

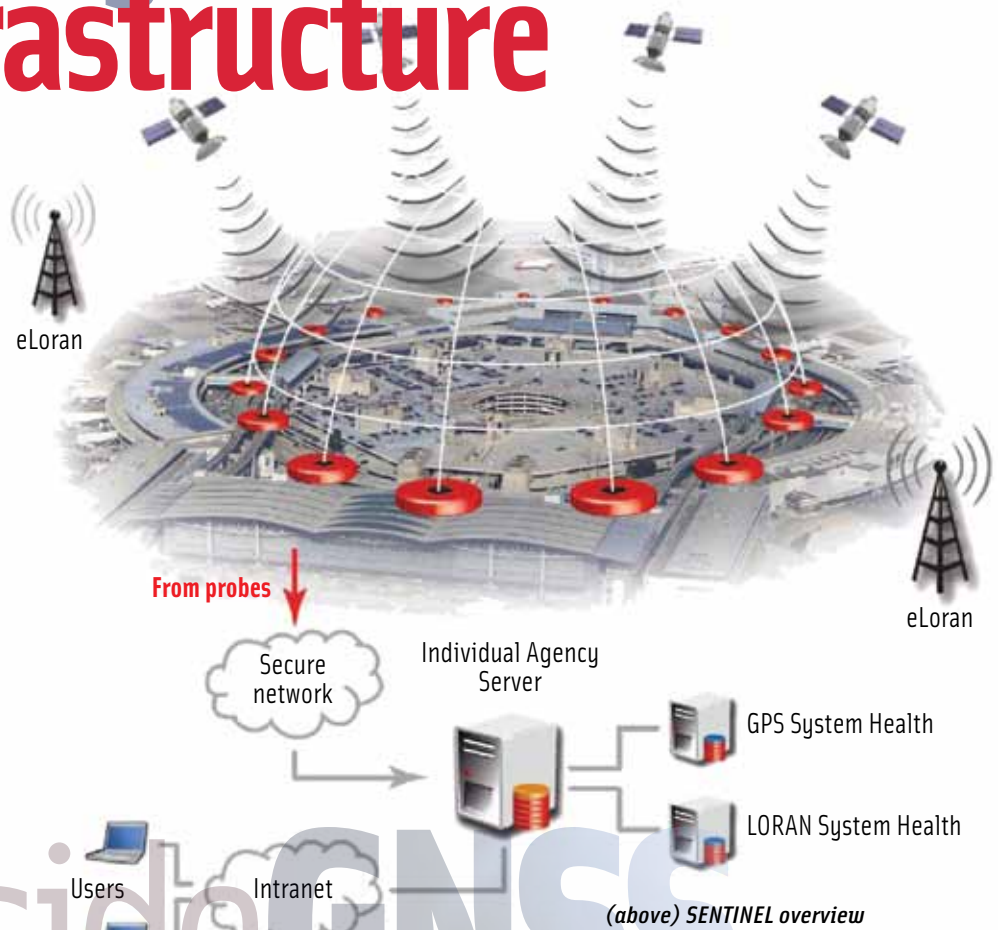
Protecting the UK Infrastructure

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



(above) SENTINEL overview

With concerns about GPS jamming incidents steadily growing, public and private agencies have launched projects to design and test GNSS interference detection and mitigation methods. Among the most advanced of these efforts is a public/private initiative in the United Kingdom that combines GNSS, eLoran, and communication links in a network of monitoring stations that have demonstrated the capability of detecting and identifying the source of intentional interference.

GNSS vulnerability is rightly one of the most talked about topics of 2011.

Publicity of events such as the “accidental” GPS jamming at the Newark Airport in the United States, the Royal Academy of Engineering report regarding the vulnerability of UK GNSS services, the recent investigations into the LightSquared “problem,” numerous conference presentations, and many articles in technical journals and news media — all address the well-known fact that space-based position, navigation, and timing (PNT) is vulnerable to localized 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 GAARD-IAN program (for GNSS Availability, Accuracy, Reliability and Integrity Assessment for Timing and Navigation). This was a wide collaboration between government, academia, and industry to develop a robust system for analyzing 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 article 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.

GAARDIAN's Guardians

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 behavior 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 the accompanying photo, acts as a semi-portable station that executes specialized 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 the probes (including anomalous events) and dedicated system (GPS and eLoran) positioning/timing performance. Further-



GAARDIAN probe as deployed around the UK

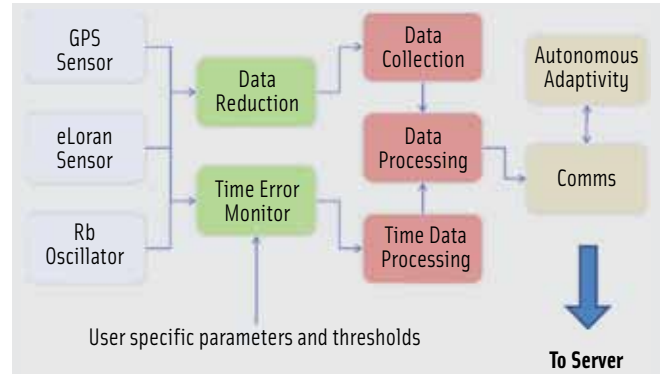


FIGURE 1 Simplified probe architecture

more, it provides the probes with information on failures that have a regional impact.

Both the probes and the server integrated specialist monitoring technologies from the partners, with the integration and normalization being carried out at and by Chronos' UK headquarters premises and staff, respectively.

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 localized problem and not systematic.

Figure 1 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 analyzed. One form of the 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).

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

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

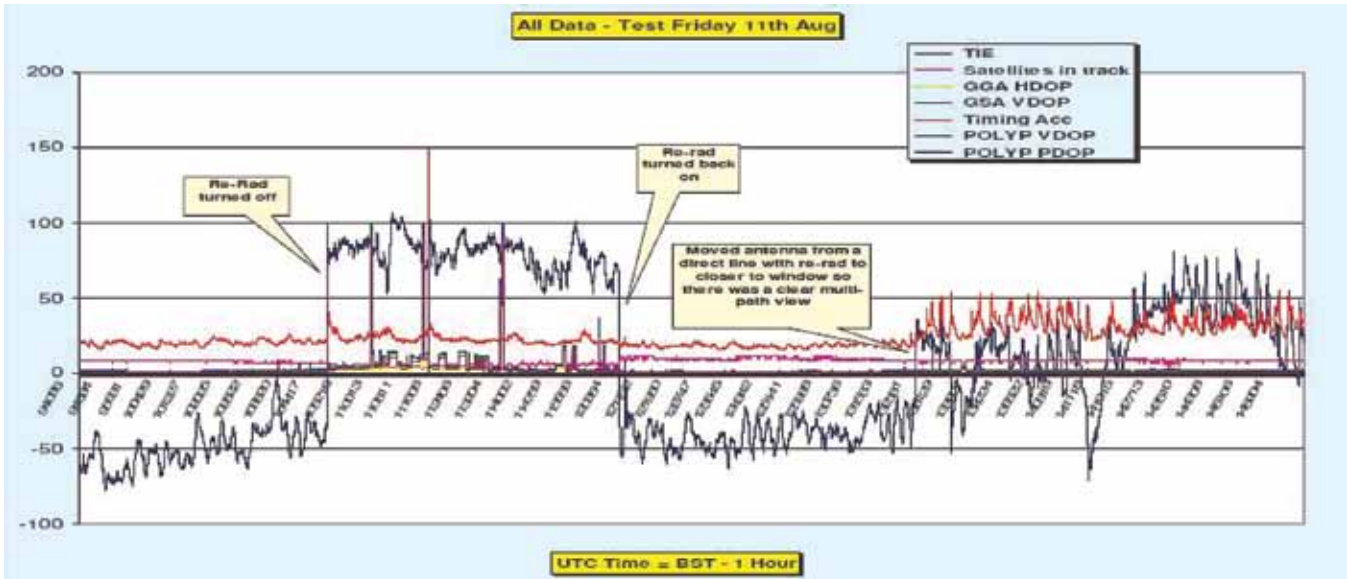


FIGURE 2 Example TIE plot showing the responsiveness to GNSS anomaly

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 2** shows some early experimental data that compares a GPS 1PPS to a cesium standard, with a jump in the TIE when a system anomaly

New GNSS Technology...



...for your Old GNSS System

NovAtel OEM628 for VME BUS Systems with NMEA and Bespoke Output

- Drop-in replacement receiver for legacy VME bus systems
- A straightforward way to upgrade certified systems with minimum risk
- Gives full multi-constellation and SPAN capability to VME systems
- Emulate a NovAtel OEM2 or OEM3 receiver
- Emulate other VME bus receivers
- Carries the OEM628 GNSS receiver and FS-D5 DSP module
- Assembly dimensions do not exceed dimensions of the NovAtel OEM3 receiver
- Direct communication to the OEM628 card via jumper settings for further development options
- Create user specific GNSS data messages to compress data amount at high data rates
- Compatible to carry OEM4-G2L and OEMV-2 instead of OEM628
- Special features available on request
- USB connection with up-to 3 virtual serial ports

FORSBERG
www.forsbergservices.co.uk
 Tel (UK): +44 (0)1524 383320
 Tel (DE): +49 (9367) 9878080
 Email: info@forsbergservices.co.uk

occurs. In the example data, the operation of a GPS repeater is causing the reaction.

In addition to this TIE measurement, the probe characterizes the GNSS RF multipath environment. This is accomplished via an algorithmic comparison of the measured GPS signal/noise ratio (SNR) for each satellite against a pre-calculated polynomial "Quickthresh" mask. This algorithm uses the SNR, azimuth, and elevation values to develop a mask for "normal" signal strength and extract some parameters related to multipath of the probe.

An "event" occurs when the SNR for a [user-configurable] number of satellites has dropped below expected tolerances, leading to the assumption that a multipath or jamming environment may exist. Other parameters are taken into account, such as standard deviation per satellite and the multipath conditions of the "normal" state.

This means that a probe can, if necessary, be deployed into a strong mul-

tipath 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 (see opening image).

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 the vicinity. The data is communicated back to a central location, and continuously available via a common web browser, making the complex data accessible quickly and easily. **Figure 3** 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.

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 we will describe 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 characterization. Even though only an experimental rather than operational system, one of the partners, Ordnance Survey, requested that a GAARDIAN probe be 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

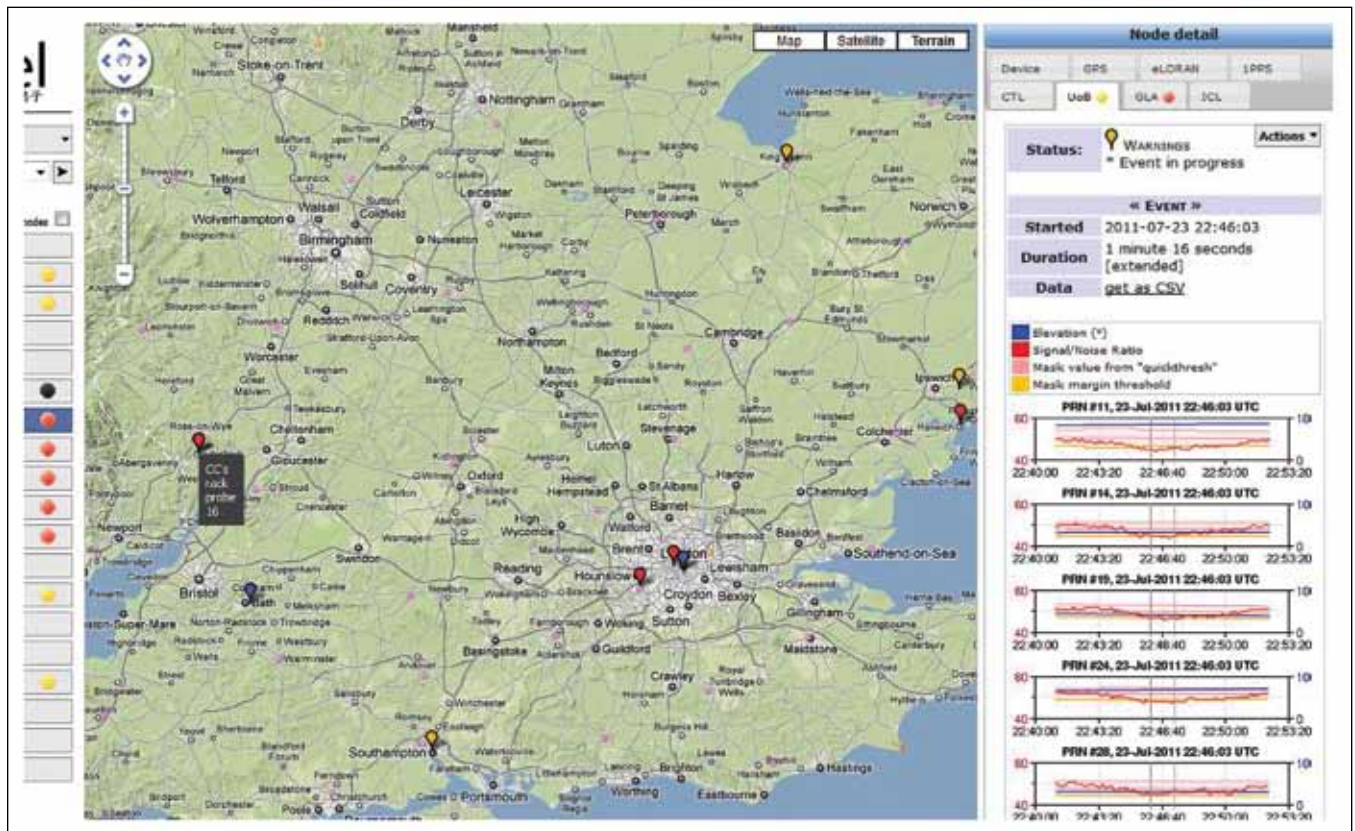


FIGURE 3 GAARDIAN/SENTINEL server interface (location identifiers removed)

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, of any of these reference stations 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 4** shows an example of the first event type, dubbed internally as "Short Shallow Fat" or SSF. The figure diagram 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 5 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.

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.

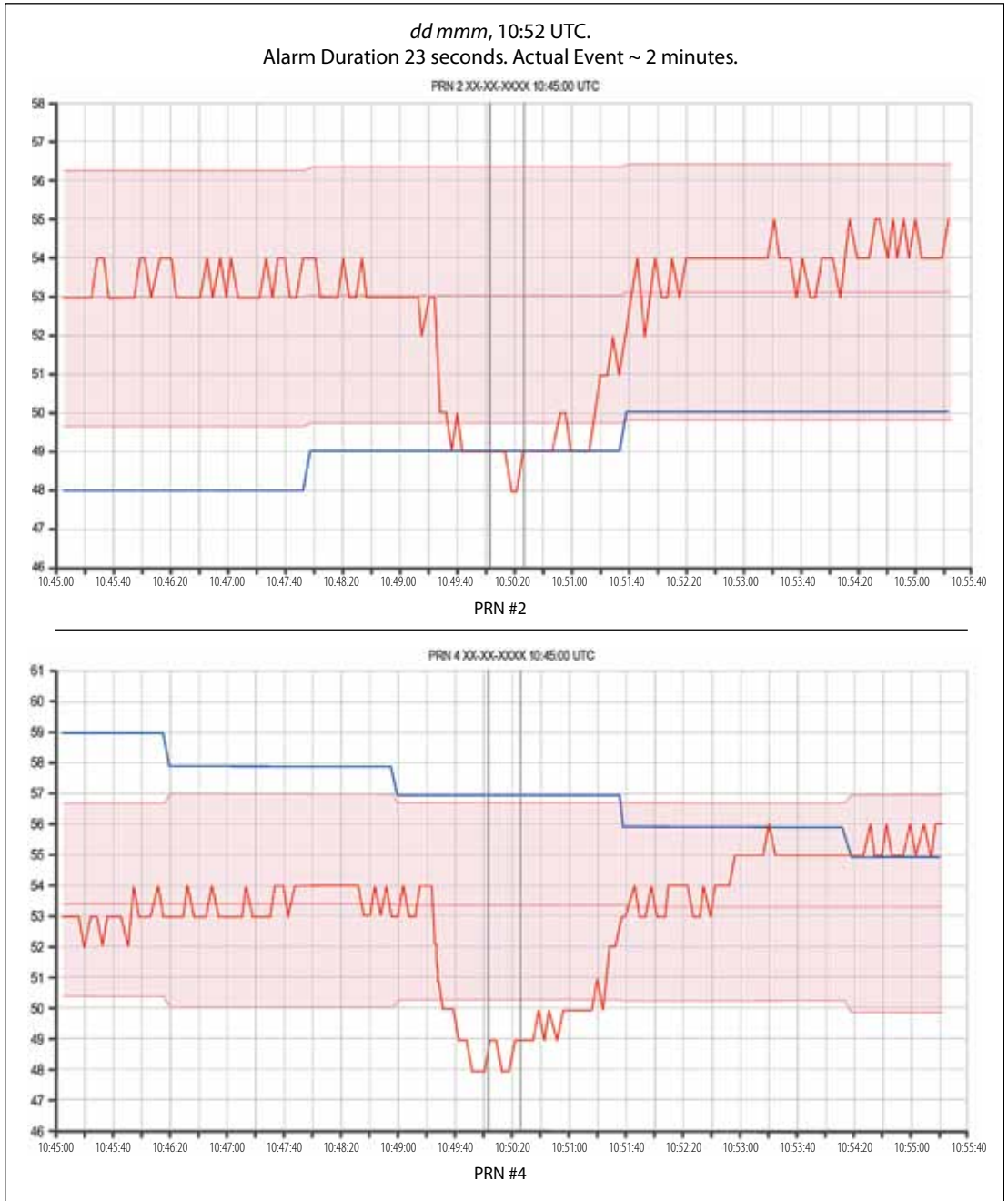


FIGURE 4 Event Type 1

"Deep Short Sharp" Signature
Signatures correlate with Loss of Lock on the OS Net Receiver co-located with the GUARDIAN probe

DSST Signature seen on Satellites PRN #2, 4, 10, 13, 20, 23.
nn mmm, 14:17 UTC. Alarm Duration 18 seconds.

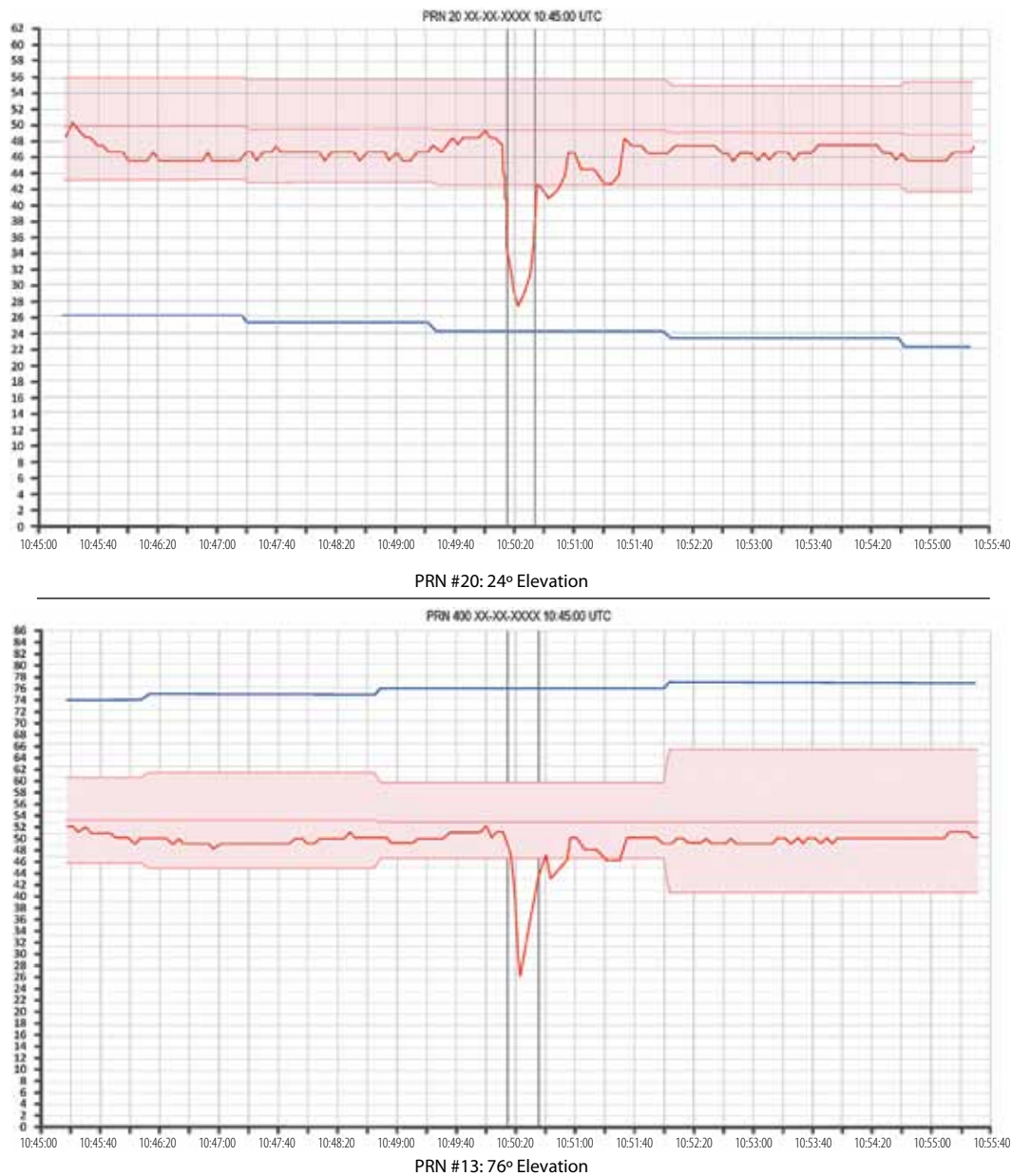


FIGURE 5 Event type 2

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)

described in the Royal Academy of Engineering report on GNSS vulnerabilities.

As a result of this event analysis, therefore, the initial assessment that the problem was manmade was proven correct. Any further action by the appropriate UK authorities is to be determined by the UK LEAs, and the GAARDIAN team will not be involved.

Conclusion

This overview and case study has shown

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 were used to aid in localizing 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.)

This article cannot provide specific details of the LEA operation nor describe how the GAARDIAN team further contributed, for reasons of operational security and possible legal proceedings. 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

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.

GAARDIAN thus fulfills the role called for by the original design concept. Further work would be needed to integrate the server and probe functionality within a customer's 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.

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

The technology mentioned in this article is also being improved upon for the SENTINEL program, which incorporates additional capabilities for determining the location of an interference source and providing a measure of trust in a PNT system.

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 deci-

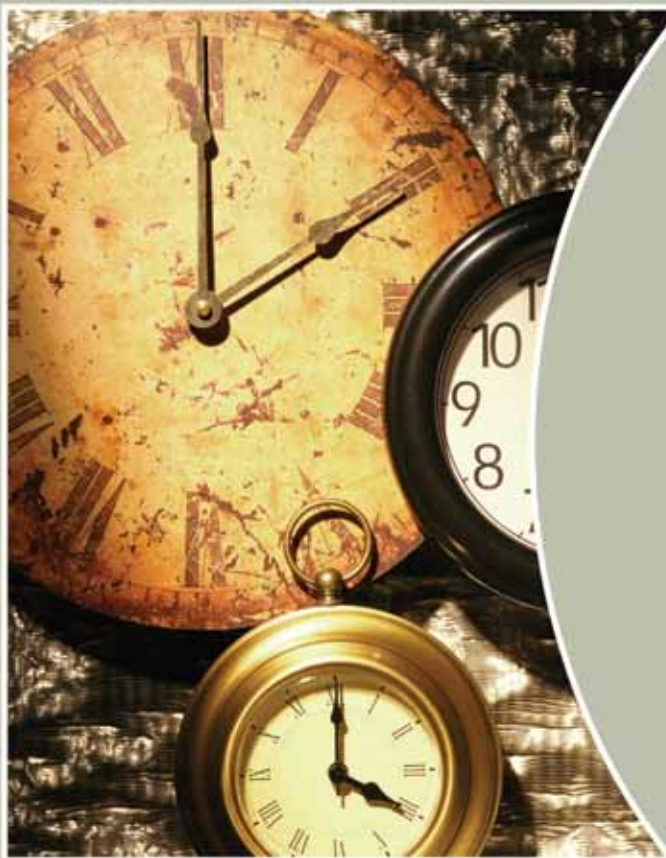


CTL3500
handheld
interference
detector

sion making on the ground, which not only proved successful but also avoided the need for potentially protracted and costly law enforcement investigation.

Manufacturers

The handheld interference detector used in the GAARDIAN program was the CTL3500 interference monitor from **Chronos Technology Ltd.**, Lydbrook, Gloucestershire, United Kingdom. The GPS receiver system used within the GAARDIAN probe is a CTL430 also from **Chronos Technology Ltd.**, and the eLoran receiver used in both the GAARDIAN and SENTINEL projects is a UN-150 eLoran Timing Receiver from **URSNAV Inc.**, Chesapeake, Virginia USA.



PTTI 2011
www.pttimeeting.org

14-17 November 2011
Hyatt Regency Hotel
Long Beach, California

Have you reserved your booth space for PTTI 2011?
Booth space may be limited.

Credit cards are accepted

Registration: nicolette.jardine@nrl.navy.mil
Exhibits: don@gmasales.com

Authors



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 almost 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.



Andy Proctor 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

during 10 years there, including global customer support, technical (including training), and sales roles. 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 organization, in a business development position. His role at Chronos is to manage the development and growth of the GNSS product and service portfolio within Chronos, including the commercial side of the GAARDIAN and SENTINEL programs. He holds a master's degree in strategic sales & management, is a member of the Royal Institute of Navigation, and a Fellow of the Institute of Sales and Marketing Management.




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 Col-

lege, 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 propa-

gation 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. 

GPS / GNSS SIMULATORS



GPS Constellation in a Box

Multi-Channel GPS Test Devices for Manufacturing and Development

ГЛОНАСС
GLONASS COMPATIBLE

Applications	Functionality
<ul style="list-style-type: none">Fully controllable GPS simulationSimulate positions, times and user movementsStandards-based GPS testsSBAS simulationRun predetermined test scenarios	<ul style="list-style-type: none">Repeatable and reliableEasy to useFast/high throughputPortable and compactWhite noise generationGLONASS Simulation

 **SPECTRACOM**
orolla Group

North America: +1.585.321.5800
www.spectracomcorp.com

sales@spectracomcorp.com
France: +33 (0) 1 6453 3980
UK: +44 (0) 1 256 303630