# Towards a Structural Framework for PNT Situational Awareness

Integrating PNT System Resilience and Human-Centric Situational Awareness for Strategic Infrastructure Protection

Andy Proctor – May 2025

## Table of Contents

## Scope and Purpose

The purpose of this essay it to collect and communicate thoughts about PNT-Situational Awareness (PNT-SA), primarily following three separate client contracts where PNT Situational Awareness ended up being a significant topic of discussion. Its purpose is to look strategically rather than technically at the challenge of PNT-SA and is written after many discussions with sector colleagues and conference presentations. There is a clear gap, we must do something, and I hope this essay starts a conversation.

## About the Author

Andy Proctor is a Director of RethinkPNT, a Chartered Engineer, Vice President, Fellow and Trustee of the Royal Institute of Navigation (FRIN), and Fellow of the Institute of Engineering and Technology (FIET). Expertise in space-based and non-space-based position navigation and timing systems, and satellite communications technology. Andy is a former naval communications and surveillance engineer, previous roles also include UK Government Space and PNT technology investor, Technical Director for GNSS at the UK Space Agency, UK ESA Board member for Navigation, and PNT technical lead across the UK Government for the UK Cabinet Office. He also has 18+ years' experience working in industry.

## Acknowledgements

I would like to acknowledge the editing skills and contributions of my fellow Royal Institute of Navigation PNT Advisory Board members, Kieran Bjergstrom and Mitch Narins.

## Executive Summary

Positioning, Navigation, and Timing (PNT) systems underpin nearly every critical function of modern infrastructure, from transport and communications to energy distribution and national security. As dependence on PNT—especially satellite-based services—continues to grow, so does the risk landscape surrounding its use. Threats from both natural disruptions and hostile actors present urgent challenges to ensuring the resilience, assurance, and integrity of PNT services.

This essay advances the concept of PNT Situational Awareness (PNT-SA) as a critical strategic capability essential to organisational and national resilience, and operational continuity. It proposes a structured way to conceptualise the situational awareness and resilience of systems that use PNT data, focusing on three key levels: perception of (use case) relevant PNT signals and conditions, comprehension of their significance and impact, and projection of their future status or degradation.

By treating PNT-SA as a discipline with aspects of cybersecurity or air traffic control, governments and private entities can move from reactive mitigation to proactive assurance. This includes investing in monitoring networks, integrating alternative[1] PNT sources, and institutionalising risk-informed decision-making processes.

It concludes with a call to action: senior leaders must recognise PNT-SA not as a technical luxury but as a strategic necessity. A comprehensive PNT-SA framework enables better detection of threats, swifter response to disruptions, and ensures continuity of operations, enabling the ability to learn and improve. Ultimately safeguarding organisational and/or national interests in an increasingly contested and complex operating environment.

[1] to Global Navigation Satellite Systems (GNSS). Alternative in this essay can be contextualised as different, another source - rather than as some have used it, a backup or secondary source.

## Introduction

Modern societies are deeply reliant on PNT services [1], yet this dependency is often poorly understood at the institutional level, and indeed all levels of organisations. PNT systems provide the foundational timing and positioning data that enable the seamless operation of critical infrastructure. For example, GNSS signals synchronise power grids, navigate aircraft, ships, trains, and even guide autonomous vehicles in transport networks, ensures accurate timestamping in financial transactions, and supports military operations through precise navigation and guidance.

Disruptions to these systems can have catastrophic consequences [2]. A GNSS outage in the transport sector could impact safety, delay logistics, disrupt supply chains and cause ripple effects in manufacturing and retail. In the financial sector, a timing anomaly could lead to discrepancies in high-frequency trading, resulting in millions of pounds in losses within seconds [3]. In the energy sector, a failure in timing synchronisation could cause grid instability, leading to widespread blackouts with severe economic and social impacts.

Despite the critical role of PNT systems, many public and private institutions lack a comprehensive understanding of their dependencies on these technologies [4]. This gap in awareness contributes to insufficient prioritisation and investment in resilience measures, poor coordination among stakeholders, and a lack of preparedness for potential disruptions.

The UK Government [1] previously has highlighted that many critical infrastructure operators were unaware of their reliance on the US Global Positioning System (GPS) for timing, leaving them vulnerable to disruptions from solar flares or intentional jamming. Very few nations and indeed organisations have formalised PNT dependency audits in their national infrastructure plans, underscoring a global gap in institutional awareness.

Current efforts within the PNT sector to enhance the resilience of systems that use PNT have largely focused on technical solutions, such as GNSS signal hardening, anti-jamming techniques, spoofing and jamming detection algorithms, and the development of alternative time and frequency sources like enhanced Long-Range Navigation (eLoran) systems or atomic clocks. While these measures are essential, they are insufficient on their own. [5-10]

Few initiatives have addressed the macro-level awareness structures needed to detect, respond to, and recover from threats and disruptions in a structured manner. I set out the basis for such an approach (Figure 1) to PNT system resilience [11], and more recently the Royal Institute of Navigation builds on this to set out top level principles for PNT resilience and encourage organisational thinking [12].

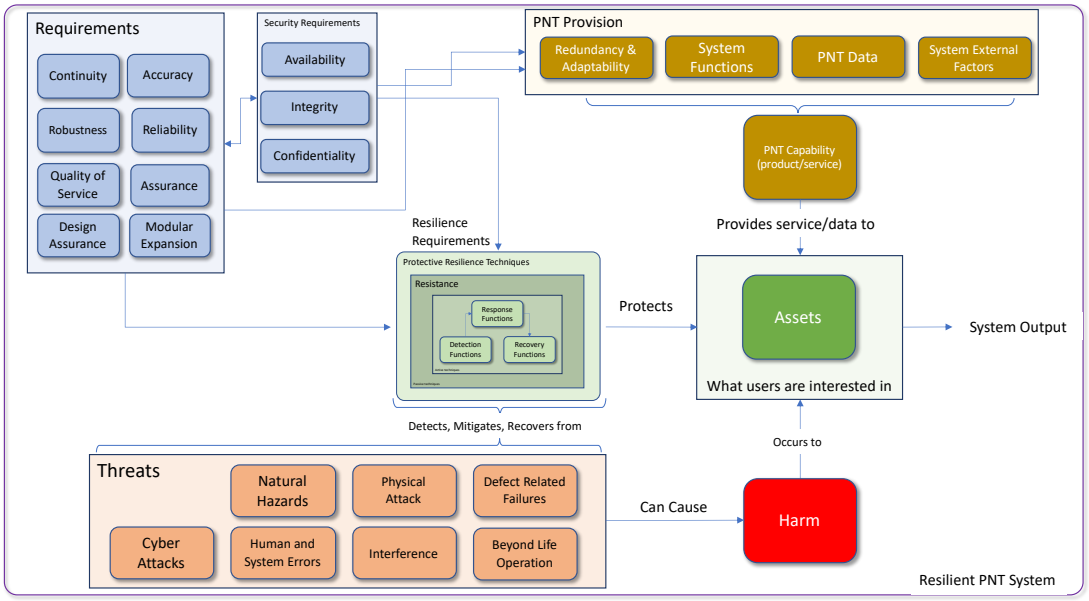


***Figure 1: A Structured approach to achieving PNT System Resilience[11]***

Combining the thinking of [11, 13, 14] a definition of [PNT] system resilience can be derived.

> *A PNT system performs in a resilient manner (exhibits resilience properties) when it sustains operations to a required performance characteristic, under both expected and unexpected conditions by adjusting its functioning (passively resist or actively detect threats, respond to them, and recover and learn from the harm they cause) prior to, during, or following events (changes, disturbances, and opportunities), while also understanding how any adaptation within the system will impact the environment in which the system operates.*

This resilience definition itself does not encompass the facets of situational awareness that are needed within PNT systems to ensure safe and efficient operations in fields like aviation, maritime, military, autonomous driving, and supporting mission-critical decisions.

Situational awareness (SA) can be defined as:

> "The perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future."[15]

As an example, from a military aviation perspective, SA refers to the capability to conceive the current and future disposition of red and blue aircraft and surface threats within a volume of space [16].

This is where Endsley's SA framework [15] becomes invaluable. The model, widely used in human factors research, defines SA across three levels: perception (detecting relevant data), comprehension (understanding its significance), and projection (anticipating future outcomes). This is shown in Figure 2.

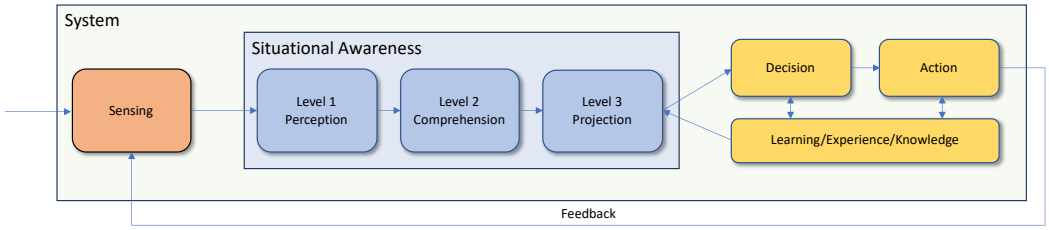


*Figure 2: Model of SA, adapted from [15, 16]*

In operation, the model has an SA core with sensing and decision-making elements being separate and external to the core SA functions. Sensors, in the PNT domain such as Controlled Reception Pattern Antennas (CRPA), spectrum analysis or other monitoring functions, sense the environment to capture its state. The sensed information, often fused from multiple methods [16], is the input to the core SA functions.

| Stage | Description | Key Characteristics |
|---|---|---|
| Level 1: Perception | Detecting and perceiving critical environmental elements and events. | - Gathering raw data (e.g., sights, sounds, alerts).<br>- Noticing cues and stimuli.<br>- Dependent on attention and sensory input. |
| Level 2: Comprehension | Interpreting and understanding the meaning of perceived information in context. | - Integrating data with prior knowledge.<br>- Assessing relevance to goals.<br>- Forming a mental model of the situation. |
| Level 3: Projection | Anticipating future states and outcomes based on current understanding. | - Predicting future events or system states.<br>- Supporting decision-making.<br>- Requires expertise and experience. |

*Table 1: The three stages of Situational Awareness, according to Endsley [15]*

Level 3 SA supports and influences decision making as the SA input determines the ability of the system or individuals to adopt “an effective problem-solving strategy” [15, 17].

How the SA information is presented to the decision-making function is therefore critical to the ability of the system or individual/organisation to make timely and critical decisions. This is both a human factors function, and an information exchange function and can determine the level of future adaptation/learning that can be achieved. System designers need to consider this in capability implementation.

## Bridging Situational Awareness and PNT Resilience

When integrated with the principles of PNT System resilience [11] and those of resilience engineering [13], this SA framework can guide the development of a national or organisational PNT-Situational Awareness (PNT-SA) function that transcends technical domains and fosters system-wide clarity.

The need for such a framework is urgent. The threat landscape for PNT systems is evolving rapidly, driven by factors such as increasing cyber threats (e.g., GNSS spoofing by state and non-state actors[18]), natural phenomena (e.g., solar storms disrupting satellite signals[2, 19]), and geopolitical tensions (e.g., regional conflicts leading to intentional jamming). The OPS Group, a group of commercial airline pilots, have highlighted the vulnerability of GNSS and PNT systems to hybrid warfare tactics, affecting both military and civilian operations [18]. These challenges highlight the necessity of a strategic, rather than purely technical, approach to PNT-SA—one that integrates human and automated decision-making, cross-sector coordination, and long-term planning to ensure system resilience.

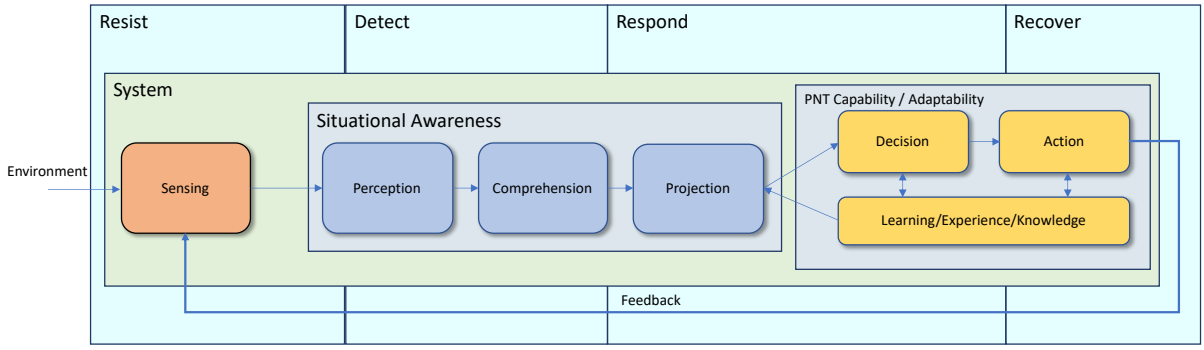


***Figure 3: Integration of the SA framework with elements of PNT System Resilience[11, 15]***

The integration of Endsley's SA model with PNT resilience functions (Figure 3) creates a dynamic framework that enhances system-wide preparedness. Table 2 outlines the alignment between SA levels, resilience functions, and their structural implications:

| **Endsley's SA Level** | **PNT Resilience Function** | **Implication** |
|---|---|---|
| Level 1: Perception | Detection | Detect and perceive critical environmental elements and events. Multi-domain real-time monitoring systems, spectral analysis, visual input, assessing system performance outputs (PNT Context - The environment is changing) |
| Level 2: Comprehension | Detection<br>Response | Interpret and understand the meaning of perceived information in context. Understanding and correlating inputs to output performance, (PNT Context - Am I being jammed? Is it impacting me, if so, how badly? What options can I use to respond?) |
| Level 3: Projection | Response<br>Recovery<br>Adaptation | Anticipate future states and outcomes based on current understanding. System performance forecasting and recovery, learning and adaption (PNT Context - I can switch PNT source, but will the jamming last long, what do I understand about it, will it stop me doing what I need |

| | | |
|---|---|---|
| | | to? What can I learn to prevent it impacting me in the future?), |

*Table 2: Integrating Endsley and Proctor [11, 15]*

### Perception, Comprehension and Detection

At the perception level, systems and/or operators must detect anomalies in PNT signals and contextual factors that may indicate potential threats. This aligns with the resilience pillar of detection. For example, a transport network reliant on GNSS for fleet management can avoid operational delays if jamming or spoofing is detected early. Multi-sensor fusion, which integrates space-based data (e.g., GNSS), terrestrial references (e.g., eLoran, Distance Measuring Equipment (DME)[20]), and user feedback, can enable early detection.

Contextual factors such as space weather (e.g., solar flares), cyber threats (e.g., spoofing by adversarial actors, or PNT data attacks), and geopolitical tensions (e.g., jamming during regional conflicts [18]) must also be monitored.

At the comprehension level, the significance of detected anomalies must be understood. For instance, if a financial sector operator detects a timing anomaly in GNSS signals, comprehension involves understanding its impact on high-frequency trading, where millisecond discrepancies can lead to significant losses. Cross-sector teams—comprising experts from transport, finance, energy, and telecoms—can assess how a PNT disruption propagates and coordinate a response.

### Projection and Recovery

At the projection level, the second- and third-order effects of PNT disruptions should [must] be anticipated, supporting the recovery and adaptation of systems. For example, a GNSS outage in the transport sector might delay logistics, impacting supply chains and, subsequently, manufacturing timelines.

Simulation models can be used *a priori* to predict impacts and cascade failures, allowing operators or system design to pre-position resources—e.g. eLoran or INS—to ensure continuity or minimise performance impact. Recovery planning ensures systems can "bounce back" by adapting infrastructure, such as integrating more resilient timing sources into future designs. The recover aspect, specifically, is defined as the system's ability to actively recover from harm after a threat is neutralised, returning to full operational status or adapting to prevent future harm.

Recovery can be full, partial (using redundant resources without repair), or minimal (degraded mode operations providing limited services), and may include evolving or adapting to avoid future harm [11].

The alignment between projection and recovery lies in their shared focus on mitigating future risks through preparedness and adaptability. Projection, by anticipating potential disruptions, directly supports the recover aspect by enabling the pre-emptive design and implementation of recovery strategies. For instance, if a PNT system senses a GPS loss (due to jamming), the immediate comprehended impacts may be minimal but the projection, based upon mission profile, is that there

is a high likelihood of complete GPS signal loss, the subsequent decision function can be triggered to automatically switch to alternative navigation methods, such as terrestrial RF, ensuring continuity of operations and facilitating swift recovery once the threat is mitigated. Learning from this scenario could be not to use GPS as a primary sensor, but only when use case metrics require it.

This anticipatory approach is particularly relevant given the dynamic and often unpredictable nature of PNT threats. By forecasting these scenarios, projection aids in the development of adaptive recovery strategies, where the system not only recovers but also evolves to prevent similar disruptions in the future, aligning with the system resilience emphasis on adaptability [11].

The integration of SA Level 3, projection, into the resilience framework has practical implications for PNT system design and operation. For example, projection can inform the implementation of degraded mode operations, where the system gracefully switches to a well-defined degraded mode to avoid complete failure, allowing for service degradation and subsequent restoration. Similarly, automatic failover to other systems, such as hot failover preferred over warm or cold failover, can be pre-planned based on projected threat scenarios, minimising downtime and ensuring rapid recovery.

Advanced techniques, such as machine learning algorithms, further enhance the alignment between projection and recovery. These algorithms, with careful consideration, can be trained using projected threat models to predict movement of vehicles or obstacles [21], to assess risk and future incidents [22], allowing the system to adapt and recover more efficiently in real-time situations, learning from past disruptions to improve future resilience.

**Decisions**

The SA functions are generally closely coupled to decision and action functions, so that the appropriate mitigations or responsive actions can be initiated. In the PNT domain, often this is managed through the employment of a specific algorithm[23], a Kalman filter (specifically switching, or extended variants), or through human intervention. Kalman filters can be deployed to support the response, recovery and decision functions, such as when to switch between a main data source, like GNSS, and a backup, like an inertial navigation system, by checking if the main source is working well. [24-26]

Kalman filters are recursive algorithms used to estimate the state of a [dynamic] system from a series of measurements. They are particularly effective in multi-sensor fusion to provide position, velocity, and orientation. They operate in two phases: prediction, where it forecasts the state (expected) based on a system model, and update, where it incorporates new measurements to refine the estimate. If the difference between expected and measured data is too big, it might mean the main source, like GPS, is faulty, maybe jammed or worse. Kalman filters can deprioritise the faulty source by adjusting how much they rely on it. For the alternate systems they have access to, they might increase priority or trust, like using the inertial system more. This can be done smoothly by changing weights or by picking a different setup if the source is totally unreliable[27].

While Kalman filters are effective, but Jayaram [26] notes the additional need for fast convergence algorithms to detect faults rapidly, especially in spacecraft dynamics.

**Interconnection and Feedback Loop**

The SA levels and resilience pillars are deeply interconnected, forming a continuous feedback loop (Figure 3): detection informs response, response outcomes guide recovery, and recovery lessons drive adaptation. For instance, if a cyberattack jams GNSS signals (detected at Level 1), its consequences are situated within the mission parameters (Level 2), the expected impacts are estimated (level 3) and the system responds by switching to an alternative PNT source (Decision). The incident is used to support modelling future risks (knowledge/experience), and potential system adaptations, investment in anti-jamming technology perhaps, enhancing overall resilience. This loop ensures that systems that use PNT information are not merely reactive but adaptive, capable of evolving in response to emerging threats.

## Current Gaps in PNT-Situational Awareness

Despite the critical role of PNT systems, several weaknesses undermine the potential success of PNT-SA.

**Overreliance on Technical Fixes**

Efforts to enhance PNT resilience often focus on device-level solutions, such as signal hardening, anti-jamming/spoofing hardware and detection algorithms, improved decision and switching functions (discussion of Kalman filers as a solution for switching PNT source, in this paper), or alternative PNT sources, without integrating or feeding back into higher level system functions, or broader governance structures.

This leaves systems that use PNT information vulnerable to systemic and cascading failures that technical fixes alone cannot address, such as organisational use of PNT-SA inputs. Research in academia tends to focus on the technical domain not on the integration of PNT-SA into existing or new command and control, or decision support systems.

This overreliance on technical fixes has several detrimental effects on PNT-SA governance and resilience:

- **Neglect of Systemic Vulnerabilities**: By focusing on technical-level solutions, the systemic vulnerabilities that drive cascading effects are sometimes neglected
- **Fragmented Resilience Efforts**: Technical fixes are often implemented in isolation, leading to fragmented resilience efforts across sectors. For instance, a financial operator might invest in atomic clocks for timing redundancy, but without coordination with the energy sector.
- **Delayed Response to Emerging Threats**: Technical fixes are reactive, addressing known threats (e.g., jamming) but failing to anticipate emerging risks, such as quantum-based attacks on GNSS encryption [28], or AI-driven spoofing. The role of unknown threats is noted in my PNT System Resilience paper, [11]

- **Increased Costs Without Proportional Benefits**: Technical fixes often require significant investment, but their benefits are limited without systemic integration. This inefficiency diverts resources from more effective, systemic solutions, such as cross-sector coordination hubs or simulation-based modelling.
- **Exacerbation of PNT-SA Literacy Gaps**: Technical fixes often assume a high level of expertise, exacerbating the PNT-SA literacy gap because this can cause reduced comprehension and misinterpretation of issues, delayed response times and erosion of trust in the system.

While technical solutions like signal hardening, anti-jamming technologies, alternative PNT sources, and multi-constellation receivers enhance resilience at the device (or product) level, they fail to address systemic vulnerabilities.

**Lack of Cross-Sector Communication Protocols**
Without standardised protocols for information exchange, it is difficult to assess and respond to multi-domain threats. Neither NMEA 0183 nor RINEX is suitable for PNT-SA cross-sector communication. NMEA 0183's unidirectional nature, low data rate, and lack of contextual integration fail to meet the real-time, bidirectional, and multi-domain needs of PNT-SA. RINEX, as a file-based format, is not designed for real-time communication and cannot support the interactive, user-friendly/focussed data exchange needed for SA coordination. While NMEA 2000 [29] offers improvements (bidirectional communication, higher data rate, fault tolerance), its maritime focus and limited contextual integration make it suboptimal without customisation and security improvements.

A custom PNT-SA protocol, built on modern networking standards (e.g., MQTT [30], JSON [31]), is the most promising solution, as it can be tailored to the specific needs of PNT-SA, addressing real-time communication, contextual integration, role-based tailoring, security, and scalability. However, implementing such a protocol requires overcoming significant development and adoption challenges, such as increasing system complexity and not introducing a new threat vector, which could be mitigated by using standards like NMEA 2000 as a transitional step.

**Inadequate Modelling of Cascading Effects**
Cascading effects refer to the chain of consequences that follow an initial disruption in a system, propagating through interconnected sectors and amplifying the overall impact. In the context of PNT systems, a disruption—such as a GNSS outage, timing anomaly, or spoofing event—can trigger a domino effect across critical infrastructure. For instance, a GNSS outage might first affect transport systems by disrupting fleet navigation, which delays logistics, impacts manufacturing supply chains, disrupts retail operations, and ultimately affects consumer markets. These second- and third-order effects are often complex and non-linear, involving feedback loops and interdependencies that are difficult to predict without comprehensive modelling [32, 33].

With reference to the models noted in this essay, this gap primarily affects the projection level, as it limits the ability to forecast how a PNT disruption will propagate through dependent systems. This, in turn, undermines the resilience pillars of recovery and adaptation, as operators cannot prepare for or mitigate the broader

impacts of a disruption. For example, a GNSS timing anomaly might be modelled for its direct impact on energy grid synchronisation, but its downstream effects on telecommunications (e.g., disrupted mobile networks) and transportation (e.g., delayed emergency response vehicles) are often ignored. This siloed perspective is a byproduct of fragmented ownership across sectors, where stakeholders lack a unified framework for modelling interdependencies.

Predicting cascading effects requires advanced simulation tools that can model complex, non-linear interactions across sectors. While some sectors use simulation for specific purposes (e.g., power grid operators simulate load balancing), these tools are rarely designed to account for PNT dependencies or cross-sector impacts. Many critical infrastructure operators underestimate their reliance on PNT systems, particularly for timing. This lack of awareness translates into a failure to model how PNT disruptions propagate through their systems. Without a clear understanding of these dependencies, operators cannot build models that accurately predict cascading effects, leaving them vulnerable to unexpected systemic failures.

**Human factors information presentation**

Human factors encompass the psychological, cognitive, and ergonomic considerations that influence how individuals interact with systems, process information, and make decisions. In the context of PNT-SA, effective information presentation is crucial for enabling systems, operators and decision-makers to operate correctly.

Information presentation involves the design of interfaces, dashboards, alerts, and reports that convey PNT system status, anomalies, and risks to human users. When not designed with human factors in mind, these systems can overwhelm users, obscure critical insights, or lead to misinterpretation, ultimately compromising the resilience of PNT-dependent infrastructure.

- Lack of User-Centric Interface Design: One of the most significant gaps in PNT-SA governance is the absence of user-centric interface design tailored to the cognitive needs of operators and decision-makers. Many existing PNT monitoring systems present data in a highly technical format, such as raw signal-to-noise ratios, doppler shifts, or pseudorange errors, which are difficult for non-experts to interpret.
- Inadequate Tailoring of Information to Stakeholder Roles: Not correctly tailoring information presentation to the diverse roles and needs of stakeholders can cause more problems that it tries to solve. Different sectors—such as transport, energy, finance, and telecommunications—rely on PNT systems for distinct purposes, and their operators have varying levels of technical expertise and decision-making authority. However, current systems often adopt a “one-size-fits-all” approach, presenting the same raw data to all users without considering their specific contexts or responsibilities [34].
- Insufficient Use of Visual and Auditory Cues for Prioritisation: Human factors principles emphasise the use of visual and auditory cues to prioritise critical information and guide user attention. PNT-SA systems must use these cues effectively, or this will lead to missed alerts or delayed responses. In addition, systems often do not provide cascade failure likelihood information.

**Resource and Expertise Constraints**
Addressing these gaps requires significant resources, including data scientists, technology and sector-specific experts, and computational infrastructure. However, many organisations—particularly in the public sector—lack the expertise and funding to undertake such tasks, particularly the modelling functions. This resource gap perpetuates the reliance on simplistic, direct-impact models that fail to capture the broader consequences of PNT disruptions. Even in advanced economies, decision-makers often lack the training to interpret PNT-related risks, inhibiting effective investment, planning, and response. Addressing these gaps requires a structural approach that institutionalises SA as a core capability across sectors, organisations and public bodies.

**Implications**
These gaps have profound implications for PNT-SA. First, they exacerbate the SA literacy gap by making it difficult for non-experts to engage with PNT data, leading to delayed or incorrect decisions. Second, they hinder cross-sector coordination by failing to provide stakeholders and second, or third-order systems, with role-specific insights, contextualised information and adequate technical detail for decision making. Third, they increase the risk of cascading failures by limiting system and operators' ability to project and mitigate these "downstream" effects.

## From Technical Monitoring to Situational Awareness

To address these gaps, PNT-SA must be elevated from a technical and somewhat tactical process to a strategic capability embedded within organisational and national frameworks. I propose four interlocking structural layers to create a comprehensive PNT-SA function:

- **System Perception Layer**
  This layer focuses on identifying and monitoring raw signals and indicators of system status:
  - Real-time GNSS Monitoring Platforms: These platforms detect anomalies such as spoofing, jamming, or signal degradation.
  - Signal Integrity Diagnostics: Tools to assess performance, quality and integrity across multiple PNT sources, ensuring redundancy.
  - Multi-Sensor Fusion: By integrating space-based data (e.g., GNSS), terrestrial references (e.g., eLoran), and user feedback, this creates a unified picture of system health.
- **Organisational Comprehension Layer**
  This layer interprets data for informed decision-making:
  - Cross-Sector Analysis Teams: These teams unite sector experts to take the organisational level decisions from a PNT standpoint or perhaps integrated into existing emergency operations cells.
  - Risk Dashboards: Tools to translate technical anomalies into actionable insights for non-experts. A dashboard might display a GNSS timing anomaly's potential impact on financial trading, prompting operators to switch to backup systems.
  - Sector-Specific Interpretation Protocols: Protocols that define thresholds for alerting and escalation, which will understandably be different sector by sector and use case by use case.

- **Strategic Projection Layer**
  This layer anticipates future threats and prepares adaptive responses:
  - Threat Scenario Libraries: These libraries capture historic and emerging threat vectors, such as quantum-based attacks on GNSS encryption. The U.S. National Institute of Standards and Technology (NIST) maintains a similar library for cybersecurity threats [35], which could be adapted for PNT risks.
  - Simulation-Based Consequence Modelling: Models to predict how PNT disruptions propagate through dependent systems.
  - Recovery Planning Workflows: Workflows (For example, checklist and action cards) integrate scenario outcomes into contingency planning. For instance, a military deployment might pre-position deployable eLoran systems to ensure continuity during a GNSS outage, based on simulation results and lived experience data.
- **Coordination and Accountability Layer (Governance)**
  This governance layer "institutionalises" PNT-SA across organisations:
  - PNT-SA Coordination Hubs: Hubs to act as organisational, national or regional points for PNT threat management, aggregating data and facilitating cross-sector communication. The UK's National Protective Security Authority (NPSA) could serve as a model, expanding its scope to include PNT-SA [36].
  - PNT-SA Owners and Champions: These resources, embedded in government agencies, critical infrastructure sectors, organisational risk or continuity functions, ensure accountability and oversight. For example, a National Timing Authority (NTA) could oversee delivery of a region, or nation-wide PNT timing capability.
  - Policy Frameworks: These frameworks define roles, responsibilities, and standards for reporting and coordination. The UK Government have started on this path, but progress is at a steady but gradual pace [37].

The four layers are interdependent domains, aligned with Endsley's SA model [15] and integrated with PNT resilience functions (detection, response, recovery/adaptation) I have previously proposed [11]. Key is governance, ensuring coordination between technical systems, human operators, and strategic leadership. This model (Figure 4) illustrates that resilience and situational awareness are interwoven; perception enables detection, comprehension supports response, projection and decisions, drive recovery and adaptation.

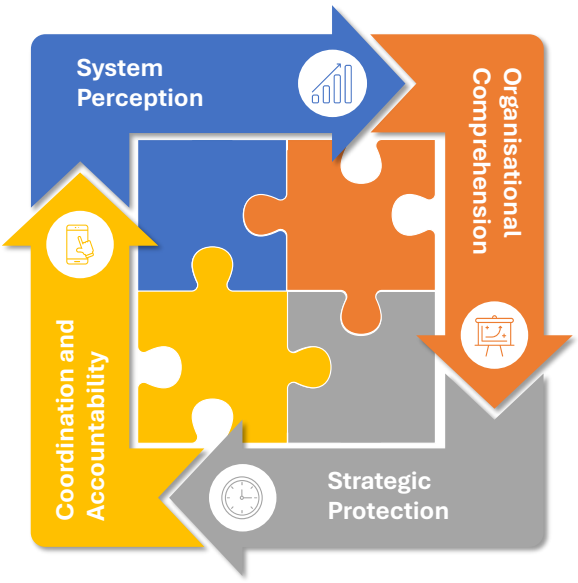


*Figure 4: Four Layers of PNT-Situational Awareness*

Feedback loops between layers ensure continuous improvement—Each layer informs the others, enhancing preparedness—**enabling PNT system resilience**.

## Implementation Challenges

Building this structural PNT-SA function will confront several challenges:

- **Fragmented Ownership:** PNT services span public and private sectors, with little centralised command. Situational awareness requires data sharing and governance coordination that are difficult under the current fragmentation.
- **Lack of Institutional PNT-SA Literacy:** Most infrastructure stakeholders are not trained in PNT principles, even if they have SA capabilities. They may monitor operational metrics without the PNT analysis and interpretation tools to understand threats beyond their domain.
- **Overconfidence in GNSS Redundancy:** The proliferation of satellite constellations (e.g., GPS, Galileo, Beidou) is often mistaken for systemic resilience. However, without PNT-SA, users may fail to detect spoofing, jamming, or timing errors until damage has occurred.
- **Absence of Simulation Culture:** Endsley emphasised the importance of mental models [15]. In a macro-PNT context, these must be built through training and simulations—yet such exercises are rare in the PNT community.

Overcoming these challenges requires cultural change, the development of a PNT situational awareness mindset that permeates not only engineering teams but also policy makers, regulators, and operational staff

## Recommendations

To implement this framework, I propose the following recommendations:

- **Establish PNT Situational Awareness Hubs:**
  - These hubs should serve as central nodes for data aggregation, threat assessment, and cross-sector communication.
  - They should maintain real-time monitoring infrastructure, such as ground-based GNSS monitoring stations, to act as a single point of truth for stakeholders.
- **Codify Cross-Domain Dependency Mapping:**
  - National infrastructure planning should institutionalise the modelling of PNT interdependencies. For instance, a dependency map might reveal that a power grid's timing system relies on GNSS, which in turn depends on satellite cybersecurity measures.
  - All critical infrastructure risk assessments should include a PNT dependency (and cascade assessment) audit, ensuring operators understand their vulnerabilities.
- **Develop SA Literacy Across Sectors:**
  - PNT-SA principles should be included in executive training, operator certification, and infrastructure planning and preparedness.
  - Cross-sector education initiatives should improve awareness of cascading impacts, using case studies.
- **Embed PNT-SA Functions in Regulatory Standards:**
  - PNT-SA functions should be required in resilience assessments and reporting mechanisms.
  - Best Practices [12] should be formulated and adopted, and where necessary, minimum standards/requirements for detection, response, and recovery capabilities should be established, ensuring all sectors meet a baseline level of preparedness.
- **Align Investments with Resilience Informed by PNT-SA:**
  - PNT-SA-derived assessments and projections should prioritise infrastructure hardening and R&D funding. For example, simulation models might identify a need for Terrestrial RF system deployment in a specific sector, necessitating collaborative research between industry and academia.
  - Pilot programs and testbeds should model resilience under realistic conditions, such as simulating a GNSS outage during a NATO exercise to test response and recovery mechanisms.

## Conclusion

Achieving resilient PNT services in the 21st century requires more than signal redundancy—it demands a strategic PNT-SA capability embedded at organisational, national, and international levels. By integrating Endsley's SA model with PNT resilience pillars, this essay creates a system where detection, response, recovery, and adaptation form a continuous loop, empowering institutions to anticipate, understand, and manage disruptions.

PNT-SA must evolve from an engineering detail to a national resilience function, enabling governance of systemic vulnerabilities with foresight and agility. As threats to PNT systems continue to evolve, this framework provides a roadmap for building a future where critical infrastructure is not merely reactive but adaptive, ensuring the stability and security of modern societies.

## References


1. Government Office for Science, *Satellite-derived Time and Position: A study of Critical dependencies*. 2018, HM Government: London.
2. HM Government, *National Risk Register 2023 edition*. 2023, HM Government: London.
3. Schroeder, F., et al., *Occasional Paper 37: Flash Crash in an OTC Market* 2018, Financial Conduct Authority.
4. Royal Institute of Navigation, *Preparing for a Loss of Position and Timing*. 2023, National Preparedness Commission.
5. Humphreys, T.E., Z.L. Clements, and W. Qin, *GNSS Interference: Situational Awareness and LEO Backup*. 2024, University of Texas at Austin.
6. Strandjord, K.L. and P. Axelrad. *A Framework for Regional GNSS Situational Awareness*. in *30th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2017)*. 2017. Portland, Oregon, USA.
7. Department of Homeland Security, *Resilient Positioning, Navigation, and Timing (PNT) Reference Architecture*. 2022.
8. Ciarán Murphy, *Reliable and resilient PNT in any environment*. 2024, Qinetiq.
9. John Plumb *PNT Resilience for an Era of Great Power Competition*. 2024.
10. Gao, G., et al. *Protecting GNSS Receivers From Jamming and Interference*. . in *Proceedings of the IEEE*. 2016.
11. Proctor, A., *A structured approach to achieving system resilience for Position Navigation and Timing (PNT) Systems (PNT System Resilience)*. 2022, RethinkPNT: Devon, UK.
12. Royal Institute of Navigation *Three Stages To Resilient PNT*. 2025.
13. Hollnagel, E. *Resilience Engineering*. 2016 [cited 2024 November]; Available from: https://erikhollnagel.com/ideas/resilience-engineering.html.
14. Linkov, I. and B.D. Trump, *Risk, Systems and Decisions The Science and Practice of Resilience*. 2019, Springer: Switzerland.
15. Endsley MR, *Towards a theory of situation awareness in dynamic systems*. Human Factors The Journal of the Human Factors and Ergonomics Society, 1995. **37**(1): p. 32-64.
16. Munir, A., A. Aved, and E. Blasch, *Situational Awareness: Techniques, Challenges, and Prospects*. AI, 2022. **3**: p. 55-77.
17. Manktelow, K. and J. Jones, *Priniciples from the psychology of thinking and mental models*. Applying cognitive psychology to user-interface design. 1987, Chichester, England: Wiley. 83-117.
18. OPS Group, *GPS Spoofing: Final Report*. 2024.
19. Met Office *Space Weather Impacts*. 2025.
20. Federal Aviation Administration *GBN - Distance Measuring Equipment (DME)*. 2024.
21. Inez Van Laer *Tesla's Self Driving Algorithm Explained*. 2022.
22. Kucher, J. and A. Drumm, *The Traffic Alert and Collision Avoidance System*. The Lincoln Laboratories Journal, 2007. **16**(2).
23. Doug Arnold *What makes a Master the best?* 2013.

24. Aswal, N., S. Sen, and L. Mevel, *Switching Kalman filter for damage estimation in the presence of sensor faults*. Mechanical Systems and Signal Processing, 2022. **175**(1).
25. K. P. Murphy, *Switching Kalman Filters*. 1998, Compaq Cambridge Research Lab Tech. Report.
26. Jayaram, S., *A new fast converging Kalman filter for sensor fault detection and isolation. Sensor Review*. Sensor Review, 2010. **30**: p. 219-224.
27. Jiang, H., et al., *Innovation-based Kalman filter fault detection and exclusion method against all-source faults for tightly coupled GNSS/INS/Vision integration*. GPS Solutions, 2024. **28**: p. 108.
28. Junquera-Sánchez, J., et al., *Assessment of Cryptographic Approaches for Quantum-Resistant Galileo OSNMA*. Journal of the Institute of Navigation, 2024. **71**(2).
29. National Marine Electronics Association *NMEA 2000*. 2025.
30. MQTT *MQTT: The Standard for IoT Messaging*. 2025.
31. International, E., *ECMA-404: The JavaScript Object Notation (JSON) data interchange syntax*. 2017.
32. Rinaldi, S.M., J.P. Peerenboom, and T.K. Kelly, *Identifying, understanding, and analyzing critical infrastructure interdependencies*. IEEE Control Systems Magazine, 2001. **21**(6): p. 11-15.
33. Pederson, P., et al., *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research*. 2006, Idaho National Laboratory: Idaho Falls, Idaho.
34. Nielsen, J., *Usability engineering*. 1993, San Francisco, USA: Morgan Kaufmann.
35. National Institute of Standards and Technology *Cybersecurity*. 2025.
36. National Protective Security Authority *National Protective Security Authority*. 2025.
37. HM Government *Positioning, Navigation and Timing: Overview*. 2025.