CYBER SECURITY THREATS TO SAFETY-CRITICAL, SPACE-BASED INFRASTRUCTURES

C.W. Johnson [(1)], A. Atencia Yepez [(2)],

[(1)] Department of Computing Science, University of Glasgow, Scotland.
http://www.dcs.gla.ac.uk/~johnson, Email: Johnson@dcs.gla.ac.uk
+44 (0)141 330 6053 (Tel.), +44 41 330 4913 (Fax).

[(2)] GNSS Business Unit, GMV, C/ Isaac Newton 11, PTM, 28760, Tres Cantos, Spain.
Email: aatencia@gmv.com

ABSTRACT

Space-based systems play an important role within national critical infrastructures. They are being integrated into advanced air-traffic management applications, rail signalling systems, energy distribution software etc. Unfortunately, the end users of communications, location sensing and timing applications often fail to understand that these infrastructures are vulnerable to a wide range of security threats. The following pages focus on concerns associated with potential cyber-attacks. These are important because future attacks may invalidate many of the safety assumptions that support the provision of critical space-based services. These safety assumptions are based on standard forms of hazard analysis that ignore cyber-security considerations This is a significant limitation when, for instance, security attacks can simultaneously exploit multiple vulnerabilities in a manner that would never occur without a deliberate enemy seeking to damage space based systems and ground infrastructures. We address this concern through the development of a combined safety and security risk assessment methodology. The aim is to identify attack scenarios that justify the allocation of additional design resources so that safety barriers can be strengthened to increase our resilience against security threats.

1. INTRODUCTION

Space-based systems play an important role in national critical infrastructures. The certification of Global Navigation Satellite Systems (GNSS) Safety of Life services extends the integration of GPS and GLONASS data into applications ranging from railway signalling through to the allocation of fire and rescue services. Considerable care has been taken to ensure that these systems meet stringent safety constraints in terms of their:

- accuracy- how correct is the position estimate;
- integrity- the largest position error without detection;
- availability- how often can an application use the infrastructure,
- continuity - the probability that an operation once commenced can be completed and time to alert should an error occur.

At the same time, a range of organisations across Europe and North America are concerned about the vulnerability of new space-based, critical infrastructures (RAE, 2011). Security attacks may invalidate many of the safety assumptions that are based on the analysis of system failures rather than security concerns (Johnson and Atencia Yepez, 2010). However, the inclusion of a combined safety-security risk based methodology for the identification of attack scenarios would improve the efficiency and completeness of the design since:

- It would cover a wider range of hazard considering not only system failures but also directed security attacks.
- It would avoid duplicated/overlapping barriers that might otherwise waste resources if security and safety analyses were to be performed independently.

A number of threats can be identified for Global Navigation Satellite Systems (GNSS) infrastructures. These include denial of service attacks on elements of the ground based infrastructures. Other concerns focus on data integrity and vulnerabilities to insider attacks. A security assessment must also consider a number of spoofing mechanisms. These concerns can be illustrated by a GNSS ground subsystem that receives input data from a number of data acquisition stations. It then processes the data to generate GNSS output, such as navigation or integrity messages. From a safety perspective, the ground subsystem design must be robust to possible hazards, including data loss or corruption from one or more stations. These hazardous events could arise from failures of the stations or from deliberate and coordinated attacks. The impact on safety is the same in both cases. However, further complexity arises when security and safety concerns overlap. This could occur if an attacker deliberately chose to exploit

vulnerabilities created by a random system failure. Alternatively, designers must consider the possibility that a deliberate attack might coincide with wider problems in the GNSS infrastructures. An integrated security analysis could, therefore, identify compound hazards not included in the safety analysis and vice versa.

This paper argues that existing safety requirements cannot be sustained in the face of deliberate external or internal attacks. In particular, we use evidence from attacks on ground-based infrastructures to anticipate future cyber-security threats to GNSS infrastructures. We also identify ways of integrating security and safety arguments to increase the resilience of space-based systems. The aim is to support safety arguments to demonstrate that an infrastructure is acceptably safe ***and*** secure to provide critical services.

2. SECURITY THREATS TO GNSS

Most of the design concerns that motivated the development of GNSS infrastructures have focused on safety rather than security requirements. The existing infrastructures remain vulnerable to a range of attacks. An early warning was provided by an approach into New Jersey during December 1997. The crew of a Continental trans-Atlantic flight lost all GPS signals; jeopardizing confidence in on-board systems. It was initially believed that this had been caused by an intentional jamming attack. It later turned out to have been the unintended result of a US military test. A 200-kilometer "interference zone" was created by a GPS antenna with a 5-watt signal, stepping through frequencies.

The UK Ministry of Defence (MOD) illustrated the potential threat for maritime navigation (Grant, Williams, Ward and Basker, 2009). A medium powered jamming device generated noise over a pre-defined area of the UK coastline. This study clearly illustrated the impact that the threats to GNSS integrity can have upon the end users of these infrastructures. Particular problems were identified for crews using integrated bridge systems. This technology brings together navigation tools with autopilot control so that a jammed GPS signal could lead to a significant deviation without warning. Even if an alert was issued, it can still be difficult to determine the vessel's correct position given a consequent loss of situation awareness. The crews in this trial were all aware that the GPS signals would be jammed. However, multiple simultaneous alarms rapidly increased their workload as the crew cross-checked navigational information. The consequences for on-board systems were compounded by the impact of jamming for shore-based systems. Numerous errors began to undermine the Vessel Traffic Services that provide an overview of coastal areas. Some of the data returned by vessels was based on incorrect GPS fixes that contradicted radar sources.

Many of the vulnerabilities associated with conventional GNSS architectures stem from the relatively weak signals that are used. A common analogy is to compare GPS output to using the power of a car headlight across one third of the Earth's surface at more than 20,000km. Most western military organizations can interrupt GNSS signals; simulation software enables planners to identify the optimal allocation and distribution of jamming systems. The military development of satellite navigation jamming devices has been mirrored by the increasing availability of hand held systems that cost little more than $100 and have a range of several kilometers. These portable technologies can be used in a range of criminal activities – for instance, to disrupt the signals to GPS tracking devices that would otherwise report the location of a stolen vehicle or shipment. It is illegal to offer these devices for sale within the European Union. This is because they cannot comply with the existing Electro-Magnetic Compatibility (EMC) directives; the prohibition was not primarily intended to protect GNSS services. Within the UK, national legislation prevents the operation of a jammer but it is legal to own such a device (RAE, 2011).

Further threats illustrate the relationship between underlying systems vulnerabilities and the usability of safety-critical applications. First generation GNSS infrastructures provide little support for users trying to authenticate signals. This makes it possible to 'spoof' location information through the broadcast of fake GNSS-like signals or the rebroadcast of valid GNSS signals. Signal simulation software can be used to recreate the anticipated GPS signals for a given route using a particular set of waypoints and timing intervals. Coupled with a spoofing transmitter, these simulators can fool the user into thinking that they are following a specified route. The problems of designing the simulator and then integrating it with effective, mobile jamming technologies have created significant barriers to their application for criminal ends. However, these are likely to be eroded in coming years and the potential threats cannot be discounted. The criminal motivation is proportionate to the diversification of GNSS applications – including route monitoring for road toll and insurance pricing.

Some of these concerns are being addressed through technological innovation. For instance, spoofing will become far more difficult once Galileo begins to provide encrypted signals for use in safety-related applications. Other threats continue to affect future GNSS architectures. The design of the EGNOS and Galileo ground based systems focused on a series of

'feared events' and failure modes. Algorithmic barriers and standard operating practices, including maintenance procedures, were then created to address these concerns. Deliberate attacks were not part of this analysis. In consequence, a number of 'low level' vulnerabilities persist.

Fortunately, the defenses that were created in response to safety concerns also provide protection against potential security threats. The same CRC and error checking techniques that help to identify potential failure modes can also identify a range of attacks. There remains some concern as to whether these defenses would offer sufficient protection against 'insider' threats. For instance, most GNSS infrastructures rely on configuration files that enable operators to respond to the failure of particular components. This increases confidence in meeting the safety requirements, cited above. However it also creates opportunities for malicious reconfiguration.

GNSS infrastructures are typically designed to operate autonomously for short periods of time. Elements of the infrastructure can also be commanded from more than one ground station. This creates a concern that external agents or insiders could spoof legitimate commands or gain temporary control of the infrastructures. This might sound relatively far-fetched. However, the investment in relatively simple attack modes such as those used by STUXNET provides a warning of future vulnerabilities as more and more national infrastructures rely on satellite based navigation and timing information[1]. These potential threats also reinforced the point that security concerns extend beyond the scope of an initial safety analysis into the entire operational life cycle of GNSS architectures through development to deployment and maintenance.

A recent report from the UK Royal Academy of Engineering (2011) argued that 6% of GDP in Western Countries depends on GNSS technology. It went on to criticize the lack of backup technologies. At a national level, agencies should monitor and report on disruption to GNSS signals. At an international level, greater attention should be paid to the vulnerabilities that over-reliance on this technology is creating in the financial markets. Managerial and operational staff should prepare for GNSS outages from ten minutes to a month. The RAE team also argued that GNSS vulnerabilities should be explicitly included in the risk assessments that support critical infrastructures. The limited scope of the RAE report did not, however, identify techniques that might support such analyses. In contrast, the following paragraphs present an integrated methodology for safety and security analysis that might increase the resilience of safety-related SBAS applications.

[1] For more on STUXNET and cyber-attacks see http://www.dcs.gla.ac.uk/~johnson/papers/Gudela

3. DEPENDABILITY AND SAFETY CASES

A range of evidence supports safety arguments for the Safety of Life (SoL) applications of Satellite Based Augmentation Systems (SBAS). This evidence includes test data, simulation results, verification and validation studies, the application of development standards, the results of external audit etc. The diversity of this evidence has motivated the use of safety argumentation techniques to provide an overview of the contribution that each of these approaches makes to an overall safety case. Several different techniques can be used to structure safety argumentation (Bloomfield and Bishop, 2010, EUROCONTROL, 2006).

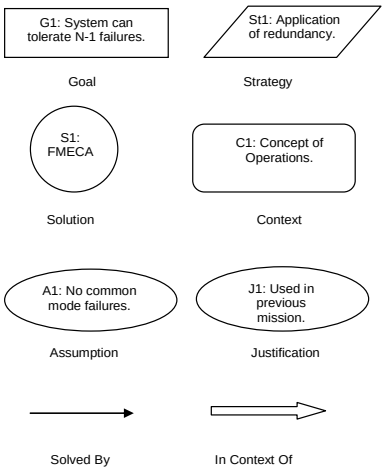

Figure 1 — Components of Safety Argumentation Techniques

Figure 1 illustrates the syntactic components of the Goal Structuring Notation (GSN) (Kelley and Weaver, 2004). A *goal or claim* represents an assertion that can be assessed as either true or false. For instance, Receiver Autonomous Integrity Monitoring (RAIMs) techniques use redundant sensors and signals to determine the users location in addition to the position information derived from a GNSS application. A developer might, therefore, assert that RAIMs techniques are 'acceptably safe during low probability continuity failures'. Although it might not be possible to derive conclusive proof of this goal, a regulator can either accept or reject the assertion.

A GSN *strategy* describes a generic approach to the arguments that are used in support of a goal or claim. For instance, reference to appropriate standards can support many different safety arguments. It might be argued that EGNOS should conform to the requirements established by the European Cooperation for Space

Standardization; Space Engineering–Verification; ECSS-E-10-02A; 17. For the North American WAAS architecture, alternate FAA and NASA standards would apply such as those described in the specification document FAA-E-2892b(C2). A GSN *solution* can be used to present the evidence that supports a goal or strategy. This is important because it provides a link between the high level argument structure embedded within GSN and the more detailed documentation provided by specific development techniques such as Fault Trees, FMECA, Formal methods etc (Johnson and Atencia Yepez, 2011).

A *context* node refers to the environment in which a system is eventually deployed. If the environment changes then this can undermine previous safety arguments; for instance by introducing new hazards that were not considered in earlier stages of development. As we shall see, this can be particularly important when new security threats undermine existing safety cases. *Assumptions* document areas of an argument that are still to be supported by the evidence from particular solutions. They indicate areas for further analysis. *Justifications* help to document the reasons why a particular strategy or solution is appropriate. They can provide regulators or auditors with explanations about the other elements in a safety argument.

Figure 2, below, uses GSN to map out some of the safety arguments relating to the design and operation of the EGNOS Satellite Based Augmentation System (SBAS) (Johnson and Atencia Yepez, 2010). As can be seen, the top level goal asserts that the SBAS is acceptably safe. This can be broken down into sub-goals. In this case, G2 focuses on eliminating or mitigating the hazards that might undermine the ICAO performance requirements in terms of accuracy, integrity, continuity and availability. G3 focuses less on the design issues than on the need to operate the SBAS according to the safety requirements embodied in Standard Operating Procedures (SOPs). These goals are placed within the context of the specification and requirements documents cited in previous sections, including EC Reg 550/2004, EGN SDD SoL etc.

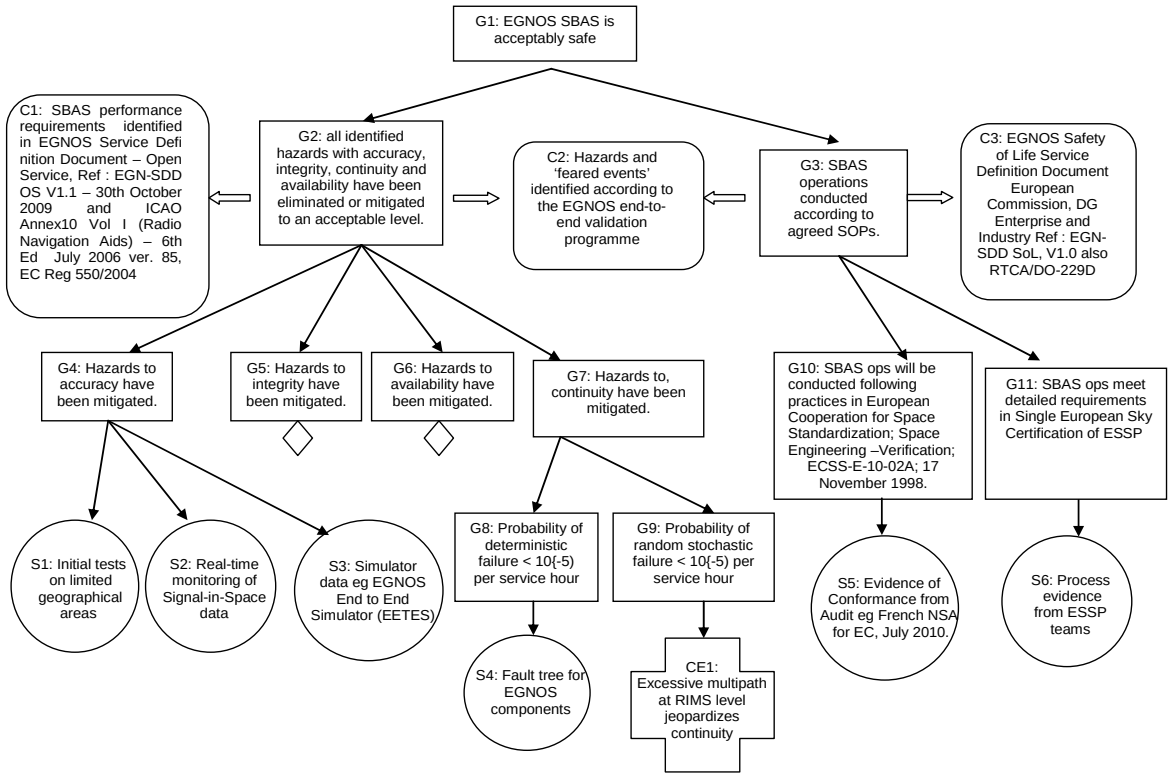

Figure 2 — Initial GSN for Satellite Based Augmentation Systems (SBAS)

The sub-goal G2 in Figure 2 is further decomposed into further sub-sub goals that focus on the mitigation of hazards associated with each of the ICAO performance criteria. Two of these, G4 and G7, are considered in greater detail while a diamond continuation symbol indicates further expansion of G5 and G6. The sub-goal G4 focuses on accuracy concerns. Evidence that these have been addressed can be derived from a range of tests – initially on limited geographical areas and subsequently by more sustained monitoring by ground stations. The EGNOS End to End Simulator (EETES)

can also provide evidence of robustness against accuracy concerns.

Figure 2 provides a partial sketch of the safety arguments that support SBAS operations. There are several sub-goals that might be added – for example in terms of the interactions between design and operations or between the ground teams that help to mitigate any residual risks. The key point is that these diagrams act as a focus for discussion about the higher level safety arguments supporting complex systems. For instance, the use of simulations and real time monitoring of limited trials provides few guarantees that accuracy concerns would be addressed under a wide range of potential operating conditions. Hence, the evidence summarized in S1 to S3 might be extended with additional analytical tools. The key point here is that the argumentation structures help to explicitly document the need to integrate more diverse forms of evidence into the underlying safety cases.

Safety argumentation techniques also provide a framework that helps to focus attention on those areas of a safety case that can be undermined by contradictory evidence. For instance, initial trials of the EGNOS architecture revealed concerns over excessive multipath effects at the Ranging and Integrity Monitoring Stations (RIMS). This jeopardized continuity requirements and became a focus for redesign. Figure 2 illustrates these concerns using the CE1 node. Such extensions show how the GSN notation can be used to develop and refine safety arguments– through both redesign and the collation of additional evidence to increase confidence that the overall goal can be sustained.

The full EGNOS safety case supported the certification for SoL applications across the European aviation industry. It, therefore, goes well beyond the sketch presented in Figure 2, for instance, by considering RAIMS receiver-based fault detection through to the integration with end user applications. The EGNOS safety case also exploits a two-part modular structure that separates design and development from operations (EUROCONTROL, 2006). Part A explains why the system has been 'designed, developed and deployed' in a manner compliant to ICAO Standards and Recommended Practices (SARPS). This was coordinated by the European Commission with support from the European Space Agency as the lead body in the initial design of the EGNOS architecture. In contrast, Part B argues that the SBAS will be operated and maintained to meet the ICAO SARPs by the commercial European Satellite Services Provider (ESSP).

Additional safety cases are then required for each of the applications that are built on top of the SBAS SoL architecture during en-route operations through to non-precision approaches. Figure 2 abstracts away from such details because we do not want to publicize potential safety and security vulnerabilities in the GNSS architectures.

4. SECURITY AND SAFETY CASES

Safety argumentation techniques have been applied to address security concerns. Elberzhager, Klaus and Jawurek (2009) describe security goal indicator trees that offer many of the benefits provided by GSN safety cases. In this approach, argumentation structures are developed to record the evidence that an application is acceptably *secure* – including threat assessments, reports of external auditors, test logs and so on. ISO 15026 has helped to motivate these techniques; it introduces the concept of a security assurance case. This has led to the promotion of dependability arguments as a generalization beyond safety to consider wider reliability requirements. Unfortunately, security assurance cases have not been widely applied by industry. They have not previously informed the reliability engineering of GNSS infrastructures. It is, therefore, important to identify further ways in which we can integrate security AND safety concerns:

- *Integration within a single dependability argument.* Under this approach, the top level goal would be to demonstrate the dependability of a complex system. A first sub-goal would present the arguments that any implement was acceptably safe. A second sub-goal would then structure the evidence showing that the system was acceptably secure. This approach raises a number of concerns – in particular, it is difficult to show that some security evidence has implications for systems safety and vice versa.

- *Integration of safety concerns into security assurance cases.* This approach would begin by constructing the security arguments pioneered by, for instance, Goodenough et al (2008). Additional nodes might then be introduced into the diagram to distinguish evidence or arguments about security concerns that might undermine the safety of any implementation. This approach suffers from a range of practical problems – for example, it is possible to identify potential safety concerns with every threat or vulnerability. However, there are additional safety hazards that would not be represented in the combined diagram because they are not strictly related to the original security assurance case.

- *Integration of security threats into safety cases.* We have chosen to adopt a third approach. This begins by developing a conventional safety case,

such as that illustrated in figure 2. The next stage is to use conventional forms of threat and vulnerability analysis to identify security concerns that were not identified during the previous step. Additional evidence must then be introduced into the hybrid structure to document any additional mitigation that must be introduced to address these security concerns beyond those that were already considered as part of an initial safety assessment. Figure 3 illustrates this approach by integrating security threats into safety arguments for GSN architectures.

We are specifically concerned to identify the impact that security threats might have upon the **safety** of an implementation. Figure 3 presents two safety concerns. The first uses evidence such as the UK MOD studies, cited above, to identify the potential for localized disturbances to a GPS or GLONASS signal that would not be visible to an EGNOS ground station. Of course, the threats posed from such interference can be mitigated through the application of the RAIMs techniques. However, the representation of security and safety arguments within an integrated GSN helps to document the importance of these approaches for the dependability of future applications.

Figure 3 presents further security concerns based around the potential 'insider threat' to GNSS infrastructures. Such threats arise when employees or contractors use specialist knowledge of an architecture to compromise protection mechanisms. This is a particular concern when technical and management staff have not been subjected to a rigorous vetting process. Insider threats are rarely modeled within simulation environments; however, coordinated attacks by individuals who are familiar with the ground architecture of an SBAS system would undermine many of the defenses that are intended to mitigate the impact of individual human errors.

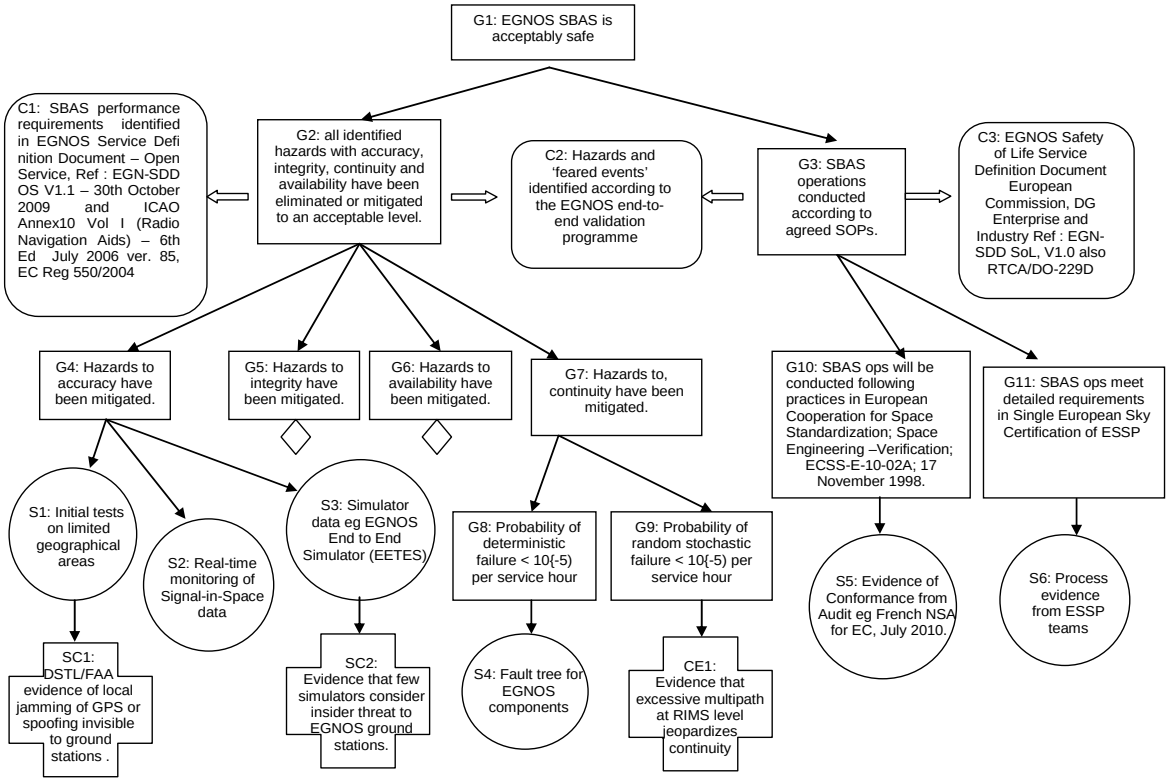

Figure 3 — Integrating Security Threats to GNSS Architectures within GSN Safety Arguments

5. FURTHER WORK

It is important to stress that the approach illustrated in Figure 3 is a first step towards the integration of safety and security concerns within a common approach. There remain many limitations. For instance, the diagrammatic GSN technique is heavily dependent on the skills and expertise of individual analysts. There are few methodological tools that can be used to guide the creation of these hybrid diagrams. This limitation is exacerbated by the lack of examples that might provide a template for the new, integrated approach, advocated here. In previous work we have also extended more formal, mathematically based techniques that have additional methodological support for reasoning

(Johnson, 2011). This used Boolean Logic Driven Markov Processes to combine safety and security arguments to identify the probability of both cyber-attacks and random, stochastic equipment failures – including situations in which these two scenarios coincide. Further work intends to explore the use of both semi-formal GSN and this more rigorous modeling using Markov Processes. We do not necessarily envisage that both will provide equal support for future systems development. However, at present, we lack sufficient experience to tell which will ultimately prove to be the most promising approach.

6. CONCLUSIONS

Space-based systems play an important role within national critical infrastructures. They are integrated into advanced air-traffic management applications, rail signalling systems, energy distribution software etc. Unfortunately, the end users of communications, location sensing and timing applications often fail to understand that these infrastructures are vulnerable to a wide range of threats. This paper has focussed on the safety implications of cyber-attacks.

It is unclear how to represent and reason about the safety concerns that are created by the diverse security threats to GNSS architectures, including jamming, spoofing and the insider threat to ground based systems. Such concerns invalidate many of the assumptions that support the provision of critical services. One approach would be to extend the application of argumentation techniques such as GSN from safety-related applications to represent security argumentation. Several examples have been developed to show how this can be done for a range of software applications. However, this suffers from a number of limitations. In particular, it can be difficult to represent and reason about the impact that security threats might have upon underlying safety arguments. We have, therefore, extended previous approaches to show how security threats might be used to challenge the evidence that supports arguments about GNSS Safety of Life applications. The intention is to provide an integrated, risk-based approach to the identification of attack scenarios that can help assess the resilience of safety cases to security threats.

Acknowledgement

The work described in the paper has been supported by the UK Engineering and Physical Sciences Research Council grant EP/I004289/1.

References

U.I. Bhatti and W.Y. Ochieng, Failure Modes and Models For Integrated GPS/INS Systems. The Journal of Navigation, 60(2):327–348, 2007.

RE Bloomfield, PG Bishop, Safety and Assurance Cases: Past, Present and Possible Future? In F. Redmill and T. Anderson (eds.), Making Systems Safer: Proceedings of 18th Safety Critical Systems Symposium (SSS'10), 51-67, Springer Verlag, London, 2010.

F. Elberzhager, A. Klaus and M. Jawurek, Software Inspections Using Guided Checklists to Ensure Security Goals, International Conference on Availability, Reliability and Security (ARES'09), IEEE Press, 853-858, 2009.

EUROCONTROL, Safety Case Development Manual, Technical report DAP/SSH/091, Brussels, Belgium, 2006.

A. Grant, P. Williams, N. Ward and S. Basker, GPS Jamming and the Impact on Maritime Navigation. The Journal of Navigation, 62(2): 173-187, 2009.

C.W. Johnson, Using Assurance Cases and Boolean Logic Driven Markov Processes to Formalize Cyber Security Concerns for Safety-Critical Interaction with Global Navigation Satellite Systems. In J. Bowen and S. Reeves (eds.), Proceedings of the 4th Formal Methods for Interactive Systems Workshop 2011, Limerick, Ireland, 2011.

C.W. Johnson and A. Atencia Yepez, Safety Cases for Global Navigation Satellite Systems' Safety of Life (SoL) Applications. In H. Lacoste-Francis (ed.), Proceedings of the Fourth International Association for the Advancement of Space Safety, Huntsville Alabama, NASA/ESA, Available from ESA Communications, ESTEC, Noordwijk, The Netherlands, ISBN 978-92-9221-244-5, ESA Technical report SP-680, 2010.

C.W. Johnson and A. Atencia Yepez, Mapping the Impact of Security Threats on Safety-Critical Global Navigation Satellite Systems. In C.G. Muniak (ed.), Proceedings of the 29th International Systems Safety Society, Las Vegas, USA 2011, International Systems Safety Society, Unionville, VA, USA, 2011.

T P Kelly and R A Weaver, The Goal Structuring Notation - A Safety Argument Notation. In Proceedings of the Dependable Systems and Networks 2004 Workshop on Assurance Cases, July 2004.

RAE, Global Navigation Space Systems (GNSS): Reliance and Vulnerabilities, Royal Academy of Engineering, London, UK, 2011. Available as of 19/3/2011 on: http://www.raeng.org.uk/news/publications/list/reports/RAoE_Global_Navigation_Systems_Report.pdf