate clock or hardware failures, simulated network attacks, or open air attacks on RF signals.

8.3 Other Analysis and Documentation

A range of approaches may provide means of determining a source or system resilience level. In addition, documentation and development standards can aid in assessing the resilience level of a source or system. Any assignment of a resilience level to a source or system should include accompanying documentation, descriptions, and explanations on how the resilience level was determined. Some potential assessment methods and relevant information include:

- Documented development processes and training for personnel
- Moderation and review processes
- Defect logging and review processes
- Code coverage analysis – establish whether all code and functionality are tested, reviewed, etc.
- Requirements traceability
- Vulnerability analysis
- Failure Mode and Effects Analysis (FMEA)

- Fuzz testing
- Evaluation, maintenance, monitoring processes for third-party software
- Functional testing
- Verification testing
- Highly accelerated life testing (HALT).

In addition, some relevant standards and associated verifications include:

- Type testing against internal standards, industry standards, regulatory standards, etc.
- Design standards: comparison to reference resilience architectures
- Coding standards, such as High Integrity C++ (HICPP); consistent practices to reduce defects
- Security standards (determine if formalized practices are in place).

REFERENCES

[1] Presidential Policy Directive -- Critical Infrastructure Security and Resilience/PPD-21 https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[2] “Time – The Invisible Utility,” Cybersecurity and Infrastructure Security Agency https://us-cert.cisa.gov/sites/default/files/documents/Technical-Level_Resilient_Timing_Overview-CISA_Fact_Sheet_508C.pdf https://us-cert.cisa.gov/sites/default/files/documents/Corporate_Leadership_Resilient_Timing_Overview-CISA_Fact_Sheet_508C.pdf

[3] “Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure”, National Cybersecurity & Communications Integration Center and National Coordinating Center for Communications, Department Homeland Security, https://www.us-cert.gov/sites/default/files/documents/Improving_the_Operation_and_Development_of_Global_Positioning_System_%28GPS%29_Equipment_Used_by_Critical_Infrastructure_S508C.pdf

[4] https://www.gps.gov/governance/advisory/meetings/2019-11/martin.pdf

[5] “Time Synchronization in the Electric Power System”, North American Synchrophasor Initiative Technical Report, NASPI-2017-TR-001, March 2017 https://www.naspi.org/sites/default/files/reference_documents/tstf_electric_power_system_report_pnnl_26331_march_2017_0.pdf

APPENDIX A: DEFINITIONS

atypical error

Error outside of the expected performance bounds. 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 systems (or 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 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 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.

observables

Measured quantities or calculated values that are 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 system

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

PNT source

A PNT 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.

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 solution

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

resilience

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.

user equipment

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

APPENDIX B: ACRONYMS

AGC	Automatic Gain Control
CAF	Cross-Ambiguity Function
CI	Critical Infrastructure
C/N_0	Carrier to Noise Density
DHS	Department of Homeland Security
FMEA	Failure Mode and Effects Analysis
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HALT	Highly Accelerated Life Testing
I/Q	In-phase/Quadrature
HICPP	High Integrity C++
INS	Inertial Navigation System
NMEA	National Marine Electronics Association
PNT	Positioning, Navigation, and Timing
PPD	Presidential Policy Directive
RF	Radio Frequency
SA	Software Assurance
SDR	Software Defined Radio
SDO	Standards Development Organization
SV	Space Vehicle
UE	User Equipment