Protecting the UK Infrastructure: A System to Detect GNSS Jamming and Interference

Andy G. Proctor & Charles W. T. Curry, *Chronos Technology Ltd.*
Jenna Tong & Robert Watson, *University of Bath*
Mark Greaves & Paul Cruddace, *Ordnance Survey*

Abstract

The vulnerability of space based position navigation and timing (PNT) systems to RF interference sources is becoming well known outside of the traditional PNT sector for example, into the critical infrastructure operations area. Risk managers of organisations in this area are becoming aware of the vulnerabilities and dependencies in using space based PNT systems. This paper presents work performed and work on-going in the UK, to develop capabilities that provide detection and early warning for operators of critical infrastructure and law enforcement agencies (LEA), to the presence of RF interference in the bands associated with space based PNT. These capabilities can detect and will be able to locate source(s) of RF interference which allows infrastructure operators and LEA to take advantage of quality of service and trust concepts when applied to these space based PNT systems. This paper also presents a case study of the detection of an intentional RF interference device, which impacted upon one organisation's critical infrastructure.

Introduction

GNSS vulnerability is rightly one of the most talked about topics of 2011. Publicity such as the "accidental" GPS jamming at the Newark Airport in the United States [1-2], the Royal Academy of Engineering report [3] regarding the vulnerability of UK GNSS services, the recent investigations into the LightSquared "problem," [4] numerous conference presentations [5-6], and articles in news media [7] — all address the well-known fact that space-based position, navigation, and timing (PNT) is vulnerable to localised RF interference at or near to the receiver operating frequency.

Some of this publicity relates to the UK's developments in the area of detecting GNSS interference, specifically the GAARDIAN (GNSS Availability, Accuracy, Reliability anD Integrity Assessment for Timing and Navigation) program [6], which was a wide collaboration between government, academia, and industry to develop a robust system for analysing interference phenomena associated with GPS and eLoran systems and the effects on their use in safety- and mission-critical applications.

The GAARDIAN program completed in 2011, this paper gives an overview of the resulting capability to detect GNSS interference and jamming. It also provides details about a specific recent detection event that demonstrated the capability of the system and that, by involving UK Law enforcement agencies, proved the system can be operationally effective. It also gives an overview of the continuing development of this technology under the SENTINEL program.

GAARDIAN

GAARDIAN, a collaboration led by Chronos Technology Ltd., included the University of Bath, General Lighthouse Authorities of UK and Ireland, BT, Ordnance Survey, National Physical Laboratory, and Imperial College London. The project was part-funded by the UK's national

innovation agency, the Technology Strategy Board, and ran between October 2008 and March 2011. The project set out to create interference detection and monitoring sensors (IDMs) that could be deployed in the vicinity of safety- and/or mission-critical PNT applications. These sensors or probes had a design brief to monitor the integrity, reliability, continuity, and accuracy of the locally received GPS and eLoran signals on a round-the-clock basis and report back to a central server, which acts as the user interface. Users were to be alerted in real time to any anomalous behaviour in either of the GPS and eLoran signals. This concept can also be considered a GNSS/PNT quality of service (QoS) monitoring and reporting system.

System Design

The GAARDIAN program has resulted in a 24x7 nationwide experimental IDM system, whose sensors continuously monitor PNT signals from both GPS and eLoran. GPS is the main GNSS technology monitored, but integration of other GNSS technologies is certainly possible. eLoran is an alternative PNT technology unaffected by interference to GPS and technically dissimilar in its dependencies, e.g., operating at different frequencies and using separate infrastructure from GNSS. The design of the GAARDIAN architecture consists of three main elements: probe, server, and communication.

The probe shown in Figure 1, acts as a semi-portable station that executes specialised functions to detect anomalous events and failures of GPS or eLoran, in the vicinity of the probe. The station also processes data obtained by the probe to reduce the amount that needs to be transmitted to the central server. The server's role is to manage and process the data received from probes and external sources including the Ordnance Survey's OS Net network of permanent GNSS receivers. The server offers the users real-time access to the output of these probes (including anomalous events) and dedicated system (GPS and eLoran) positioning/timing performance. Furthermore, it provides the probes with information on failures that have a regional impact.

Both the probes and the server contain specialist monitoring algorithms from the consortium partners, with the integration and normalisation having been carried by Chronos' UK staff.

FIGURE 1: GAARDIAN probe as deployed around the UK

The probe is designed to be adaptable to various user applications, and specific functionality can be enabled or disabled depending on user requirements. Every probe performs a minimum set of functions:

- Interference detection
- Failure identification
- Data capture during anomalous events
- eLoran validation

The specific functionality of the probes and the server, summarised above are based on these activities. For example, assessment of conditions such as space segment failures can be performed to ensure an event is due to a localised problem and not systematic.

Figure 2 outlines the basic probe architecture in which the outputs from a GPS receiver, an eLoran receiver, and a small form factor rubidium atomic clock are analysed. One form of analysis performed is an investigation of the 1PPS output of the two PNT sources against a common reference.

A time interval error (TIE) measurement of these outputs is conducted continuously over multiple sample window sizes. This is converted to maximum time interval error (MTIE) and compared with a predefined limit. This enables short-, medium-, and long-term timing anomalies to be reported. Not only does this feature enable the detection of multipath, interference, and system anomalies in the GPS signal, it also

provides a readymade QoS service should eLoran become the accepted technological alternative PNT to GPS or for adopters of the future Galileo Publicly Regulated Service (PRS).

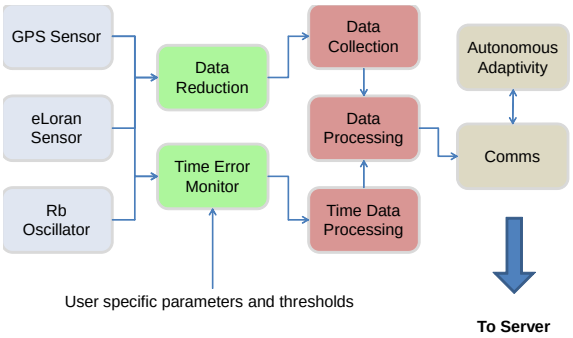

FIGURE 2: Simplified probe architecture

MTIE is the largest peak-to-peak TIE (i.e., wander) in any observation interval of length *t*, calculated as follows:

$$\mathrm{MTIE}(n\tau_0) \cong \max_{1\le k\le N-n}\left[\max_{k\le i\le k+n} x_i - \min_{k\le i\le k+n} x_i\right], \quad n = 1,2,\ldots,N-1$$

EQUATION 1: Maximum time interval error

where *n* is the number of samples in the measurement window, τ_0 is the sample interval, *N* is the number of samples in the data set. The index variable *i* is incremented to scan across the window and *k*, representing the starting point of the current data set, is incremented for sliding the measurement window.

This principle can be used to set thresholds of maximum allowable TIE, which when exceeded can be flagged as an alert. Figure 3 shows some early experimental data that compares a GPS 1PPS to a cesium standard, with a jump in the TIE when a system anomaly occurs. In the example data, the operation of a GPS repeater is causing the reaction.

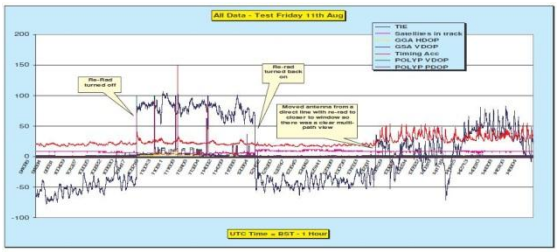

FIGURE 3: Example TIE plot showing the responsiveness to GNSS anomaly

In addition to this TIE measurement, the probe characterises the GNSS RF multipath environment by using the Signal-To-Noise Ratio (SNR), azimuth and elevation values to determine a mask for "normal" signal strength and extract some multipath parameters. An interference event can then be said to occur when the SNR for a [user-configurable] number of satellite drops below an expected tolerance, which takes into account the multipath conditions and the variance of the SNR of the normal state.

This means that a probe can, if necessary, be deployed into a strong multipath environment. Over the course of the GAARDIAN program, the time required for the normal state determination was reduced to a level that enables the rapid deployment of a probe to a location of interest, a concept being used in the successor program, SENTINEL[1] (Figure 4).

[1] GNSS SErvices Needing Trust In Navigation Electronics Location and timing, a part Technology Strategy Board funded program, led by Chronos Technology

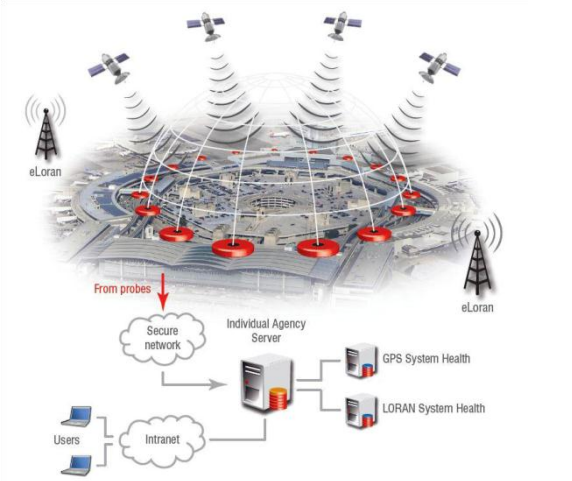

FIGURE 4: SENTINEL overview

Probes are currently deployed at various locations around the UK and Ireland and continuously report on the integrity, continuity, accuracy, and reliability of the PNT signals in their vicinity. The data is continuously available via a common web browser, making the complex data accessible quickly and easily. Figure 5 shows the server's graphical user interface through which users are alerted and, in turn, can access data from individual probes and perform detailed event analysis.

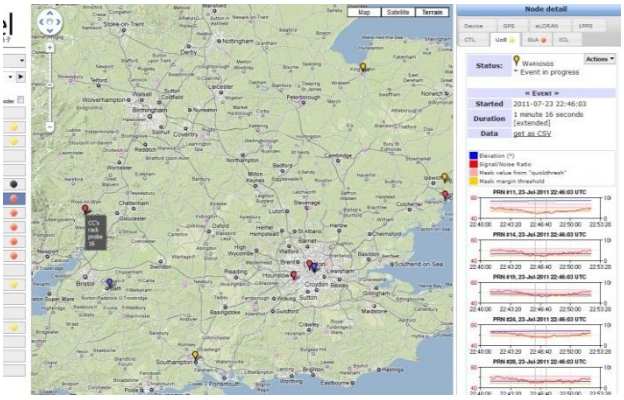

FIGURE 5: GAARDIAN/SENTINEL server interface

Server side analysis tools include the ability to perform historical trend analysis of both the GPS and eLoran data from the probes. These tools enable operators and users to monitor long-term factors, such as the eLoran *additional secondary factor* (ASF) variations, and analyze long-term GPS QoS metrics and event patterns.

This pattern analysis capability was used during a recent investigation by the GAARDIAN program team, which will be described next.

Event Investigation

GAARDIAN as a research tool has delivered a number of key firsts in the field of GPS interference detection; eLoran monitoring techniques and GPS multipath characterisation. Even though only an experimental rather than operational system, one of the partners, Ordnance Survey, requested that a GAARDIAN probe was moved to a specific site of interest in the UK.

This article will not detail the location of this probe, but the reason for the deployment was that an Ordnance Survey OS Net reference station at the location was experiencing significant failures. The OS Net network, consisting of more than 100 continuously operating GNSS receivers, facilitates a core geodetic remit of Ordnance Survey as well as providing data and services for internal and commercial GNSS correction services across the whole of Great Britain. Therefore, failure of an OS reference station, particularly intermittent failure, has a significant effect on business continuity because of the resulting data loss.

Deployment of the GAARDIAN probe to the site of the OS Net reference station represented the first operational deployment of the system in the UK. Installation and set-up work by Chronos Technology meant that the same RF environment as seen by the reference station was also seen by the probe. Although the probe detected immediate loss-of-signal events, the program team allowed the probe to gather three weeks' worth of data before full analysis was undertaken.

Human or Natural?

The analysis showed two clear and distinct types of event; Figure 6 shows an example of the first event type, dubbed internally as "Short Shallow Fat" or SSF. The figure shows carrier/noise values against time, and the event is clearly visible. This event was found to be sidereal in nature and therefore discounted as the cause of the problem.

The root cause of this first type of event is currently under investigation and not part of this article.

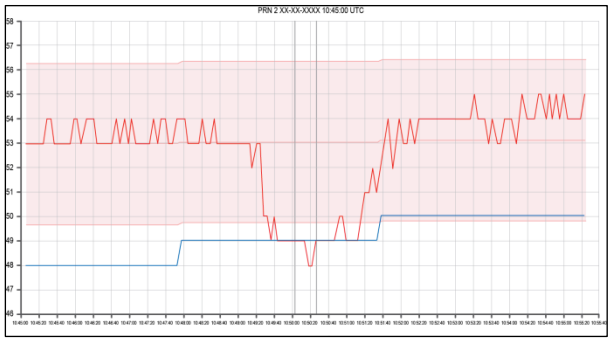

FIGURE 6: "SSF" PRN 2 Alarm Duration 23 seconds. Actual Event ~ 2 minutes

Figure 7 shows the second type of event detected by the GAARDIAN probe. Its signature was christened internally as "Deep Short Sharp" or DSS. Again, the event can be clearly seen in the data and was found to have an average duration in the order of only a few seconds. This was the event that correlated each time with the loss of lock experienced by the OS Net reference receiver. The DSS event affected signals from all satellites in view at the time of the event.

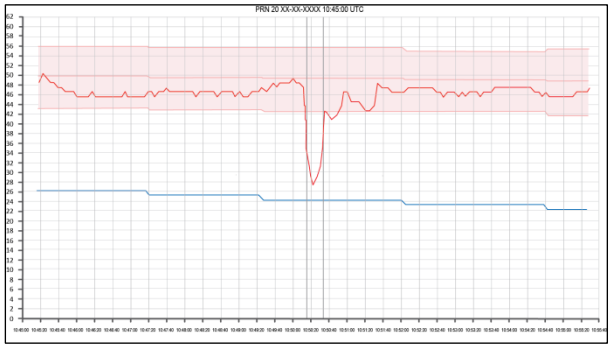

FIGURE 7: "DSS" PRN 20 Alarm Duration 18 seconds

Detailed analysis concentrated on the DSS profile, particularly the frequency of occurrence, looking for trend patterns. This analysis showed that the event exhibited regularity in terms of days of the week upon which it occurred. The event also changed activity during a public holiday (e.g. an expected Monday event happened on a Tuesday as Monday was a public holiday). In addition to other indicators that cannot be detailed here, this pattern led the team to suspect it was not caused by a natural event, but rather by manmade means.

Enforcement

To progress this analysis further and to bring the OS Net reference site back to full and reliable operation clearly called for some "on the ground" investigation and mitigation. During the GAARDIAN program, strong links were forged with elements of UK law enforcement and culminated in the SENTINEL program. This activity included gaining the UK Association of Chief Police Officers ITS Working Group (ACPO ITS) as a full partner. Discussions with ACPO ITS and other law enforcement agencies (LEAs) allowed the GAARDIAN team to compile a confidential report on the events described here, which led to the deployment of LEA assets to the vicinity of the site in question.

Small, handheld detection devices, Figure 8, were used to aid in localising any interference source, as GAARDIAN itself cannot provide a location or bearing of the interference source. (*This latter capability is part of the SENTINEL program*.)

FIGURE 8: Handheld GPS interference detection device

For reasons of operational security, this paper cannot provide specific details of the LEA operation nor describe how the GAARDIAN team further contributed. We can say, however, that the LEA ground operation did identify a source of the interference, which was identified as one of the vehicle based GPS jamming devices seen frequently on the Internet and as described in the Royal Academy of Engineering report on GNSS vulnerabilities.

As a result of this event analysis, the initial assessment that the problem was manmade was proven correct. Action by the appropriate UK authorities, including LEAs was taken, and a jamming device recovered. This device is being analysed by the SENTINEL team on behalf of the UK LEAs and as part of the testing capability for the SENTINEL program.

Case Study

This detection and recovery case study has shown that the GAARDIAN system, although an experimental network, is fully capable of detecting deliberate and accidental GPS interference & jamming. And, as the case described here demonstrates, it is capable of being the primary detection sensor used in an operational law enforcement environment. Detection of interference events lasting just a few seconds has shown to be possible.

We should also note that occasional variants of the DSS profile described in the article exhibited a "tail," i.e., a shallow recovery back to a normal signal/noise state. This was subsequently identified as a waiting period by the vehicle emitting the jamming signal at nearby traffic lights.

As collateral benefits of the GAARDIAN project in addition to achieving the core goals of GPS interference detection, additional capabilities have been realised, such as long-term eLoran ASF monitoring and calibration, differential eLoran calculations, and the introduction of a multiple technology PNT QoS monitoring system.

SENTINEL

During the GAARDIAN program it was clear to the team that although the requirements for GAARDIAN did not call for them, capabilities were missing from the system which would bring additional operational benefits. Clearly if a system can detect the presence of GPS interference and jamming, then it could (or should) in some form be used to locate the source of the interference and jamming. This concept can be taken further to categorise instances of jamming, enabling LEAs to build up an intelligence framework. The system could (or should) also deliver a measure of trust to safety-, and mission-critical services operators such that they can determine if their applications and systems, which depend upon PNT technology, are liable to compromise and/or degradation. A further capability not present in the GAARDIAN requirements is to determine and understand the extent and nature of the problem of GPS jamming in the UK as a whole. These additional capabilities form a part of the research and deliverables of the SENTINEL (GNSS SErvices Needing Trust In Navigation Electronics Location and timing) program, which again is a collaborative program in part funded by the Technology Strategy Board and led by Chronos Technology. Partners for this program include the University of Bath, General Lighthouse Authorities of UK and Ireland, Ordnance Survey, National Physical Laboratory, ACPO (as previously discussed) and Thatcham Vehicle Security.

Figure 4 shows the basic concept of SENTINEL and the technological approach taken for GAARDIAN remains a valid first step in delivering the aims of SENTINEL. New steps for SENTINEL therefore are:

- Research into interference & jamming localisation - geo-location of the interference or jamming, investigating Angle-of-Arrival, Time-Difference-of-Arrival and power measurement techniques
- Development of additional algorithms for the detection of high-level "above the receiver noise-floor" interference
- Development of algorithms for the detection of interference "below the receiver noise-floor", "GNSS like" signals to determine if they are legitimate GNSS signals, jamming, or perhaps spoofing signals
- Determination of specific user and system requirements for a GNSS interference detection system

- Research into the extent and nature of the criminal use of GPS jammers in the UK
- Development of algorithms for the discrimination between space weather effects upon GNSS services and intentional jamming

The last bullet above is particularly relevant to the next 18 months as the next "Solar Maximum" is scheduled for 2012/13. It is a known fact that solar maxima can have severe impact on the economy with (for example) significant disruption to power utilities and satellite (including GPS) services.

The proliferation of GPS enabled services since the last solar maximum in 2002 means that many mission/safety critical applications have never been tested under space weather conditions. Figure 9 shows this solar cycle.

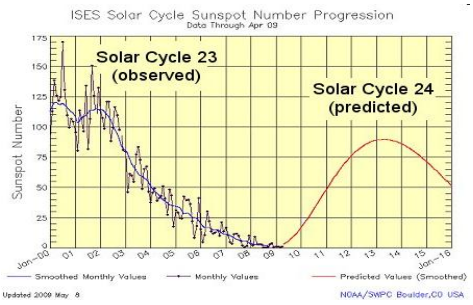

FIGURE 9: Solar cycle observations and predictions 2000-2016

Converging requirements

SENTINEL has adopted a rigorous user requirements approach to enable any subsequent deployment to be fast, agile and importantly cost-effective. The user requirements are set against the background of existing and predicted threat scenarios and have been developed by a cross-government requirements analysis team led by ACPO using the 'Converge' systematic requirements methodology. This means that testing throughout the program has direct correlation to a real world scenario and thus capability proving and demonstration is built into the plan from the start.

The Converge process has determined both functional and operational requirements upon which the system will be based, and as they are based around threat scenarios and use-cases, strong testing plans can be developed alongside the technical development stream. This leads to strong key success criteria ultimately leading to user acceptance criteria, a key aspect of any operationally deployed system.

Additional Events

Within this use case and threat scenario approach, re-deployment and upgrade of sensors from the GAARDIAN program has and will continue to be carried out to take advantage of the previous technical approach and to keep project costs low. These re-deployments are starting to deliver significant results both in terms of increasing the project teams' knowledge of the extent of interference to critical infrastructure, framing the technical priorities within the boundaries set by the user requirements, and also by delivering data to infrastructure operators about their vulnerability to GNSS outages and the impacts on systems. Where possible, results from these redeployments will be published.

Conclusion

The GAARDIAN technology mentioned in this paper clearly showed that the technical approach is fit for purpose within the bounds of an experimental system, and work is on-going to take this forward, via the SENTINEL program to have increased capability and operational functions. SENTINEL differs from GAARDIAN in some key areas, specifically incorporating capabilities for determining the location of an interference source, spoofing detection and providing a measure of trust in a PNT system.

GAARDIAN thus fulfils the role called for by the original design concept. Further work would be needed to integrate the server and probe functionality within a customers' existing monitoring infrastructure, or perhaps to form the core of a monitoring system that needed to be implemented from the ground up. A number of

avenues are currently being explored in this respect.

Cooperation between the GAARDIAN team and UK LEAs, based on analysis of GAARDIAN data, enabled a quick and effective identification of the source of radio interference. GAARDIAN data was an invaluable aid to decision making on the ground, which not only proved successful but also avoided the need for potentially protracted and costly law enforcement investigation.

SENTINEL is taking the basic research from GAARDIAN and bringing the capabilities needed for users to a detection system. The program is also taking forward the eLoran technology and bringing QoS concepts to PNT systems in general and not just satellite based systems. Further results from the SENTINEL program will be published when available.

It is clear that the UK government, through primarily the UK Innovation Agency, the Technology Strategy Board is taking a lead in the sponsorship and encouragement of GNSS interference detection technology and both GAARDIAN and SENTINEL are strong examples of this lead.

Acknowledgements

An abridged version of this paper was published in the September/October 2011 InsideGNSS magazine and the authors would like to acknowledge the contribution and editorial advice of Glen Gibbons to this article.

In addition the authors would like to acknowledge the Technology Strategy Board for the role they have and continue to play in both the GAARDIAN and SENTINEL programs.

References

[1] Doherty, J. (2010). A*lternate position Navigation and Timing Initiative – The need for robust navigation*. Presented at NAV2010, London, UK.

[2] National PNT Advisory Board. (2010). *Jamming the Global Positioning System - A National Security Threat: Recent Events and Potential Cures*. National PNT Advisory Board.

[3] The Royal Academy of Engineering. (2011). *Global Navigation Space Systems: reliance and vulnerabilities.* London. The Royal Academy of Engineering

[4] United States Global Positioning System Industry Council. (2010). *Overview of the Final Report of the Working Group Established by the FCC to Study Overload/Desensitization Interference on GPS Receivers and GPS-Dependent Applications from LightSquared Terrestrial Broadband Operations*. USGIC

[5] Grant, A. Williams, P. Ward, N. (2010). *The Potential effects of GPS Jamming on Marine Navigation*. Presented at NAV2010, London, UK.

[6] Proctor, A. (2010). *GAARDIAN UPDATE*. Presented at NAV2010, London, UK

[7] Gibbons, G. (2010). *UK Focuses on GPS Jamming & Interference*. Retrieved October 2010 from http://www.insidegnss.com/node/1934

Biographies

Andy Proctor holds Master's degree in strategic sales & management and is the GNSS Divisional Manager at Chronos Technology. He spent 12 years in the Royal Navy, leaving in 1998 as a chief communications and electronic warfare engineer. He joined a GNSS and wireless testing company, holding a number of roles over 10 years, including global customer support, technical (including training), and sales. During this time Proctor was involved in the development of the A-GPS standard for 3GPP and GCF/PTCRB. He later managed a wireless/GPS testing facility in the UK before moving to the security and intelligence sector with a UK communications systems organisation, in a business development position. At Chronos he manages the development and growth of the GNSS product and service portfolio, including the commercial side of the GAARDIAN

and SENTINEL programs. He is a member of the Royal Institute of Navigation, and a Fellow of the Institute of Sales and Marketing Management.

Charles Curry is a Fellow of the Institution of Engineering and Technology (IET) and founder & Managing Director of Chronos Technology Ltd. Charles graduated in Electronics from Liverpool University in 1973. He founded Chronos, a leading UK system integrator for synchronisation, timing and GNSS products and services, in 1986. Charles founded the International Telecom Sync Forum (ITSF) in 2001 and chairs the ITSF Steering Group. He is also a member of the Workshop in Sync in Telecommunications Systems (WSTS) Steering Group and is on the Steering Group for the Technology Strategy Board's Knowledge Transfer Network (KTN) for Digital Systems - Location and Timing Programme. Charles is also a member of the Industry Advisory Boards for the Universities of Liverpool and Bath, Electrical and Electronics Faculties

Paul Cruddace is the geodesy and positioning manager at Ordnance Survey, Great Britain's national mapping agency. He is responsible for the development and implementation of the overall strategy including the national GNSS infrastructure. He is a chartered surveyor with a background in the use of precise GPS positioning to determine earthquake hazards.

Mark Greaves is one of two geodetic analysts at Ordnance Survey. He holds an M.Sc. in engineering surveying and geodesy and is a member of the Royal Institute of Chartered Surveyors. Greaves specializes in geodetic GNSS computations and analysis. He has worked at Ordnance Survey for over 25 years during which time he has been responsible for several national GNSS network adjustments, including two internationally ratified realizations of the ETRS89 coordinate reference system in Great Britain. He also developed the OSTN02 transformation that relates GNSS measurements to the British National Grid. Greaves has also been in the team responsible for managing and developing the OS Net GNSS network since its inception.

Jenna R. Tong is a postdoctoral researcher at the Electronic and Electrical Engineering Department at the University of Bath. Her first degree was at Imperial College, London, and her Ph.D. in electron tomography was achieved at the University of Cambridge.

Robert Watson received B.Eng. and Ph.D. degrees in electronic engineering from the University of Essex, Colchester, UK. From 1995–1998 he was a senior research officer at the University of Essex where he was involved in a number of radio propagation and remote sensing projects. In October 1998, he joined the academic staff at the Department of Electronic and Electrical Engineering, University of Bath, where he is currently a senior Lecturer. He has consulted widely for industry. His research interests include radio-wave propagation and remote sensing. Watson is a member of the IEEE and Commission F representative to the UK panel for the International Union of Radio Science.