The Royal Institute of Navigation

WHITE PAPER

Recommendations to Promote the Adoption of Resilient Position, Navigation and Timing in the UK

With Growing Capabilities Come Growing Threats

JULY 2023

Contents

Foreword

Over recent years we have all become increasingly dependent on Positioning, Navigation and Timing (PNT) services throughout so many aspects of our daily lives. For many of us that reliance is hidden and unknown, but the last five to ten years has seen the publication of a number of reports in the UK and internationally, all highlighting the criticality of and our dependence on, precise and reliable PNT and the increasing vulnerabilities of these services.

This white paper makes a significant contribution to raising the awareness of the need for resilience in PNT and I commend the authors for taking the initiative to compile this work. This is an important step forwards and I truly hope it stimulates the debate and actions necessary to facilitate the establishment of resilient PNT services.

Professor Terry Moore OBE
Past President, RIN
Professor Emeritus, University of Nottingham, UK

Authors and acknowledgements

This paper was prepared by RIN Fellows Ramsey Faragher and Mitch Narins with support from the RIN's PNT Advisory Group.

Thanks also to Richard Bowden, Guy Buesnel, Bob Cockshott, Alan Grant, Todd Humphreys Mike Jones, Terry Moore, John Owen, John Pottle and Andy Proctor for contributions, comments, advice and reviews.

Executive summary

Background

While the 20th Century was focussed on the provision of ubiquitous and accurate Positioning, Navigation and Timing (PNT), the 21st Century's focus has shifted to ensuring that PNT services may be trusted and are reliable and resilient. As we move to more and more systems that are either fully automated, or are automated to the point of human complacency, we are recognising the need for PNT systems that will: operate in unprecedented threat-challenged environments (both civil and military); continuously provide usability and integrity status; fail (ideally) very rarely; and when they do fail, do so safely, securely and elegantly. Failing safely and securely means providing a warning and ensuring that no users are put in danger during the system outage, regardless of the cause of such failure. Failing elegantly means ensuring that the system will seamlessly move between nominal operation, degraded modes and back to nominal operation, while keeping the user aware of these performance changes. Identification of PNT system/service system failures (e.g. outages or loss of trusted service) would be determined by a risk management/probability of failure analysis, similar to those used in the aviation sector, which would identify the requirements for establishing complementary PNT (CPNT) capabilities.

PNT system/service failures can be caused by a wide range of problems – the root causes at times traceable to design decisions and underestimated operational threat environments. These failures can be the result of natural or man-made, intentional or unintentional occurrences, including power outages, sensor failures, sensor obscuration, exceeding maximum limits on sensor inputs, electronic denial of service interference, space weather, atmospheric events and spoofing (the provision of false signals or the injection of fake data into sensors). PNT systems that can protect users by identifying, resisting and recovering from these failures automatically, and resume nominal operations, are described as Resilient PNT systems.

Purpose

The RIN believes that the UK has the opportunity to provide much-needed leadership in the area of improving PNT performance, underpinned by deep expertise and a track-record of innovation and development in these areas over recent decades.

This paper identifies a suggested RIN-led approach to establish practical guidance and steps to achieve this.

We hope this paper will stimulate feedback and discussion, following which the RIN plans to take feedback on board and build support to move ahead in these areas.

Findings

The findings of this paper include the following:

- There is no current standard (or set of standards) that identifies the performance requirements needed to ensure resilient PNT to satisfy the needs of all UK Critical National Infrastructure (CNI) stakeholders (i.e. services providers, users and use cases);
- While a space-focussed National Space Strategy was defined in September 2021, an announcement on an overarching UK PNT strategy is anticipated, but has not been made at the time of writing;
- Over the past two decades, both manufacturers and users in UK and throughout the world, have migrated to using PNT services derived from Global Navigation Satellite Systems (GNSS) as a highly precise and accurate, albeit not resilient, source of PNT services without the need to determine their actual PNT requirements or understanding the impacts of the loss or degradation of these services – seeing GNSS as being both a technically and economically sound solution and in many cases remaining unaware, ignoring or underestimating its vulnerabilities;
- Creating a single universal standard to cover all sectors and use cases would be a huge and lengthy task and delay much-needed rollout of resilient PNT capabilities. A more productive approach for the UK and for the Royal Institute of Navigation (RIN) would be to propose a set of guidelines for assessing the resilience of the current or proposed PNT systems for CNI and recommended "best practices" to guide CNI sector users and service providers in their selection and operation of PNT user equipment. While "best practices" are neither standards nor statutes, they can help inform, influence and motivate users to adopt resilient PNT services and solutions.

Recommendations

1. Establishment of a small, focussed RIN-led Working Group, composed of PNT experts and representatives of CNI stakeholders, to develop a PNT Resilience Action Plan that identifies specific steps, timeframes and incremental improvements needed to promote an accelerated implementation of resilient PNT services and solutions;
2. Establishment of "Best Practices for Use of PNT by UK CNI Services", by which both PNT users and service providers would be invited to assess their PNT risks and determine the failure modes and effects that result from loss or manipulation of minimum required PNT services; and
3. Consult within RIN and with interested stakeholders as to other contributions RIN can deliver in support of an anticipated overarching UK National PNT strategy.

Introduction

Positioning, Navigation and Time (PNT) are the collective terms for the information required to calculate a position and move along a course (i.e. navigate) through an environment and to determine absolute time-of-day, time durations and precise frequency. Apart from the magnetic compass, celestial measurement tools and manual almanacs (e.g. astrolabes), which are well over 1000 years old, most of the PNT approaches used today has been developed in the last 100 years. Inertial navigation, barometric altimeters and long- and short-range radio positioning technologies were developed during the First and Second World Wars, providing navigation aids for naval and airborne platforms. During the cold war era, Global Navigation Satellite Systems (GNSS) were invented and, over the last 20 years, indoor positioning technologies based on Ultra-Wideband (UWB), Wireless Networking (WiFi) and Bluetooth (BLE) have become default features of our smart devices. Today, without even thinking about it, we all use PNT services multiple times every day, whether we are checking the weather on our smartphones, hailing a taxi via a mobile application, communicating with others by voice or text, searching for nearby services, navigating on land, sea and in the air, or even playing video games. PNT services have become deeply embedded and are critical in the support of a vast majority of our activities – including the provision of services in all CNI sectors. PNT services are also a key means of supporting safety, security and economic wellbeing, but due to their vulnerabilities, this can be a mixed blessing unless proper cautions and controls are put in place. It should be noted that not all users will require positioning and navigation and timing information. Some users just require a source of absolute time; others just require a precise, stable and trustable frequency reference.

All PNT systems and sensors are susceptible to disruption (i.e. interference), intentional or unintentional, by both natural and man-made sources. Even clocks and inertial sensors, which appear self-contained and that generate updated information on time or motion internally, are regularly updated by other sensors to ensure that they maintain accurate position, time and precise, stable frequency. Because of its high performance, low cost and worldwide coverage, today those updates are typically provided by GNSS or other radio-based aids. All radio-based PNT sensors are vulnerable to interference, replay attacks, denial of service (jamming) and manipulation (spoofing). Additional information into PNT systems and their vulnerabilities may be found on the Resources tab of the RIN Website (https://rin.org.uk/page/Our_Resources). In particular there is useful repository of information in the Resource Portal for Resilient PNT at https://rin.org.uk/page/ResilientPNT and a range of relevant Webinars, accessible via https://www.youtube.com/@royalinstituteofnavigation.

The challenge has been and continues to be, to promote the identification and implementation of resilient and complementary PNT systems and user equipment such that CNI and other users of PNT services can maintain both safety and security and ensure the economic

wellbeing of the nation. The problem has been studied for well over two decades[i]. It is crucial that the knowledge gained from these many studies on the needs and methods for providing resilient PNT solutions be implemented to preclude significant, yet not unforeseen damage.

Motivation for this white paper

This paper investigates the value of developing and using standards and guidelines in the selection and implementation of PNT equipment to minimise the risks to CNI when those PNT equipment are facing disruption. Mandating that PNT systems must conform to a certain resilience standard to be certified for CNI applications is an effective means for ensuring that resilient PNT systems are in use by CNI. Using legislative levers to ensure that PNT Systems are resilient to the loss of one or more PNT services is another positive action the government can take that will be considered in this paper.

Defining Resilient PNT

Before addressing how best to achieve resilient PNT, it is important that we establish a common understanding of what we mean by *resilient* [ii]. Historically, *robust* and *assured* have also been used in discussing the need to strengthen PNT systems and services. To facilitate understanding, our use of these terms will conform to the following Cambridge Dictionary definitions:

> **Resilient: "*Able to return quickly to a previous good condition after problems*".**
>
> **Robust: "*Strong and unlikely to fail*".**
>
> **Assured: "*Certain to be achieved or maintained*".**

We can see, therefore, that while a Resilient PNT system may suffer failures and outages, it returns quickly to its previous level of capability when the "problem" (i.e. threats, hazards and/or disruptions) has passed. A Robust PNT system is one that has been specifically designed to be unlikely to fail. Assured PNT implies that particular PNT performance levels (accuracy, availability, integrity, or continuity) can be verified, achieved, or maintained.

[i] The first "seminal" public report was published by the Volpe Center https://rntfnd.org/wp-content/uploads/Vople_vulnerability_assess_2001.pdf. A "seminal", and more recent, UK report is the Blackett Review https://www.gov.uk/government/publications/satellite-derived-time-and-position-blackett-review

[ii] The definition by the Cabinet Office in "EC-RRG resilience guidelines for providers of critical national-telecommunications infrastructure" is "The word 'Resilience' is to be interpreted in the broadest sense as the ability of an organization, resource or structure to be resistant to a range of internal and external threats, to withstand the effects of a partial loss of capability and to recover and resume its provision of service with the minimum reasonable loss of performance."

Therefore, it follows that *resilience* is the most basic, foundational PNT aspect, its key feature being the ability to *quickly* return to full working condition after encountering problems. To be truly resilient, a system that provides PNT information must demonstrate that it is capable of protecting its critical assets from harm when subjected to disruption and then return to normal operation after the issue has been dealt with or passed. A critical metric is *how quickly* normal operation resumes and *how to maintain safety, security and minimum economic loss* in the interim. However, resilience needs to apply beyond the PNT equipment to the "users" of the PNT services, as well. Therefore, while resilience allows return to "a previous good condition", it should also support the needs for safety and security. To fulfil this requirement, resilient systems must also warn the "user" when it is encountering a "problem", i.e. when its services are unavailable or do not meet specified performance levels – e.g. its outputs have reduced in accuracy or are invalid and should not be trusted. While a GNSS receiver is somewhat resilient to a momentary power outage because it stores satellite orbital data in non-volatile memory and switches to acquisition mode on regaining power to search for the signals again and autonomously regain a positioning and timing solution, to be resilient it must also preclude the use of hazardous and misleading information from a spoofed signal during and after restoral. Unlike a GNSS receiver, a pure inertial navigation system is not inherently resilient to loss of power since it has no way of correctly reinitialising its initial PVT states on powering back up without external assistance.

From its definition, *robustness* is a metric based on its likelihood of breaking or failing. To achieve "Assured PNT" a PNT solution must be subjected to and pass a set of tests that subject it to known operational threats, hazards and disruptions to ensure that it will continue to operate within its stated performance limits. As noted above, the PNT performance metrics that must be addressed are accuracy, availability, integrity and continuity. Depending on the use case, coverage may need to be considered as well (e.g. indoors, urban canyons, high RF environments, etc.).

To ensure that the performance metrics are being achieved, a user (or a system using a PNT device) should be warned when the PNT capabilities are reduced in performance or unavailable. It should also be made clear when the problem has ended and that the system has returned to trustable nominal operation.

CNI: A System-of-Systems requiring Resilience

Various UK CNI already define resilience for other parts of their systems. For example, the Cabinet Office states in "EC-RRG Resilience Guidelines for Providers of Critical National-Telecommunications Infrastructure"[iii]:

[iii] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1020214/EC-RRG_Resilience_Guidelines_v3.1__2021_.pdf

> *"The word 'Resilience' is to be interpreted in the broadest sense as the ability of an organization, resource or structure to be resistant to a range of internal and external threats, to withstand the effects of a partial loss of capability and to recover and resume its provision of service with the minimum reasonable loss of performance."*

The US National Institute of Standards and Technology (NIST) Special Publication 800-160 Vol2 on Developing Cyber-Resilient Systems [1] describes resiliency as "the ability to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks, or compromises on systems" and notes that this definition can be applied to a variety of entities, including:

- A system
- A mechanism, component, or system element
- A shared service, common infrastructure, or system-of-systems identified with a mission or business function
- An organisation
- A critical infrastructure sector or a region
- A system-of-systems in a critical infrastructure sector or sub-sector
- The Nation

Resilient PNT also encompasses this same wide range of entities, from a system and its components right up to the Nation as whole.

Key strengths of the UK PNT landscape

The UK has been a global leader in PNT for centuries, dating back to the origins of the Greenwich meridian and the Longitude Prize. During World War II, the UK pioneered many radio navigation aids and early terrain-mapping radar navigation systems. The legacy has continued into the 21st Century with the UK taking a leading role in key areas of PNT innovation. Examples are too numerous to list, but some notable areas of UK leadership include innovation in signals and control for GNSS systems, PNT satellites, receiver development spanning military specification through to enabling developments for smart phone navigation, precise timing transfer and control, system integration and PNT-enabled applications and test, measurement and verification.

The UK is also where the essential development of the International GNSS Service (IGS) occurred, a service that provides accurate, precise and highly reliable positioning, navigation and timing information to users worldwide. The original concept for an international GPS service, which began to crystallise at the 1989 International Association of Geodesy (IAG) Scientific Assembly in Edinburgh, UK [2], now includes over 200 organisations in 80 countries operating the cooperative global tracking network of over 350 GPS stations upon which IGS

depends. The UK has also been a leading participant in the Galileo satellite navigation system, including contributing to the BOC signal structure design and the PRS encryption scheme and has pioneered developments into quantum technologies for sensing and navigation [3].

Challenges to the UK PNT landscape

Leaving the European Union (EU) has impacted Britain's access to secure PNT systems, since only EU or authorised "Third Party" states have automatic access to the European Geostationary Navigation Overlay Service (EGNOS) Safety-of-Life (SOL) service and to the Galileo encrypted Public Regulated Service (PRS) signal. It may be possible to negotiate access to PRS, but this is not guaranteed [4] and the current policy is not to pursue this [5]. A potential further complication could be, in theory, a further reduction in cooperation and coordination between the UK and EU in terms of future PNT system development and maintenance. The UK will likely not have access to any future EU PNT programmes, e.g. if the EU pursues a navigation constellation in Low Earth Orbit (e.g. IRIS2 LEO constellation).

Some countries have developed their own Global or Regional Navigation Satellite Systems and so provide, or could provide in the future, authenticated or encrypted signals to their own critical services to increase robustness. The United States, China, Russia and the European Union have global systems, while Japan and India maintain regional systems. As noted above, under the Polaris/Trident agreement, the UK has access to US P(Y) and M-code encrypted GPS signals for military use, but not for CNI.

Resilient PNT standards and guidelines

An option for promoting the establishment and use of resilient PNT systems in the UK and its use across the CNI is through the establishment of PNT guidelines, best practices, or standards. Each of these represents significantly different levels of detail, focus and effort. According to the Institute of Electrical and Electronic Engineering (IEEE), "Standards are published documents that establish technical specifications and procedures designed to maximise the reliability of the materials, products, methods and/or services people use every day." They also "form the fundamental building blocks for product development by establishing consistent protocols that can be universally understood and adopted." Standards can be instrumental in promoting the development and use of resilient PNT systems in a number of ways:

- Compliance and Conformance: Standards can provide a framework for defining and evaluating required performance. Conforming to a standard will help ensure that PNT systems meet minimum technical and operational requirements needed to achieve

resilience, as well as helping to maintain compatibility and prevent interference with other systems.

- Encourage best practices: Standards can allow experts to provide best practice guidance directly to all of the sectors of the UK National Infrastructure in an efficient manner.
- Interoperability: Standards can help ensure that different PNT systems are able to work together seamlessly, which can improve the overall resilience of the PNT system by providing complementary PNT capabilities through redundancy and diversity.
- Cost-effectiveness: Standards can help to ensure that PNT systems are designed and implemented in a cost-effective manner, which can help reduce the overall cost of implementing and maintaining PNT systems.
- Collaboration: Standards can also facilitate collaboration between different organisations and stakeholders, which can help to promote the development and implementation of resilient PNT systems by expanding markets that can avail themselves of similar, if not identical resilient PNT solutions. Standards can also promote the design, development and manufacture of PNT solutions that support multiple sectors/use cases, as well as the test and evaluation methodologies that can support PNT UE acquisition and implementation decisions.

Standards can also play an important role in sparking innovation and economic growth [6]. Small companies can contribute essential patents into a standard, allowing them to access new and larger markets more quickly. Standards can also provide a basis for regulation, which can help to promote innovation and economic growth by ensuring that new technologies and products are developed and used in a safe and responsible manner.

The activities required to develop a UK-led standard depend on its scope and type, but could include some or all of the following:

- Setting up a task force comprising representatives from relevant government agencies, industry and academia to develop and promote a resilient PNT standard for critical national infrastructure.
- Identifying and prioritising key challenges and requirements by conducting a comprehensive analysis of the current state of PNT systems and identifying key challenges and requirements for a resilient PNT standard, taking into account the specific needs of critical national infrastructure.
- Developing the standard based on the analysis of CNI users and use cases, that includes best practices, technical/performance requirements and evaluation criteria for designing and implementing resilient PNT systems for CNI, including identification of the threats, hazards and disruptions environments in which resilient PNT systems must operate.
- Developing a framework for compliance and conformance evaluation and guidance for testing and validation of systems, equipment and technology, to ensure that the standard is being followed.

- Promoting implementation among relevant stakeholders and working with industry to implement the standard.
- Conducting regular reviews of the standard to ensure that it remains up-to-date and relevant in light of new developments in PNT technology and changing requirements for critical national infrastructure.
- Encouraging the UK government to work with other countries and international organisations to promote the standard and ensure that it is adopted internationally.

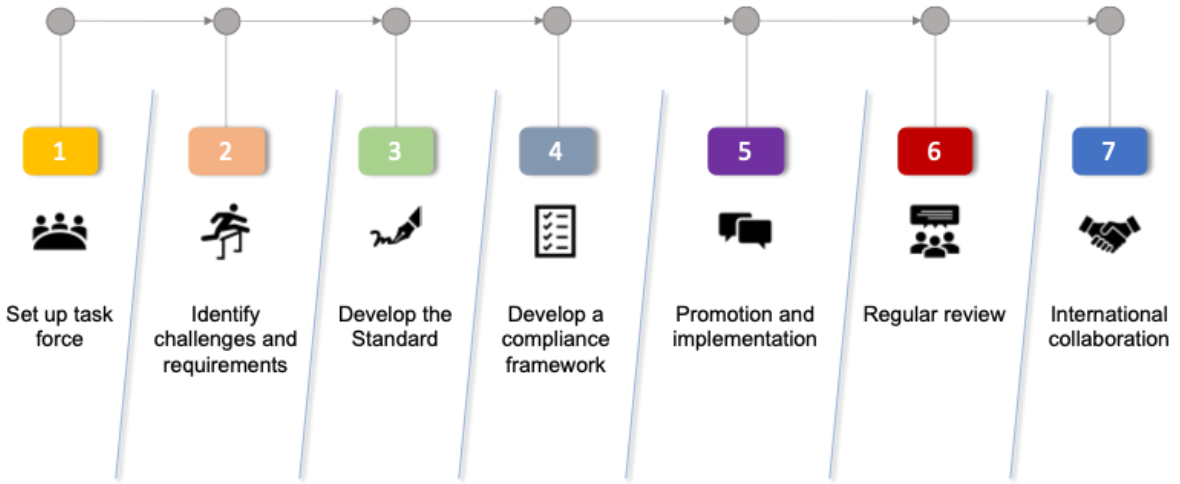

Figure 1. Action Plan activities to promote PNT resilience for CNI via guidelines or a standard

Discussion of existing standards and guidelines

A collection of standards related to resilient PNT is provided in Annex A. Standards typically focus on performance requirements and the demonstration and verification that the system complies with these requirements.

A highly-relevant standard that is currently in development is the IEEE P-1952 standard [7]. This standard specifies technical requirements and expected behaviours for resilient PNT User Equipment. The scope is limited to the reception, ingestion, processing, handling and output of PNT data, information and signals. Based on technical requirements, the standard aims to define different levels of resilience to enable users to select a level that is appropriate based on their risk tolerance, budget and application criticality.

Due to the vast number of sources, sensors, methods, users and use cases involved in PNT, there is no "one size fits all" PNT system; however, there may be categories of PNT use cases that could achieve needed resilience by using the same PNT source(s). Currently, many applications derive their PNT information from a single GNSS receiver – and nothing else. To be resilient, all PNT resilience and performance metrics must be considered, including accuracy, availability, integrity, continuity and coverage. For some, a system that appropriately

combines GNSS and inertial (INS) or oscillators may suffice. A local positioning system, especially indoors, may use UWB, WiFi, BLE or other local beacons instead of or in addition to GNSS. A logistic tracking system monitoring high value materials may use cellular positioning instead of or in addition to GNSS. Robotics platforms may use visual navigation. Each use case presents its own set of required performance metrics, as well as its own operational challenges.

Therefore, an all-encompassing "Resilient PNT standard" aiming to cover all possible technologies, methods and use cases would be a very large, unwieldy document simply because of the very large number and diversity of PNT users. A more tractable solution would be to provide universal guidelines and a generic framework for checking the level of resilience in a given PNT system, agnostic to the sensor set and methods in use. UK CNI is well defined (Chemicals, Civil Nuclear, Communications, Defence, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport and Water) and so guidelines and best practices could be developed that exhaustively covers the requirements and specifications for resilient PNT for each sector.

Resilient PNT guidelines could provide the expected behaviours or outcomes for the system under given conditions or in response to certain events in order to be classified as resilient to threats. Such guidelines would typically include several key requirements or features to ensure that PNT systems recover elegantly and correctly following an outage, attack, or failure.

Suggested requirements for UK Resilient PNT guidelines and best practises for CNI

While creating such guidelines is beyond the scope of this paper, we strongly recommend that a working group be created to develop one. A similar framework has been developed by the US Department of Homeland Security Science and Technology Directorate. The Resilient Positioning, Navigation and Timing (PNT) Conformance Framework [8] provides guidance for defining expected behaviours in resilient PNT equipment and describes five tiers of resilience levels. The logic behind this is to make it easily achievable for low-cost consumer grade equipment to pass some rudimentary level of resilience, with higher tiers involving stricter requirements. The analysis needs to be completed to determine if this is the right approach for the UK. A desired outcome for the working group would therefore be to assess the applicability of the US DHS framework and ongoing IEEE P-1952 efforts and to build upon or adapt them to best support UK resilient PNT needs.

The UK resilient PNT guidelines could, e.g. include a recommended sequence of steps for identifying and appropriately mitigating threats to ensure continued safe, secure and economically beneficial operational environments, such as:

1. Power up and declare initialisation stage
2. Perform any self-checks
3. Declare normal operational status or error state
4. Detect and warn of the presence of a threat condition, problem, attack
5. Warn of reduced performance level or unusable data affecting P and/or N and/or T
6. Maintain trustable behaviour in the presence of the threat or advise of reduced or loss of required P/N/T services
7. Monitor environment and return autonomously to normal/full operation when possible
8. Report to user initial assessment, operational and update status and return to step 1 or 2, as required

Verifying that this sequence can be followed by the system during each proposed threat/event listed in the guidelines would provide the CNI with some level of confidence that their PNT system would be resilient to attacks. A full and detailed set of guidelines may include specific examples across UK CNI, e.g. the timing receivers used for the National Grid may use a different sequence of stages than the navigation receivers used by the Defence sector.

The guidelines should also inform on the likelihood and level of threats, ideally categorised by CNI. It is likely that there will be a universal minimum set and that different CNI Sectors may each have extra threats to test based on their unique needs and/or operational environments. An example set of threats are listed here. The guidelines would recommend that the PNT system be checked for its behaviour during the exposure to the threat and that the system returns to the desired provision of PNT information (with or without assistance as required) when the threat is no longer present during:

- Power cycling
- Temporary removal/replacement of each sensor input (e.g. detaching an antenna)
- Saturation interference/jamming of any sensor that detects and processes electromagnetic radiation
- Signal/input replay attacks of any sensor that detects and processes electromagnetic radiation
- Meaconing (live rebroadcast attacks) of any sensor that detects and processes electromagnetic radiation
- Spoofing
- Specific threats, hazards or scenarios that could reasonably be encountered during operations by a particular CNI

Clearly, the working group will need to draw from a large enough pool of expertise to identify, define, describe in detail this set of threats appropriately for each CNI. The Royal Institute of Navigation is well placed to establish this working group from its network of PNT experts.

Ideally each CNI would also provide or nominate a representative to support the WG to assist with sector-specific analyses.

Developing, implementing and maintaining UK PNT guidelines and best practises should involve several organisations and stakeholders, including:

- The UK government, through agencies such as the Department for Science Innovation and Technology (DSIT) and the National Cyber Security Centre (NCSC), could play a key role in developing and maintaining Resilient PNT guidelines for the UK. They could also mandate or incentivise conformance to the guidelines if considered appropriate.
- Industry groups, such as the Rail Safety and Standards Board (RSSB), the Atomic Weapons Establishment, [and many others], could play a key role in developing and maintaining the guidelines, as well as working with industry to implement them.
- Universities and research institutions could provide valuable input and expertise in the development and maintenance of the guidelines, through research and development in the field of PNT.
- Standards organisations, such as the British Standards Institution and the National Physical Laboratory, could play a key role in developing and maintaining the guidelines into various PNT standards, as well as promoting them internationally.
- International Organisations: The UK government could also work with international organisations, such as the International Civil Aviation Organization and the International Telecommunications Union, to develop and promote Resilient PNT guidelines.

Conclusions and recommendations

This paper's conclusions are

a) There is no current standard for resilient PNT that would satisfy the needs of all UK CNI sector users and use cases.
b) While the IEEE P-1952 standard is an example of work in progress on this topic, the task is very challenging due to the extensive range of sensors, methods and technologies in use across all PNT systems.
c) Mandating that PNT systems used to support CNI applications must conform and be certified to use-case category specific minimum PNT resilience standards could bring benefits such as incentives to develop appropriate resilient PNT systems (or systems-of-systems) and ensure a broad CNI customer base. Such a mandate would be independent of any decision to develop a sovereign UK PNT capability with high resilience designed from the inception. If such a capability existed, it would represent a complementary PNT (CPNT) option that manufacturers/users could incorporate into their PNT service solutions to comply with the standard to ensure resilience.
d) A more tractable option for the UK would be to propose a set of best-practice guidelines for resilient PNT based around two key components: a threat-handling workflow and a simple set of tests that are designed to be equipment agnostic but CNI sector specific.
e) A recommendation is to form a small RIN-led working group to develop these guidelines and to propose associated best practices.
f) The working group should contain both PNT subject matter experts and representatives that cover each of the sectors of UK CNI.

The recommendations of this white paper are:

1. Establishment of a small, focussed RIN-led Working Group, composed of PNT experts and representatives of CNI stakeholders, to develop a PNT Resilience Action Plan that identifies specific steps, timeframes and incremental improvements needed to promote an accelerated implementation of resilient PNT services and solutions;
2. Establishment of "Best Practices for Use of PNT by UK CNI Services", by which both PNT users and service providers would be invited to assess their PNT risks and determine the failure modes and effects that result from loss or manipulation of minimum required PNT services; and
3. Consult within RIN and with interested stakeholders as to other contributions RIN can deliver in support of an anticipated overarching UK National PNT strategy.

Annex A – List of existing standards

Standard or Guideline	Body	Description	Relevance to Resilient PNT
Resilient Positioning, Navigation and Timing (PNT) Conformance Framework v2.0	US Dept of Homeland Security	Guidance for the design, development and implementation of resilient PNT systems	High
Standard for Resilient Positioning, Navigation and Timing (PNT) User Equipment	IEEE	This standard specifies technical requirements and expected behaviours for resilient Positioning, Navigation and Timing (PNT) User Equipment (UE).	High
PNT System Resilience	Rethink PNT	Overview of the current state of PNT (positioning, navigation and timing) system resilience and the challenges facing the industry	High
Use of On-Train Satellite Positioning Technology Based Locator for Railway Applications	Railway Safety Standards Board	The standard outlines the technical and performance requirements for PNT systems to ensure that they are able to provide accurate and reliable information even in the event of disruptions or failures.	High
EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure	UK Cabinet Office	This document provides guidelines for telecommunications companies on how to design and implement resilient telecommunications infrastructure in order to ensure the continuity of critical national services	High
National Institute of Standards and Technology. 2021. "SP 800-160 Vol. 2 Rev. 1: Developing Cyber-Resilient Systems: A Systems	NIST	A framework for integrating cyber resiliency into the system development life cycle, covering key aspects such as risk management, security engineering and testing. The document provides specific guidance for various stakeholders, including	High

Security Engineering Approach		system owners, developers, architects and security engineers, to ensure the development of cyber-resilient systems.	
Performance Standards for Multi-System Shipborne Radionavigation Receivers	IMO	The resolution MSC.401(95) outlines performance standards for multi-system shipborne radionavigation receivers. The performance standards cover various aspects of the receivers, including their accuracy, integrity, continuity, availability and resilience. The resolution also emphasises the need for proper installation, testing and maintenance of these receivers to ensure their reliable and effective operation.	Medium
EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure		Guidelines on the resilience of electronic communications networks and services for public electronic communication network providers, national regulatory authorities and other stakeholders in the European Union. It includes recommended measures to improve the ability of electronic communications networks and services to resist and recover from various incidents and emergencies. These guidelines aim to improve the overall resilience of electronic communication networks and services in the EU.	Medium
ISO/IEC 27001: Information technology - Security techniques - Information security management systems	ISO	ISO/IEC 27001 is a standard that provides a framework for establishing, implementing, maintaining and continually improving information security management systems. It specifies requirements for information security management, including risk assessment, security controls and ongoing management and monitoring of the ISMS.	Medium

Further related standards:

NIST SP 800-53:	Security and Privacy Controls for Federal Information Systems and Organizations. This standard provides a set of security and privacy controls for federal information systems, including PNT systems, to ensure their confidentiality, integrity and availability.
IEC 62351:	Power system control and associated communications - Cyber security. This standard provides guidelines for cyber security in power systems, including PNT systems, to ensure their confidentiality, integrity and availability.
ENISA:	Good Practice Guide on Information Security for PNT systems. This standard provides good practice guidelines for information security for PNT systems, including guidelines for risk management, incident management and security requirements for PNT systems.
ISO/IEC 15408:	This standard provides a framework for evaluating the security of IT systems, including PNT systems, to ensure their confidentiality, integrity and availability.
ISO/IEC 27032:	This standard provides guidelines for managing cyber security incidents and ensuring the continuity of PNT systems.

EUROCAE:

ED-36B	MOPS for MLS Airborne Receiving Equipment
ED-114A Ch. 1	MOPS For Global Navigation Satellite Ground Based Augmentation System Ground Equipment To Support Category I Operations - Status: Published
ED-114B	MOPS For Global Navigation Satellite Ground Based Augmentation System Ground Equipment To Support Precision Approach and Landing - Status: Published
ED-259	Minimum Operational Performance Standards for Galileo - Global Positioning System - Satellite-Based Augmentation System Airborne Equipment - Status: Published

ED-259A	Minimum Operational Performance Standard for Galileo - Global Positioning System - Satellite-Based Augmentation System Airborne Equipment - Status: Draft
ED-75D	MASPS Required Navigation Performance for Area Navigation - Status: Published
ED-75E	Minimum Aviation System Performance Standards - Required Navigation Performance for Area Navigation - Status: Draft

RTCA:

RTCA SC-159	Navigation Equipment Using the Global Navigation Satellite System (GNSS)
DO-373	MOPS for GNSS Airborne Active Antenna Equipment for the L1/E1 and L5/E5a Frequency Bands
DO-368	Minimum Operational Performance Standards for GPS/GLONASS (FDMA + antenna) L1-only Airborne Equipment
DO-316	Minimum Operational Performance Standards for Global Positioning System/Aircraft Based Augmentation System
DO-310	Minimum Operational Performance Standards for GPS Ground-based Regional Augmentation System Airborne Equipment
DO-301	Minimum Operational Performance Standards for Global Navigation Satellite System (GNSS) Airborne Active Antenna Equipment for the L1 Frequency Band
DO-253D	Change1 Minimum Operational Performance Standards for GPS Local Area Augmentation System Airborne Equipment
DO-253D	Minimum Operational Performance Standards for GPS Local Area Augmentation System
DO-253C	Minimum Operational Performance Standards for GPS Local Area Augmentation System Airborne Equipment Airborne Equipment
DO-253B	Minimum Operational Performance Standards for GPS Local Area Augmentation System Airborne Equipment

DO-253A	Minimum Operational Performance Standards for GPS Local Area Augmentation System Airborne Equipment
DO-245A	Minimum Aviation System Performance Standards for Local Area Augmentation System (LAAS)
DO-229E	Minimum Operational Performance Standards for Global Positioning System/Satellite
DO-229E	Minimum Operational Performance Standards for Global Positioning System/Satellite-Based Augmentation System Airborne Equipment
DO-229D	Minimum Operational Performance Standards for Global Positioning System/Satellite Based Augmentation System Airborne Equipment
DO-229C	Minimum Operational Performance Standards for Global Positioning System/Wide Area Augmentation System Airborne Equipment
DO-228	Minimum Operational Performance Standards for Global Navigation Satellite Systems (GNSS) Airborne Antenna Equipment
DO-217	Minimum Aviation System Performance Standards DGNSS Instrument Approach System: Special Category I (SCAT-I) Revised to include Change 1
DO-208	Minimum Operational Performance Standards for Airborne Supplemental Navigation Equipment Using Global Positioning System (GPS)
DO-202	Report of Special Committee 159 on Minimum Aviation System Performance Standards (MASPS) for Global Positioning System (GPS)
CTF-1	RTCA Task Force 1 Report on Global Navigation Satellite System (GNSS) Transition and Implementation Strategy

ETSI:

ETSI TS 103 252 V1.1.1 (2015-06) Satellite Earth Stations and Systems (SES); Assisted GNSS logical channel for a broadcast system

ETSI TS 103 246-3 Satellite Earth Stations and Systems (SES); GNSS based location systems; Part 3: Performance requirement

ETSI TS 138 171 5G; NR; Requirements for support of Assisted Global Navigation Satellite System (A-GNSS) (3GPP TS 38.171 version 15.3.0 Release 15)

ETSI TS 136 171 LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Requirements for Support of Assisted Global Navigation Satellite System (A-GNSS) (3GPP TS 36.171 version 16.1.0 Release 16)

ETSI TR 103 183 V1.1.1 (2012-10) Satellite Earth Stations and Systems (SES); Global Navigation Satellite Systems (GNSS) based applications and standardisation needs

ETSI TR 101 593 V1.1.1 (2012-09) Satellite Earth Stations and Systems (SES); Global Navigation Satellite System (GNSS) based location systems; Minimum performance and features

ETSI TS 103 246-4 V1.2.1 (2017-03)Satellite Earth Stations and Systems (SES); GNSS based location systems; Part 4: Requirements for location data exchange protocols

ETSI TS 137 355 LTE; 5G; LTE Positioning Protocol (LPP) (3GPP TS 37.355 version 16.1.0 Release 16)

ETSI TS 136 355 LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); LTE Positioning Protocol (LPP)

ETSI TS 151 010-7 Digital cellular telecommunications system (Phase 2+); Mobile Station (MS) conformance specification; Part 7: Location Services (LCS) test scenarios and assistance data

ETSI EN 303 413 Satellite Earth Stations and Systems (SES); Global Navigation Satellite System (GNSS) receivers; Radio equipment operating in the 1 164 MHz to 1 300 MHz and 1 559 MHz to 1 610 MHz frequency bands; Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU

ETSI EN 302 645 Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices; Global Navigation Satellite Systems (GNSS) Repeaters; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive

ETSI TS 138 3055G; NG Radio Access Network (NG-RAN); Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN

ETSI TS 136 305 LTE; Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Stage 2 functional specification of User Equipment (UE) positioning in E-UTRAN

ETSI TS 134 172 Universal Mobile Telecommunications System (UMTS); Terminal conformance specification; Assisted Global Navigation Satellite Systems (A-GNSS); Frequency Division Duplex (FDD)

ETSI EN 301 489-19 ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 19: Specific conditions for Receive Only Mobile Earth Stations (ROMES) operating in the 1,5 GHz band providing data communications and GNSS receivers operating in the RNSS band (ROGNSS) providing positioning, navigation and timing data; Harmonised Standard covering the essential requirements of article 3.1(b) of Directive 2014/53/EU

ETSI TS 144 031 Digital cellular telecommunications system (Phase 2+) (GSM); Location Services (LCS); Mobile Station (MS) - Serving Mobile Location Centre (SMLC) Radio Resource LCS Protocol (RRLP)

ETSI TS 125 173 Universal Mobile Telecommunications System (UMTS); Requirements for support of Assisted Galileo and Additional Navigation Satellite Systems (A-GANSS) Time Division Duplex (TDD)

ETSI TS 125 172 Universal Mobile Telecommunications System (UMTS); Requirements for support of Assisted Galileo and Additional Navigation Satellite Systems (A-GANSS) Frequency Division Duplex (FDD)

ETSI EN 302 890-2 (On Approval) Intelligent Transport Systems (ITS); Facilities Layer function; Part 2: Position and Time management (PoTi)

ETSI TS 143 059 Digital cellular telecommunications system (Phase 2+) (GSM); Functional stage 2 description of Location Services (LCS) in GERAN

ETSI EN 303 098 Maritime low power personal locating devices employing AIS; Harmonised Standard for access to radio spectrum

ETSI TS 125 453 Universal Mobile Telecommunications System (UMTS); UTRAN Iupc interface Positioning Calculation Application Part (PCAP) signalling

ETSI TR 102 893 Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)

ETSI TR 102 496	Electromagnetic compatibility and Radio spectrum Matters (ERM); System Reference Document; Short Range Devices (SRD);

SAE International:

SAE 6857	Requirements for a Terrestrial Based Positioning, Navigation and Timing (PNT) System to Improve Navigation Solutions and Ensure Critical Infrastructure Security
SAE 9990	Transmitted Enhanced Loran (eLoran) Signal Standard
SAE PNT	Committee Work in Progress
SAE 1004	Raw Measurements from Global Navigation Satellite System (GNSS) Receivers
SAE 1012	Global eLoran User Equipment Interface Standard
SAE 1013	Guidelines for Resilient GNSS Receivers
SAE 1014	Standard for Interfacing Resilient GNSS Receivers
SAE 1015	Improving the Accuracy, Availability, Integrity, Continuity, or Coverage of Positioning, Navigation and/or Timing Solutions Using Raw Measurements from Global Navigation Satellite System (GNSS) Receivers
SAE 1016	Security and Resilience Recommendations for Positioning, Navigation and Timing (PNT) Users
SAE 2020	Inertial Measurement Unit (IMU) Interface Requirements for Military and Aerospace Vehicle Applications
SAE 2021	Simulated Inertial Measurement Unit (IMU) Interface Requirements for Military and Aerospace Vehicle Applications
SAE 2022	Test Plan for the SAE2020 Inertial Measurement Unit (IMU) Interface
SAE 9980	Specification of The Transmitted Loran-C Signal
SAE 9991	Receiver Standard for the Transmitted eLoran Signal

SAE 9992	Introduction to the Operation and Use of the Transmitted Enhanced Loran (eLoran) Signal
SAE 9993	A Guideline for Using the Transmitted Enhanced Loran (eLoran) Signal for Timing, Phase and Frequency

References

1 National Institute of Standards and Technology. 2021. "SP 800-160 Vol. 2 Rev. 1: Developing Cyber-Resilient Systems: A Systems Security Engineering Approach (Supersedes SP 800-160 Vol. 2 (11/27/2019))." Authors: Ron Ross, Victoria Pillitteri, Richard Graubart, Deborah Bodeau, Rosalie McQuaid. https://doi.org/10.6028/NIST.SP.800-160v2r1.
2 https://www.iag-aig.org/doc/5d12072a94e91.pdf
3 UK National Quantum Technologies Programme https://uknqt.ukri.org/
4 DIRECTIVES FOR THE NEGOTIATION OF A NEW PARTNERSHIP WITH THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND Brussels, 25 February 2020 https://www.consilium.europa.eu/media/42736/st05870-ad01re03-en20.pdf
5 Press Release from the Prime Minister's Office "UK to tell EU it will no longer seek access to secure aspects of Galileo" 1 December 2018 https://www.gov.uk/government/news/uk-to-tell-eu-it-will-no-longer-seek-access-to-secure-aspects-of-galileo
6 CEBR report "The Economic Contribution of Standards to the UK Economy" June 2015 https://www.bsigroup.com/LocalFiles/en-GB/standards/BSI-The-Economic-Contribution-of-Standards-to-the-UK-Economy-UK-EN.pdf
7 IEEE P1952 - RESILIENT POSITIONING, NAVIGATION and TIMING USER EQUIPMENT WORKING GROUP https://sagroups.ieee.org/p1952/
8 USA Department of Homeland Security Science and Technology Directorate. The Resilient Positioning, Navigation and Timing (PNT) Conformance Framework https://www.dhs.gov/sites/default/files/2022-05/22_0531_st_resilient_pnt_conformance_framework_v2.0.pdf