Mapping the Impact of Security Threats on Safety-Critical Global Navigation Satellite Systems

Chris W. Johnson (1), A. Atencia Yepez (2)

(1) School of Computing Science, University of Glasgow, Glasgow, UK, G12 8RZ.
(2) GNSS Business Unit, GMV, C/ Isaac Newton 11, PTM, 28760, Tres Canto, Spain.

Abstract

Safety cases provide high-level support for the development of critical systems. They present a graphical overview of arguments and evidence to demonstrate that complex applications are acceptably safe within a particular context of use. This paper shows how safety cases support the application of the latest generation of augmented Global Navigation Satellite Systems (GNSS). Unfortunately, at almost the same time as these satellite-based systems have been approved to provide location and timing information in safety-critical applications, a range of organisations including the UK Ministry of Defence, have raised concerns about our increasing vulnerability to attacks on architectures that depend upon GPS, GLONASS etc. These threats are compounded by the difficulty of representing and reasoning about the impact of jamming, spoofing and insider threats within safety argumentation techniques. Such attacks invalidate many of the assumptions that support the provision of critical services. We show how a risk based approach to the identification of attack scenarios can be used to assess the resilience of safety cases to the impact of external security threats.

Introduction

The integration of complex, safety-critical systems in dynamic environments has led to the development of a range of argumentation techniques. These tools help the designers, operators and maintainers of application processes. They provide a structure that can be used to support the many different forms of evidence that helps to demonstrate systems are acceptably safe. The sources of evidence include analytical results derived from the use of Fault Trees, FMECA, HAZOPS etc as well as the results of empirical testing. Figure 1 shows these information sources as the evidence that can be cited by developers and operators in support of a claim that their system is acceptably safe. Evidence is gathered to support the arguments in favour of particular goals or claims. A top level goal is that the system is acceptably safe. However, argumentation techniques also explicitly represent more detailed sub-goals or claims, such as 'software has been developed to an appropriate integrity level' or 'the probability of a high consequence hazard occurring is less than 1 in 10-6' etc (Bloomfield and Bishop, 2010). It is important to stress that the approach sketched in Figure 1 also provides a focus for discussion between the stakeholders who can have very different viewpoints on the validity of particular safety arguments. It is also important to note that some safety case techniques do not rely on graphical overviews but instead exploit text based alternatives (Holloway, 2008).

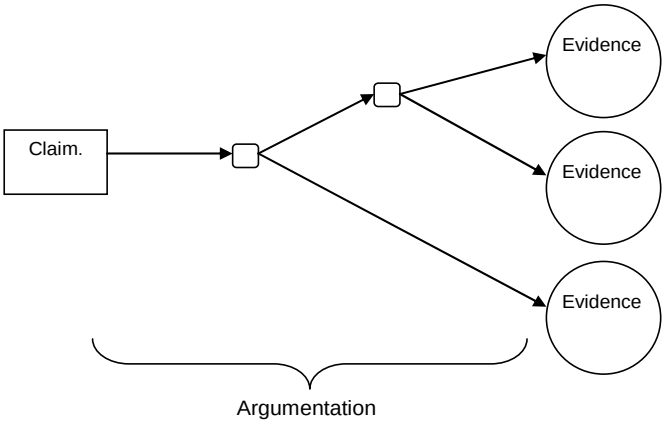

Figure 1: A High-Level View of Safety Arguments

The use of these techniques has been supported across a range of industries; eg UK Military Standard 00-56, EUROCONTROL, 2006. More recently, the US Presidential report into the Deepwater Horizon accident advocated the development of safety argumentation across the oil and gas industry (US Presidential Commission, 2011). The use of safety argumentation techniques does not guarantee that a system will be

acceptably safe (Greenwell et al, 2006). However, the apparent success of this approach across many different industries has encouraged a number of national and international space agencies to consider the use of safety argumentation.

The remainder of this paper proposes a means of extending the use of these argumentation techniques to integrate security concerns into the validation of safety cases. This is a significant issue given that much of the underlying evidence summarised in figure 1 can be undermined by the consequences of deliberate and coordinated attacks rather than random stochastic failures. In particular, we focus on the impact of security concerns for the safety argumentation that supports the present generation of Global Navigation Satellite Systems (GNSS). Our concern is partly justified because there is a growing dependency on timing and location information provided by these systems. This creates significant vulnerabilities for many different infrastructures across Europe and North America (RAE, 2011). Europe has just certified the EGNOS GNSS for Safety of Life (SoL) applications, including approaches to aircraft runways.

Overview of Global Navigation Satellite Systems (GNSS)

First generation GNSS architectures, such as GPS and GLONAS, suffer from a number of known error sources. Some of these problems stem from satellite geometry. If all the satellites are closely grouped together then the benefits of differential signal processing will be reduced. This tends to act as a multiplier for errors induced from other sources. For instance, gravitational forces create subtle changes in the orbit of the satellites within a GNSS constellation. Further problems arise from multipath effects. The signals arriving at a receiver are often reflected from large structures including buildings. This creates inaccuracies of between 2-3 meters because the reflected signal will take longer to arrive than a direct transmission. Further problems stem from ionospheric effects. Radio waves can be considered to travel at the speed of light in outer space. However, the ionizing effects of solar radiation form layers that refract electromagnetic waves from satellite transmissions. Most end users do not correct for unforeseen changes such as variations introduced by strong solar winds (Köhne and Wößner, 2010). These errors help to explain why first generation GNSS architectures have not been widely integrated into safety-related systems (Bhatti and Ochieng, 2007).

Satellite Based Augmentation Systems (SBAS) address these limitations and are intended to support Safety of Life (SoL) applications. These architectures include the North American Wide Area Augmentation System (WAAS) and the Asian Multi-functional Satellite Augmentation System (MSAS) as well as the European Geostationary Navigation Overlay Service (EGNOS). These systems use a number of ground stations to compare known information about the time and their location with the signals received from the satellites to derive error measurements. This information is collated by a smaller number of master stations that then broadcast deviation corrections using a second network of geostationary satellites. End users then apply the corrections to location information derived from the GPS or GLONASS networks. This helps to compensate for atmospheric delays. The net effect is to improve the accuracy of the satellite location information from 17-20 meters to around 2 meters.

A number of additional requirements have to be satisfied before SBAS can be used to support safety-related applications. The International Civil Aviation Organization (ICAO) Required Navigation Performance criteria include **Accuracy**- how correct is the aircraft's position estimate; **Integrity-** the largest aircraft position error can reach without detection; **Availability-** how often can the aircraft use the systems and have the desired Accuracy and Integrity and **Continuity -** the probability that an operation once commenced can be completed.

The EGNOS infrastructure uses redundancy to address many of these concerns in SoL applications. For instance, each of the four master stations rotates from being the Master to a Hot-Back-Up and then to be a Cold-Back-Up. The design of this infrastructure was also guided by the assumption that no single operator error would lead to a loss of integrity. Fault trees as well as Failure Modes, Effects and Critical Analysis were supported by operational observations of test applications to provide evidence that helped to demonstrate conformance with these requirements. In Europe, EGNOS certification was conducted under EC Regulation 550/2004. The infrastructure operating entity had to apply to the National Supervisory Authority of the member state in their principal place of business for "certification of conformity" to the Common requirements (under EC reg. 2096/2005). By March of 2009, EGNOS was also certified according to European Interoperability Regulation (EC No 552/2004), Service Provision Regulation (EC No 550/2004) – Provision of air navigation services in the Single European Sky, Commission Regulation (EC No 2096/2005) – ANSP certification process and Safety Oversight Regulation (EC No1315/2007).

Other regulatory guidance has created more specific technical requirements. For example, FAA Advisory Circular AC90-100A, Europe Aviation Safety Agency (EASA) requirements AMC 20-4 and JAA TGL10 as well as the International Civil Aviation Organization's (ICAO's) Performance-Based Navigation (PBN) Manual, Doc 9613 have encouraged the use of Receiver Autonomous Integrity Monitoring (RAIM) when GNSS is the primary navigation aid. RAIM detects faults with redundant GNSS measurements. Additional signals that are not used in calculating the receivers location, for instance from other satellites arrays, are used to confirm the fixes derived from the main system. EGNOS assumes fault free performance from the GPS/GLONASS constellation. These satellites are outside the control of the immediate infrastructure operators. RAIM techniques can, however, be introduced by the end users of EGNOS services. Reliability tests are conducted in real time on the aircraft to validate satellite signals against model predictions. Detection, Identification and Adaptation (DIA) procedures can be used to locate outliers and anomalies in the range measurements that may then be excluded or used to indicate problems in the calculated position. From the users' perspective RAIM services can be directly integrated into existing navigation systems. They can also assist pilots to plan around periods of reduced GNSS availability. In critical phases of flight, such as an approach, the pilot needs to be informed of such inaccuracies as soon as possible so that they can determine whether or not to perform a go-around manoeuvre etc (Oliveira and Tiberius, 2008).

An Introduction to Dependability and Safety Cases

The previous paragraphs have identified the range of evidence that supports safety arguments for the Safety of Life (SoL) applications of Satellite based Augmentation Systems (SBAS). The diversity of test data, of development standards and of audits 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 structure safety argumentation (Johnson, 1999, Bloomfield and Bishop, 2010). Figure 2 illustrates the syntactic components of the Goal Structuring Notation (GSN) (Kelly and Weaver, 2004). A *goal or claim* represents an assertion that can be assessed as either true or false. For instance, a developer might 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 *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 be used to support many different safety arguments. For instance, 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 *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.

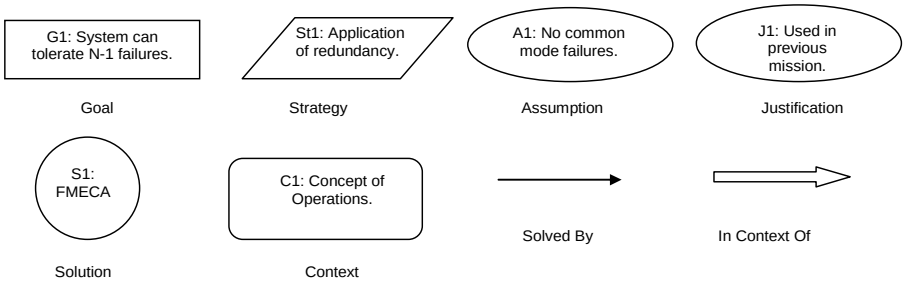

Figure 2: Components of Safety Argumentation Techniques

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 components in a safety case.

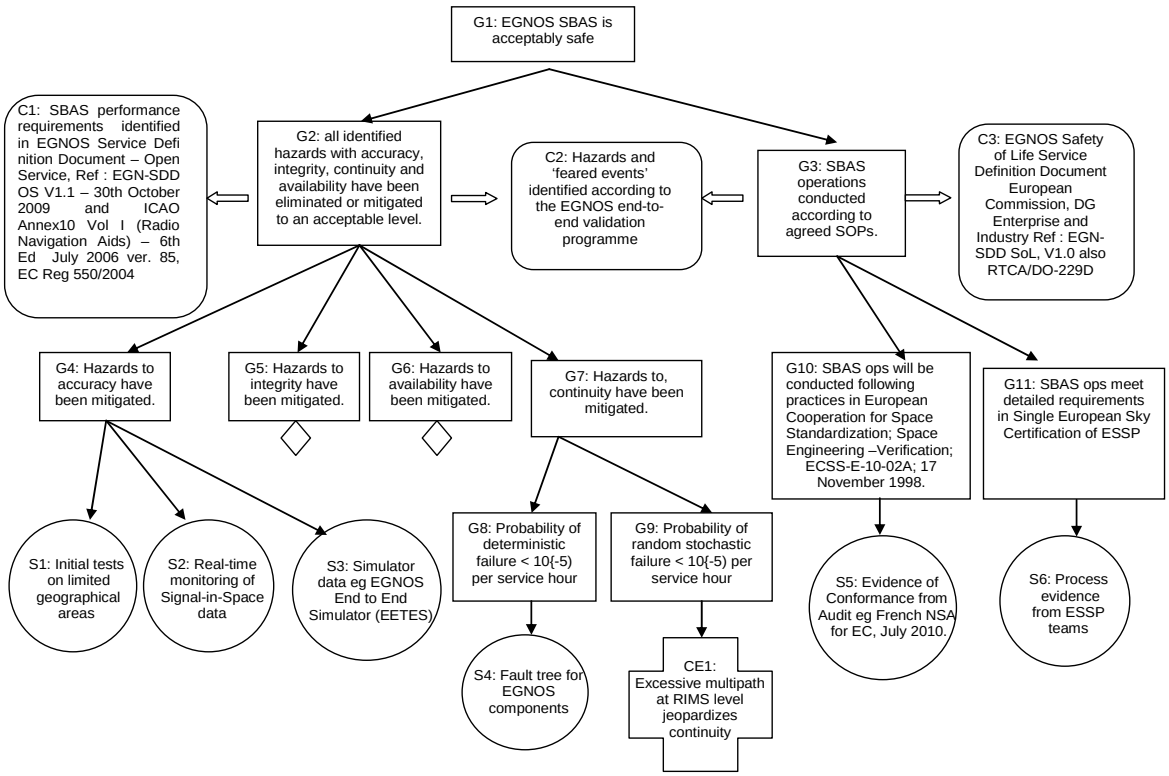

Figure 3: Initial GSN for Satellite Based Augmentation Systems (SBAS)

Figure 3 illustrates an application of the GSN approach to provide a high-level sketch of 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 acceptable 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 identified safety requirements documents 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.

The sub-goal G2 is, in turn, broken down into further aims that focus on the mitigation of hazards associated with each of the ICAO performance criteria, G4 to G7. 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. It is important to stress that Figure 3 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 provides few guarantees that accuracy concerns would be addressed under a wide range of potential operating conditions. Hence, the evidence summarised 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 that concerns over excessive multipath effects at the Ranging and Integrity Monitoring Stations (RIMS). This raised concerns over the ability to meet continuity requirements. Figure 3 illustrates this using CE1. Such extensions illustrate the need to further develop the safety argument– through both redesign and the collation of additional evidence to increase confidence that the overall goal can be sustained.

It is important to stress that the safety case structure illustrated in Figure 3 was intended to provide an introduction to the overall approach. In practice, these diagrams quickly grow both in scale and complexity. The EGNOS safety case was developed to support the certification for SoL applications across the European aviation industry. It, therefore, goes well beyond the sketch presented in Figure 3, by considering RAIMS receiver-based fault detection through to the integration with end user applications. The EGNOS safety case also exploits a modular structure that separates design and development from operations (Johnson and Atencia Yepez, 2010). 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. As we shall see, a further argument for introducing the simplifications illustrated in Figure 3 is so that we do not publicise potential vulnerabilities in the GNSS architecture as we consider more detailed security threats.

Security Threats to GNSS Infrastructures

The remainder of this paper identifies the ways in which cyber security threats undermine the arguments that are made in safety cases. Denial of service attacks, threats to data integrity, spoofing combine to invalidate many of the assumptions that support the provision of critical services. An early warning of potential security concerns was provided by an approach into New Jersey during December 1997. A Continental trans-Atlantic flight lost all GPS signals. It was initially believed that this had been caused by an intentional jamming attack, however, it later turned out to have been the result of a US military test that had unintended consequences. A 200-kilometer "interference zone" was created by a GPS antenna with a 5-watt signal, stepping through frequencies.

The potential threat for maritime navigation can be illustrated by a study in 2008 conducted for the UK Lighthouse Authorities and the UK Ministry of Defence (MOD) Defence Science and Technology Laboratory (Grant, Williams, Ward and Basker, 2009). A medium powered jamming device was used to generate noise over a pre-defined area of the UK coastline. This had a severe effect on maritime GPS signals. The subsequent report identified a broad range of potential threats. There was an obvious impact on navigation aids over a large geographical area. It is difficult to underestimate the impact that this could have for mutual situation awareness. Particular problems were identified for vessels fitted with integrated bridge systems. This technology brings together navigation systems with autopilot control so that a jammed GPS signal could lead to a significant deviation without warning the crew. Even if the crew are alerted there are significant barriers to identifying the correct position given the loss of situation awareness, mentioned above. The crews in this trial were all aware that the GPS signals would be jammed, however, they struggled to respond as numerous alarms provided additional distractions and significantly increased workload as they continued to cross-check navigational information. The impact for on-board systems was compounded by the impact of jamming for on-shore services. In particular, it became difficult to compile the Vessel Traffic Services information that provides an overview of traffic in coastal areas. Some of the data returned by vessels was based on erroneous GPS input that contradicted radar sources.

These initial studies have been mirrored by more malicious attacks. The relatively low cost of GPS technology and the widespread provision of detailed information about satellite based infrastructures has made it relatively easy to construct low cost jamming devices. Existing first generation GNSS infrastructures provide little support for users trying to authenticate signals. This makes them vulnerable to spoofing through the broadcast of fake GNSS-like signals or through rebroadcast of valid GNSS signals to create confusion. It is illegal to offer jamming equipment for sale within the European Union. However, these provisions can be interpreted as a by-product of Electro-Magnetic Compatibility (EMC) directives that were originally drafted with other ends in mind. Within the UK, national legislation prevents the operation of a jammer but it is not illegal to own such a device (RAE, 2011).

Many of the vulnerabilities associated with convention 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. This helps to explain the relative ease with which it is possible to spoof first-generation GNSS signals. In many cases this is done unintentionally, hence the

provisions of the EMC directives that are intended to minimise the risks of such interference. However, almost all western military organisations have experimented with tools and techniques to deliberately jam the GNSS signals of opposing forces. Not only has this resulted in the development of specialist devices, it has also led to the development of simulation tools that enable planners to identify the optimal allocation and distribution of jamming systems. The military development of satellite navigation jamming devices has been mirrored by the rise of low-cost, hand held systems that cost little more than $100 and have a range of several kilometres. 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 a relatively simple matter to create broad band noise or pulsed signals that will disrupt GNSS services. It is more difficult, however, to 'spoof' location information so that a receiver will be fooled into using an alternate location signal. The last decade has seen the development of signal simulation software that will 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 will fool a receiver into thinking that it is following the 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. As before, the potential rewards are significant if consignments can be diverted to alternate destinations. The criminal motivations for developing these hybrid technologies will multiply in proportion to the diversification of GNSS applications – these would include the use of spoofing devices to undermine route monitoring for toll or insurance pricing.

A recent report from the UK Royal Academy of Engineering (2011) enumerated the security risks associated with any 'overreliance' on GNSS infrastructures. This argued that some 6% of GDP in Western Countries was dependent on this technology. A range of threats were identified, including those mentioned above. The report criticised the lack of backup technologies and went on to make a number of recommendations. For example, it was argued that critical infrastructures should include GNSS vulnerabilities within their risk assessments. National response teams should also be organised to coordinate this analysis. In addition, the safety arguments supporting critical applications should be extended to consider what might happen during GNSS outages for various periods of time ranging from ten minutes to a month. 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. Finally, recommendations proposed the development and application of alternative technologies including terrestrial GNS proxies, such as eLoran. eLoran is a radio based triangulation system that does not yet provide security services comparable to those embedded within SBAS. However, it might provide an additional external reference to complement the RAIM applications described in previous sections. The Royal Academy report did not consider the detailed cost implications of developing these redundant infrastructures.

As mentioned above, a key finding from the recent UK review was that national infrastructure providers and other safety-related users of GNSS services should conduct systematic risk assessments to assess their vulnerability to the loss of navigation and timing information. The limited scope of the RAE report did not, however, provide opportunities to discuss the techniques that might be used to support such analyses. In contrast, the following paragraphs identify a range of ways in which argumentation techniques might be extended from the development of safety cases to increase the resilience of SBAS applications.

The Integration of Security and Safety Cases

Safety argumentation techniques have been applied to address security concerns. Elberzhager, Klaus and Jawurek (2009) have introduced the concept of security goal indicator trees that offer many of the same benefits provided by argumentation techniques for safety cases. In contrast, Goodenough, Lipson and Weinstock (2008) have extended the application of GSN to create security assurance cases. Their work focuses on software concerns. The example they use includes a claim about the absence of buffer overflow vulnerabilities. They support this with arguments that programmers were trained to avoid such vulnerabilities in their code and that other programmers were used to review the software. A further argument focussed on the use of static analysis tools to identify potential problems. The final argument rested on a series of test cases that were created to determine if known vulnerabilities appeared in the final code. As we have seen for safety cases, the security argumentation structures were developed to record the array of evidence that supported each of these lines of argument – including records of training provided to the coders, the reports of external auditors, test logs and so on. ISO 15026 has helped to motivate many of these projects; it introduces the concept of a security assurance case. In this case, the top level goal is to demonstrate that a system is acceptably secure. This has led to the

promotion of dependability arguments as a generalisation beyond safety to consider wider reliability requirements.

Unfortunately, security assurance cases have not been widely applied by industry. In particular, they have not previously informed the reliability engineering of GNSS infrastructures. This can be explained in terms of a Catch-22 argument. We have few examples of security assurance arguments; hence there are few templates that might be re-used to inform the development of security cases. Conversely, we are unlikely to be able to provide appropriate templates for security argumentation until they are more case studies in the application of this approach. These problems are further compounded by the understandable reluctance of those organisations who have exploited this approach to publish their findings, given that the graphical structures encapsulate the measures they have taken to mitigate security risks.

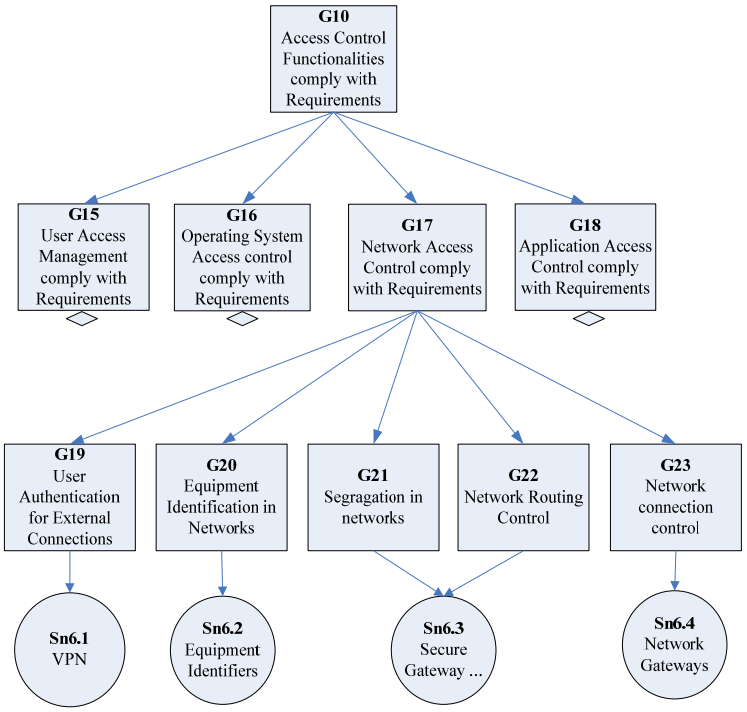

Figure 4: Sub-section of He's Generic Security Argumentation Structure (With Permission)

These limitations have led Ying He (2011) to develop a generic security argumentation structure that integrates components of security cases from many different applications. A subsection of this approach is illustrated in Figure 4. The intention is to provide a template that can be used and reused to structure the specific safety arguments that must be used in support of the any particular application. For example, the top level goal is to ensure that a system is acceptably secure. One set of sub-claims then develops argumentation that related to the application of security standards. Another sub-goal deals with arguments relating to the competency and recruitment of security professionals. Further areas of the generic argumentation structure help to structure arguments about the development and maintenance of security management systems (SecMS). The lower levels of the tree help to identify the sources of evidence that might be gathered to support the arguments used in diverse security applications, for instance showing how external audits might be used to verify the implementation of a SecMS. An important aim in this approach is to encourage a consistent approach to security across complex organisations by guiding analysts in the creation of dependability arguments. Subsequent weaknesses identified in one application can then be used to strengthen the security cases made for a wider class of systems. However, this work is relatively immature and a number of problems remain to be addressed before He's approach can support the reliability of safety-related GNSS architectures. Although the security certification of EGNOS is based on EC 2096 through the ISO/IEC 27001 standard; the generic security structure has not been instantiated to support this class of applications. It is unclear whether the template can identify appropriate mitigations for the broad range of military and civil threats to satellite timing and navigation systems enumerated in this paper.

A further problem for all of the approaches cited above is that it is unclear how to develop a dependability case that effectively integrates both security and safety concerns. The previous sections of this paper have argued that we are at a cross-roads in terms of GNSS provision. Last month, Europe certified the EGNOS SBAS for

use in Safety of Life applications. At almost the same time, the RAE report focussed attention on the security vulnerabilities that can be exposed by our increasing reliance on these infrastructures. Of course, one approach would simply be to integrate safety and security arguments into one enormous graphical structure. This ad hoc approach is flawed unless there is some means of representing and reasoning about the interactions that exist between security and safety. This can be illustrated by the extended GSN illustrated in Figure 5.

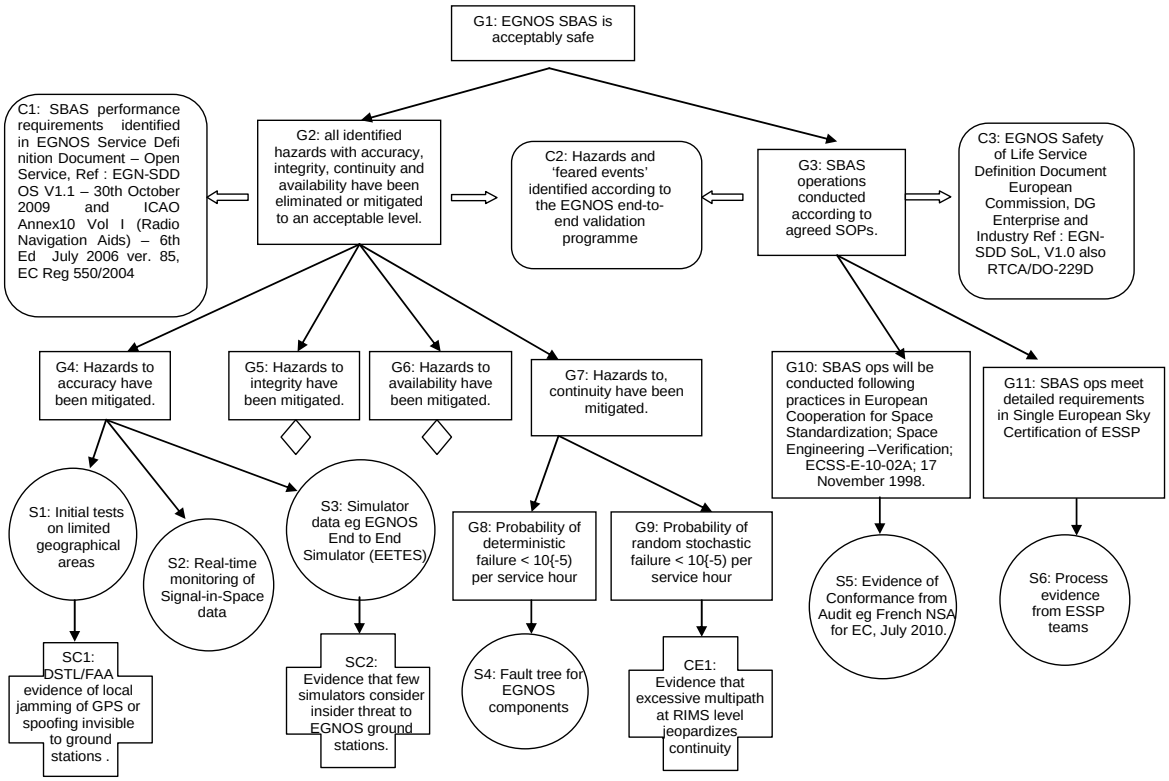

Figure 5: Integrating Security Threats to GNSS Architectures within GSN Safety Arguments

This illustrates how we are integrating security threats into safety arguments for GSN architectures. The overall approach is to use convention forms of security threat analysis to identify evidence that might undermine the evidence that we use at the lower layers of a safety case. In this case our aim is NOT to make general claims about the security of a GNSS architecture; this can be done using any of the specialise security argumentation techniques mentioned earlier. In contrast, we are specifically concerned to identify the impact that security threats might have upon the **safety** of an implementation. In this case, we can see two safety concerns. The first uses evidence susch as the UK MOD studies to identify the potential for localised 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 mentioned in previous sections of this paper. 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 5 also includes a second set of security concerns based around the potential 'insider threat' to GNSS infrastructures. These are rarely modelled within simulation environments, however, coordinated attacks by individuals who are familiar with the ground architecture of an SBAS system would undermine many of the defences that are intended to mitigate the impact of individual human errors.

Conclusions

Safety cases provide high-level support for the development of critical systems. They present a graphical overview of the arguments and evidence, which can demonstrate that complex applications are acceptably safe within a particular context of use. This paper shows how safety cases can be used to support the latest generation of augmented Global Navigation Satellite Systems (GNSS). We have chosen these applications because they have recently been approved for use in safety-related applications across Europe and North America. Unfortunately, at the same time that these satellite based systems have been approved for location and timing information in safety-critical applications, a range of organisations including the US Department of

Defense and UK Ministry of Defence, have raised concerns about increasing civil vulnerability to attacks on the underlying infrastructures.

Further concerns arise because 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 security 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.

J. Goodenough, H. Lipson and C. Weinstock, Arguing Security - Creating Security Assurance Cases, Software Engineering Institute, Carnegie Mellon University, 2008. Available as of 19/3/2011 on https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/assurance/643-BSI.pdf

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.

Y. He, A Generic template for Security Arguments, Technical Report, University of Glasgow, Scotland 2011.

C.M. Holloway, Safety Case Notations: Alternatives for the Non-Graphically Inclined? In C.W. Johnson and P. Casely (eds.), Proceedings of the IET 3nd International Conference on System Safety, IET Press, Savoy Place, London, 2008.

C.W. Johnson, A First Step Towards the Integration of Accident Reports and Constructive Design Documents. In M. Felici, K. Kanoun and A. Pasquini (eds.), Computer Safety, Reliability and Security: Proceedings of 18th International Conference SAFECOMP'99, 286-296, Springer Verlag, 1999.

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.

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

Biography

Chris.W. Johnson, DPhil, MA, MSc, FBCS, CEng, CITP,
School of Computing Science, Univ. of Glasgow, Glasgow, G12 8RZ, Scotland, UK.
Tel +44(141)3306053, Fax +44(141)3304913, Johnson@dcs.gla.ac.uk, http://www.dcs.gla.ac.uk/~johnson

Chris Johnson is Professor of Computing Science at the University of Glasgow in Scotland. He heads a small research group devoted to improving the reporting and analysis of incidents and accidents across safety-critical domains ranging from healthcare, to the military to aviation and rail.

Amaya Atencia Yepez,
GNSS Business Unit, GMV, C/ Isaac Newton 11, PTM, 28760 Tres Cantos, Spain
Tel + 34918072257 , Fax +34 918072199, E-mail: aatencia@gmv.com

Amaya Atencia Yepez is...