Standardisation of GNSS Threat reporting and Receiver testing through International Knowledge Exchange, Experimentation and Exploitation [STRIKE3]

M Pattinson, M Dumville, Y Ying
Nottingham Scientific Ltd
Nottingham, UK

M Zahidul H Bhuiyan, H Kuusniemi
Finnish Geospatial Research Institute
National Land Survey of Finland
Helsinki, Finland

B Gabrielsson, Å Waern
Swedish Defence Research Agency (FOI)
Stockholm, Sweden

M Poloskey
Automotive & Rail Innovation Center (ARIC) of AGIT mbH4
Aachen, Germany

S Hill
Satellite Applications Catapult Limited
Harwell, UK

N Shivaramaiah, S Kibe
GNSS Labs
Bengaluru, India

S Lee
ETRI
Daejeon, Republic of Korea

J Reyes Gonzalez
European GNSS Agency (GSA)
Prague, Czech Republic

STRIKE3 is a new European initiative to support the increasing use of GNSS within safety, security, governmental and regulated applications. The aim of STRIKE3 is to develop international standards in the area of GNSS threat reporting and GNSS receiver testing. This will be achieved through the deployment and operation of an international GNSS interference monitoring network to capture the scale and dynamics of the problem, and through work with international GNSS partners to develop, negotiate, promote and implement standards for threat reporting and receiver testing. The paper shall present the latest information on the STRIKE3 project and shall conclude with initial findings emerging from the international STRIKE3 network of threat monitoring stations.

Keywords—Interference; jamming; threats; resilience

I. INTRODUCTION

Dependence on GNSS is increasing as GNSS is used for an ever expanding range of safety, security, business and policy critical applications. GNSS functionality is being embedded into many parts of critical infrastructures and European economies are now dependent on uninterrupted access to GNSS positioning, navigation and timing services. At the same time, GNSS vulnerabilities are being exposed and threats to denial of GNSS services are increasing. Reports of events of loss of GNSS services are commonplace. To ensure GNSS is protected, there is now a need to respond at an international level to ensure that there is (i) a common standard for GNSS threat monitoring and reporting, and (ii) a global standard for assessing the performance of GNSS receivers and applications under threat. This will ensure the dominance of GNSS as the backbone to our positioning, navigation and timing needs.

The STRIKE3 project is being supported by the European GNSS Agency (GSA) within the Horizon 2020 research programme to address the need to monitor, detect, characterise and mitigate threats to GNSS services and applications. The project can be likened to the earliest developments in anti-virus software. Given societal dependence on GNSS, there is a growing need to persistently monitor the threat scene, to develop the "anti-virus" and to ensure GNSS as a robust and hardened system against any kind of attacks, be it intentional or unintentional.

STRIKE3 will develop international standards in the area of GNSS threat reporting and GNSS receiver testing. This will be achieved through international partnerships. GNSS threat reporting standards are required to ensure that

international GNSS threat databases can be developed. GNSS receiver test standards are required to ensure new applications can be validated against the latest threats. Both standards are missing across all civil application domains and are considered a barrier to the wider adoption and success of GNSS in the higher value markets.

STRIKE3 will persistently monitor the international GNSS threat scene to capture the scale and dynamics of the problem and shall work with international GNSS partners to develop, negotiate, promote and implement standards for threat reporting and receiver testing. This is being achieved through the deployment and operation of an international GNSS interference monitoring network.

This paper presents the latest information on the STRIKE3 project.

II. Understanding the Threat

GPS signals are very weak and are therefore susceptible to interference. The presence of interference can cause difficulties in acquiring or tracking signals, and in the worst case complete loss of service.

There are many potential sources of interference and these may be unintentional or intentional. Unintentional interference is that which is not intended to interfere with GNSS signals but nevertheless causes problems with signal acquisition and/or tracking. This may include man-made interference (such as mis-tuned or faulty equipment) as well as natural phenomena (e.g. Space Weather). Intentional interference is that which is designed specifically to interfere with GNSS signals and includes effects such as Jamming, Spoofing and Meaconing, although it is noted that intentional interference against a specific target can have unintended consequences for other GNSS users nearby.

Depending on the nature of the interference and the strength of the interfering signal, a user may be affected in several ways. At the receiver level there may be increased position errors due to the presence of range errors and biases, or due to degraded geometry caused by loss of tracking of some satellites. At a service level, depending on the nature of the application and the fall-back position in case of degraded GNSS position, the impact may range from a small nuisance to an economic or a safety impact.

To mitigate the threat and the impact there are a number of potential countermeasures. These include:

- Legislation against jammers to restrict their supply, possession and use
- Education activities to raise awareness about legislation and to point out that 'personal' jammers can have unintended consequences
- Enforcement, including
    - Detection and removal of jammers / interference sources
    - Direct or indirect detection (e.g. use of dedicated interference detection equipment as well as things like 'crowd sourcing' reports of GNSS interruptions)
- Equipment solutions to mitigate against interference or its effects:
    - Antenna technology to reduce interference
    - Receiver technology to mitigate against interference
    - Hybridisation (with other sensors and technologies) to ensure continuity of service
- Development of procedures and processes to enable operations or define a fall-back mode in case of loss of GNSS

However, the success of many of these countermeasures is dependent on having a detailed understanding of the threats. In order to establish this understanding, and to maintain an up to date knowledge of the threats - both in terms of types of threat and number of threats – it is necessary to monitor the threat environment and the impact on performance.

Monitoring and reporting is one part of the approach and is required to inform stakeholders of the threats that exist in the real-world. This helps directly with enforcement (detecting and removing sources of interference) as well as monitoring the response to changes in legislation or education activities. In addition, specific information about the types of threat can be used in receiver testing. This can help to check the protection offered by antenna or receiver technologies, and to help with the development of improved mitigation techniques.

III. Previous Initiatives

The GSA and ESA (and member states) have recognised the threat from jammer technology on the continuity and availability of GNSS services. As a direct result, several initiatives have been launched within EU to develop GNSS jammer detection, isolation and mitigation capabilities and technologies. Most notable among these initiatives are the GSA DETECTOR project, the GSA PROTECTOR study and the ESA Interference Monitoring System (IMS) study.

A. GSA DETECTOR project

The DETECTOR project [1] has developed a low-cost GNSS radio frequency interference detection service for use within road transport and critical applications. Roadside probes connected to a back-office detect and characterise interference using techniques which are made possible using software receivers. The ability to analyse interference at the digital sample level allows more reliable detection and characterisation of the interfering signal, helping to differentiate unintentional interference sources from deliberate jamming.

DETECTOR software and hardware has been tested in a laboratory and in field trials using dedicated sensors, and also

using data available from existing GNSS reference networks. In all cases the DETECTOR solution was able to reliably detect and characterize a range of typical jammers and to assess their potential impact on GNSS services.

DETECTOR is now a commercial product providing a continuous monitoring capability at target locations [2].

B. GSA PROTECTOR Study

In 2009, the GSA launched an Invitation To Tender (ITT) for the PROTECTOR study. PROTECTOR (Protection, Evaluation and Characterisation of Threats Originating from Radio-sources) examines what is needed to protect European GNSS systems and services against radio-sources interferences in L-band, S-band and Ku-band to prevent service disruptions. The PROTECTOR study examined the risks and proposed a Jamming and Interference Monitoring System (JIMS) concept and explores how JIMS can interface with Member States and with the European GNSS Security Centre [3].

The STRIKE3 project is a complement to the GSA work by addressing a missing element in the protection against GNSS interference sources and malicious use of localised GNSS jamming technology. Whereas current GSA activities (i.e. PROTECTOR study) addresses the protection of GNSS infrastructure and services, the STRIKE3 project shall address the need to provide protection for GNSS denial at the application level, with a particular focus on transport and critical national infrastructure applications.

The PROTECTOR study has defined and specified an operational service to ensure the protection and continuity of European GNSS infrastructures and services. This principally includes the monitoring and protection of EGNOS and Galileo sites. The PROTECTOR vision also includes the potential use of advanced receiver technologies, with a focus on PRS receiver capabilities. In contrast, the STRIKE3 project shall only utilise civil technology to deliver the detection capability.

Finally, the PROTECTOR study has examined the existence and integration of Member States' assets and capabilities to better understand the European dimension and the gaps that exist and need to be addressed by PROTECTOR. At a national level, most states have detection equipment, which may include localization utilities, to identify the presence of RF interference sources within spectrum policing operations. STRIKE3 will demonstrate the integration of national monitoring capabilities into the larger STRIKE3 system through the adoption of international standards for threat monitoring and reporting.

C. ESA Interference Monitoring System

The European Space Agency (ESA) has recently awarded a project under the European GNSS Evolutions Programme for the development of a demonstrator Interference Monitoring System (IMS) [4]. The objective of the study is to develop and demonstrate an Interference Monitoring System (IMS) for use at sensor stations. The proposed Interference Monitoring System (IMS) will provide near real-time information on interference at Sensor Stations. Such stations include Galileo Sensor Stations and EGNOS RIMS stations. The IMS will consist of a Processing Facility (PF) and several Local Elements (LEs). The PF will comprise a Work-station, receiving data from several LEs, providing access to information and data. The LE is a device capable of monitoring the relevant spectrum and providing results in digital format.

D. InCarITS

The InCarITS project [5] is being carried out by the University of the Federal Armed Forces in Munich under funding sponsorship by DLR. The project aims to address the challenges facing the wider use of GNSS within ITS and in particular road tolling. There is a specific focus on GNSS interference detection and mitigation solutions which is relevant to STRIKE3. The work involves GNSS, VANET (vehicle ad-hoc networks) floating car data and local dynamic maps. The project has carried out a lot of analysis of different types of jammer and is proposing that a jammer detection system and message should be included within the safety related vehicular communication protocol and standards. The InCarITS project is focussing in the specific domain of ITS and developing solutions for ITS market, whereas STRIKE3 is looking across all domains, all threats and all markets with the sole aim to learn more about the threat in order to discover what we can do to reduce the likelihood or reduce the severity of impact of such threats.

E. Other projects and Initiatives

In the US, the GPS Jammer Detection and Location System (JLOC) has been developed to provide GPS jammer alerts and products for U.S. warfighters [6]. This is now expanding into Homeland Security and Civilian applications.

Recognising the dependence of GPS within the US, Overlook Systems have taken the step of developing a suite of commercial products "Patriot Watch, Patriot Shield and Patriot Sword" to address the detection, localisation and mitigation of GPS interferers [7]. While the main focus is to protect GPS time for telecommunications and energy networks, the concept is scalable for other application domains and demonstrates that there is commercial potential in the underlying STRIKE3 concept.

In November 2010, the US PNT (Position, Navigation Time) advisory group published a report into the vulnerabilities of GNSS, the consequences of loss of GNSS and the measures that should be taken (technical, legal, institutional) to ensure that society is protected from natural and malicious interference [8]. Within the document, specific reference is made to a detection capability, as well as location, countermeasures and back-up systems. This report provides further evidence of the scale of the threat and the severity of denial of GNSS services to the economy. It therefore strengthens the argument for STRIKE3 capabilities.

In the UK, the GAARDIAN [9] and Sentinel [10] project is seeking to use the UTC-traceable timing signal from the UK eLoran station along with analysis of GPS signal data to authenticate GPS timing wherever it is needed for mission and safety critical applications. As part of the timing

authentication, basic GNSS integrity and interference checks are carried out. Sentinel is now focussing on enforcement through integration with ANPR cameras to help the authorities identify perpetrators. The Sentinel solution is also being used within the Excelis Sentry 1000 system as part of a jammer geo-localisation system [11].

Finally, the MAGIC project (Management of Galileo Interference and Counter Measures) was commissioned by the Galileo Joint Undertaking as a proof of concept of detection, mitigation, and location of potential unintentional or intentional interferer(s) of the Galileo signals [12]. A demonstrator was developed and demonstrated during the project in order to verify, different concepts and approaches.

Other recent developments that will impact on the work within STRIKE3 include:

- MITRE in the US has developed an ANDROID APP that delivers crowd sourcing information on GNSS interference and jammers. This does not provide the level of information proposed within STRIKE3 to enable the GNSS community to harden their products. Nevertheless it does identify "hot spots" of activity.
- Universities and research institutes have published numerous papers on GNSS spoofers – providing basic instructions (and components) that could support development of such technology.
- US, Russia and China have indicated their interest in GNSS interference monitoring standards at the UN ICG [13, 14].

All of these projects, developments and initiatives provide valuable inputs, insights and directions for the STRIKE3 project.

IV. STRIKE3 Approach

The rationale for STRIKE3 arises from several key observations from previous monitoring activities. Firstly, is the observation that the threat environment is not static and shows quite significant variation – even at a single site. The results below show the number of detected chirp signatures (typical of small hand-held or in-car jammers) that were observed at a single site over a 2-year period. The total monthly figures are shown.

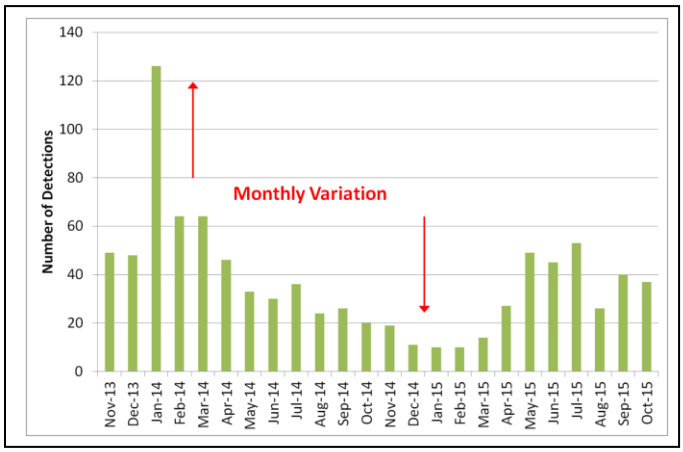

Fig. 1. Monthly Number of Detected Chirp Signatures at a Single Site for 2-Year Period

It can be seen that there is a significant variation within this period, from a minimum of just 10 chirp signatures to over 120 detections is one month. Having such a high variation shows that for anyone wishing to understand the threat environment at a location, long-term monitoring is essential.

Secondly is the observation that the threat environment is location specific, and even similar types of site located in the same region are affected by greatly different numbers of interference events. The figure below shows monthly results for the same month (October 2015) at two different sites. Both sites were located close to major roads in a similar region of the country with the same type of detection equipment, but it can be seen that the number of events at each site is very different. For site A, there are 1436 detected events in total, of which 37 are chirp signatures, whereas at site B there are 250 detected events of which 11 are chirp signatures. This illustrates that in order to get a view of the general threat environment, information from multiple sites must be collected.

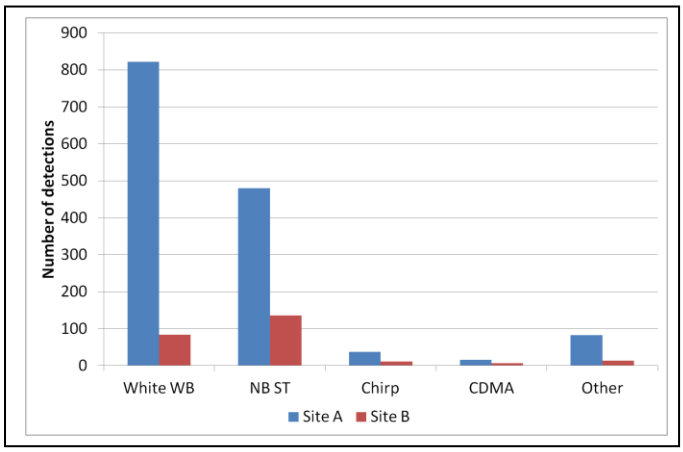

Fig. 2. Number of Detected Events of Each Type at Two Sites for one Month

Thirdly is the fact that the longer a site is monitored, and the more sites you monitor, the greater variety of events will be detected. Monitoring for a week at a single site may identify 20 different types of signature, but through monitoring for a longer period additional types of interference signature will be found, and monitoring at a different site will provide yet another set of events and interference signatures. Having such a database of interference signatures, and continually updating such a database with new information, will prove a valuable resource for testing the resilience of existing receiver technology and algorithms to real-world threats, and to help with the development of enhanced mitigation techniques.

The aim of STRIKE3 therefore is to develop a standard monitoring and testing approach in order to maximize the potential benefit. The scope of STRIKE3 covers the definition, development and demonstration of a low-cost GNSS interference and jammer detection device to support infrastructure operators, service providers and the authorities in their fight against the use of GNSS jamming technology in serious and organised crime as well as mainstream crime. The proposed solution is a composite of multiple innovations as follows:

- Innovation 1 GNSS threat monitoring and reporting standard

  There are two principal innovations within the project that aim to secure global appeal. The first innovation is the development of a GNSS threat monitoring and reporting standard. This will help the GNSS community to receive consistent reports of events that impact on GNSS services. A standardised approach is necessary to combine messages from multiple systems and to help statistics and analyses that can feed into risk assessments.

- Innovation 2 GNSS threat testing standard

  The second innovation relates to the production of test standards. In March 2015, the GSA published the 4th GNSS Market Report [15]. None of the GNSS receiver manufacturers within the report currently market a product that is capable to operate in the presence of a threat. The availability of threats and test standards is critical to developing the next generation of receiver technologies to support the wider use of GNSS in safety and liability critical high-value applications.

- Innovation 3 International GNSS threat monitoring network

  STRIKE3 will deliver an international threat monitoring network. This will enable partners, EC and GSA to see the trend of GNSS threats across all continents from a dedicated monitoring network. This will provide valuable information for the STRIKE3 project team and the EC and GSA to support discussions with international partners and GNSS service providers. New threats will be detected and compared to the emergence of similar threats at other locations across the globe. A picture of the dynamics of the threat scene will emerge.

- Innovation 4 Centralised GNSS threat database

  All events detected at the STRIKE3 network sites will be transmitted to and stored within the STRIKE3 central database. All events will adhere to the STRIKE3 standard. All events will be available for analysis (trending, pattern detections etc.).

- Innovation 5 "Systems of Systems"

  STRIKE3 will enable a group of existing detection systems to become a networked "system of systems" through the application of a common standard. The standard will be offered to the wider community to support the persistent monitoring of GNSS threats at key sites with the common and shared objective of improving GNSS through better knowledge of the threat to GNSS.

- Innovation 6 Advanced technologies

  STRIKE3 will deliver a database of threats which will stimulate the development of countermeasures and mitigation technologies to reduce the impact of the threat. This represents the overall longer term ambition from the STRIKE3 project. The overarching aim must be to ensure that next generation GNSS receivers and technologies are robust to the threats and ensure that GNSS applications are protected from denial of service attacks and related threats.

The links, associations and dependencies of the innovations from the STRIKE3 project are illustrated graphically below.

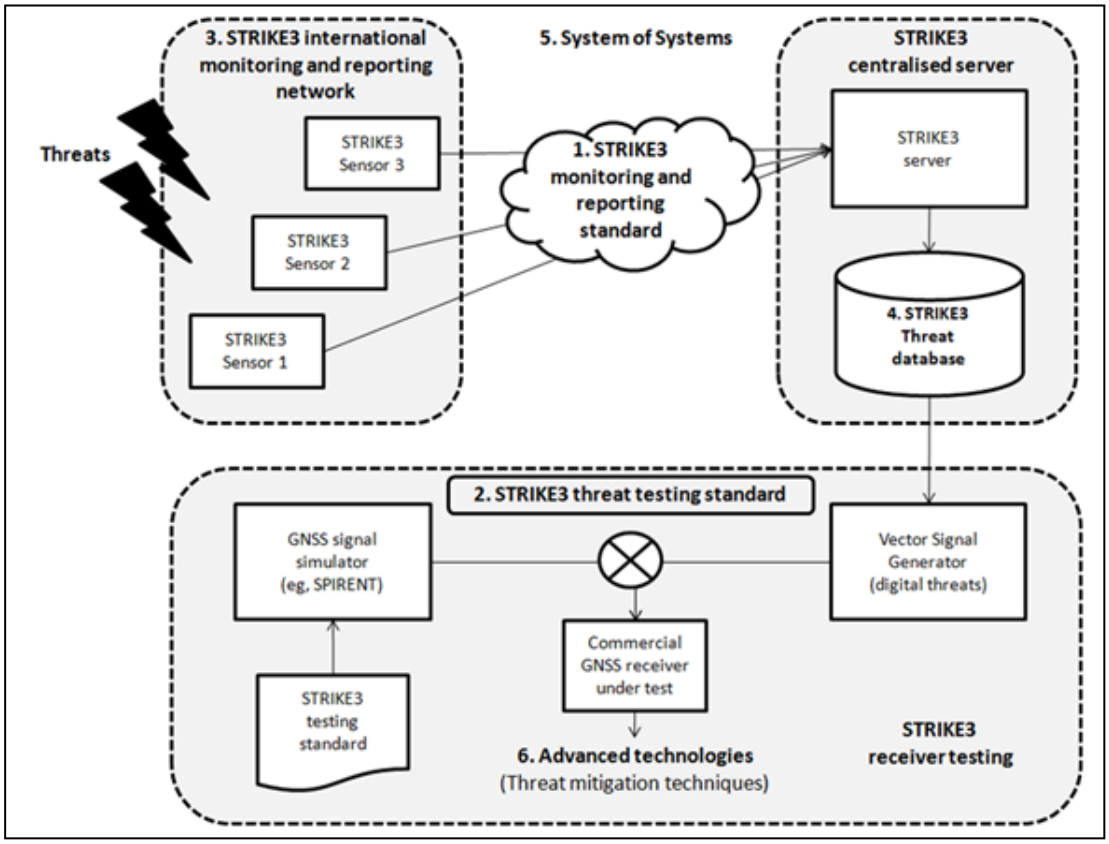

Fig. 3. Overview of STRIKE3 Innovations

The STRIKE3 project kicked-off in February 2016 and is currently in the initial stages of state-of-the-art review and international threat collection. The deployment of the monitoring network started in March and currently consists of 9 different monitoring sensors installed in 5 different countries in Europe. The further deployment of additional sensors in Europe and around the world is ongoing. It is planned to develop a set of draft reporting and testing standards for early 2017, followed by validation of the standards in long term monitoring trials and receiver testing activities.

V. Conclusions

With the increasing dependence on GNSS it is important that GNSS vulnerabilities, such as interference are properly addressed. The STRIKE3 project is addressing this need through the development of monitoring and reporting standards, the deployment of a worldwide monitoring network to test the reporting standards and to provide a database of real-world events, the development of receiver testing standards against threats, and the testing of receivers against the real-world threats detected by the monitoring network in order to test resilience and propose improved mitigation measures.

Acknowledgment

The work presented in this paper has been co-funded under the H2020 programme through the European GNSS Agency (GSA).

References

[1] K. Sheridan, Y. Ying and T. Whitworth, “Pre- and Post-Correlation GNSS Interference Detection within Software Defined Radio”, Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012), Nashville, TN, September 2012, pp. 3542-3548

[2] “GSS100D Detector, GPS/GNSS Interference Detector”, http://www.spirent.com/Products/GSS100D-Detector

[3] N. Davies, C. Schäfer, B. Vauvy and M. Schoenhuber, “PROTECTOR, Protecting European GNSS Services”, GNSS Interference, Detection & Mitigation Conference, National Physical Laboratory, Teddington, London, 10 March 2011

[4] Wendel, J., Kurzhals, C., Houdek, M., Samson, J., "An Interference Monitoring System for GNSS Reference Stations," Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2013), Nashville, TN, September 2013, pp. 3391-3398

[5] D. Fontanella, R. Bauernfiend and B Eissfeller, “In-Car GNSS Jammer Localization Using Vehicular Ad-Hoc Networks”, Inside GNSS, Working Papers, May/June 2013

[6] A. Brown, D. Reynolds, D. Roberts and S. Serie, “Jammer and Interference Location System – Design and Initial Test Results”, Proceedings of the 12th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 1999), Nashville, TN, September 1999, pp. 137-142

[7] "Patriot Watch, Patriot Shield, Patriot Sword: A Proposed Solution to Address Risk to US Critical Infrastructure", http://overlooksys.com/assets/files/Patriot%20WatchShieldSword.pdf

[8] "National PNT Advisory Board comments on Jamming the Global Positioning System - A National Security Threat: Recent Events and Potential Cures", November 4 2010

[9] C. Curry, "GAARDIAN Project Results & Introduction to The Sentinel Project", GNSS Interference, Detection & Mitigation Conference, National Physical Laboratory, Teddington, London, 10 March 2011

[10] C. Curry, "Sentinel Project, Report on GNSS Vulnerabilities", Project Report 001, 04 April 2014

[11] "Signal Sentry 1000", http://www.exelisinc.com/solutions/signalsentry/Pages/default.aspx

[12] A. Ferreol, P. Morgand and E. Rossini, "Detection, Mitigation and Isolation of Galileo Interferers", ENC-GNSS 2008 Conference, Toulouse, France April 22-25, 2008

[13] S. Kizima, "International Interference Detection & Mitigation System for GNSS", ICG Working Group A, 8th Meeting of the International Committee of GNSS, Dubai, UAE, November 2013

[14] W. Zhen and X Zhao, "Suggestions on Standardized Reporting Form of GNSS Interference", ICG Working Group A, 8th Meeting of the International Committee of GNSS, Dubai, UAE, November 2013

[15] European GNSS Agency, "GNSS Market Report", Issue 4, March 2015