SAFETY ARGUMENTS FOR NEXT GENERATION, LOCATION AWARE COMPUTING

C.W. Johnson[†] and C.M. Holloway*,

[†]Department of Computing Science, University of Glasgow, Glasgow, Scotland, UK, G12 8RZ.
johnson@dcs.gla.ac.uk, http://www.dcs.gla.ac.uk/~johnson

*NASA Langley Research Center, 100 NASA Road, Hampton VA, 23681-2199, USA,
c.m.holloway@nasa.gov

Keywords: WAAS, EGNOS, location aware systems, safety.

Abstract

Concerns over accuracy, availability, integrity, and continuity have limited the integration of Global Positioning System (GPS) and Global Navigation Satellite System (GLONASS) for safety-critical applications. More recent augmentation systems, such as the European Geostationary Navigation Overlay Service (EGNOS) and the North American Wide Area Augmentation System (WAAS) have begun to address these concerns. Augmentation architectures build on the existing GPS/GLONASS infrastructures to support location-based services in Safety of Life (SoL) applications. Much of the technical development has been directed by air traffic management requirements, in anticipation of the more extensive support to be offered by GPS III and Galileo. WAAS has already been approved to provide vertical guidance for aviation applications. During the next twelve months, the full certification of EGNOS for SoL applications is expected. This paper discusses similarities and differences between the safety assessment techniques used in Europe and North America.

1 Introduction

Navigational aids have been integrated into a broad range of safety-related applications. For example, a recent accident report described the standard navigational aids on board a fishing vessel equipped for a crew of three: a radar, an echo sounder, a watch keepers' alarm, and an autopilot. The fishing vessel also carried two GPS plotters and a GPS receiver (Maritime New Zealand, 2004). The subsequent investigation found that the vessel had run aground because the skipper had not set waypoints but had instead been using the cursor on one of the GPS plotters to keep an informal note of course and position. Pilots, mariners and drivers have placed undue confidence in GPS and GLONASS[1] applications (Johnson, Shea and Holloway, 2008).

Security concerns have also limited the integration of GNSS into safety-related applications. It is relatively easy to jam low powered transmissions. First generation infrastructures lack authentication mechanisms. This makes them vulnerable to spoofing through the broadcast of fake signals or through rebroadcast of valid GNSS signals.

Other problems stem from the inherent inaccuracies within first generation satellite-based navigation systems (Johnson and Atencia Yepez, 2010). These arise from satellite geometry. For example, if all the satellites are closely grouped together then the benefits of differential signal processing will be reduced. Gravitational forces create subtle changes in the orbit of the satellites within a GNSS constellation. Multipath errors arise when the signals arriving at a receiver are reflected from large structures including buildings. Atmospheric effects are also important. Radio waves can be considered to travel at the speed of light in outer space. However, this is reduced in the ionosphere (80-400km) where the ionizing effects of solar radiation form layers that refract electromagnetic waves from satellite transmissions. Each GNSS message exchange helps to synchronize the receiver's clock. However, clock inaccuracies lead to an error of around 2 meters with an additional 1 meter being due to rounding and calculation problems. Relativistic effects can arise when GPS satellites move at more than 12,000 km/h relative to the receivers. Time also moves more slowly in stronger gravitational fields and satellites are exposed to a much weaker gravitational force than earth-bound receivers.

Regulators have responded to these concerns by placing strict limits on the use of GNSS in safety-related applications. The International Civil Aviation Organization (ICAO) has drafted the following Required Navigation Performance parameters:

- *Accuracy*. How correct is the position estimate;
- *Integrity*. The largest position error that might arise without detection;
- *Availability*. How often can the systems be used within the desired levels of Accuracy and Integrity;
- *Continuity*. The probability that an operation once commenced can be completed.

In North America, the WAAS Satellite Based Augmentation System has already been approved to provide vertical guidance against these criteria in aviation applications.

[1] For the remainder of this paper GNSS will be used to refer to GPS and GLONASS together.

During the next twelve months, the full certification of EGNOS for SoL applications is expected. This papers use these architectures to illustrate key concepts behind the safety of augmentation-based-GNSS that provide a stepping stone to next generation architectures, including Galileo and GPS III.

EGNOS uses a network of approximately 40 ground stations and 3 geostationary satellites. The ground stations compare known information about the time and location with the signals received from the satellites to derive error measurements. This information is collated by four master stations that broadcast corrections using the geostationary network. End users then apply these corrections to location information derived from the GNSS networks. The net effect is to improve accuracy from 17-20 meters to around 2 meters in the augmented approach. Continuity is supported by the use of redundancy; each of the four master stations rotates from being active to serve as either hot or cold-back-up. The WAAS architecture exploits a similar combination of ground stations and satellite correction broadcasts with similar improvements in horizontal and vertical accuracy.

2. Safety-Assessments for GNSS Infrastructures

The Probability of Hazardously Misleading Information (PHMI) is an important metric for the certification of augmentation systems (Blanch, Walter and Enge, 2007). This metric measures the likelihood that the information contained in a navigation message leads to a position error larger than a particular error bound, known as the protection level. The Safety of Life (SoL) user can then assess the risk that the accuracy falls below the threshold and thus determine whether or not it is 'safe' to rely on location services.

For instance, the FAA maintains that WAAS will alert aircrew within 6-8 seconds, depending on the airborne equipment, whenever the input signal for positioning becomes unusable. The PHMI must be less than 1E-07 for the specified vertical and horizontal protection levels (FAA, 2010).

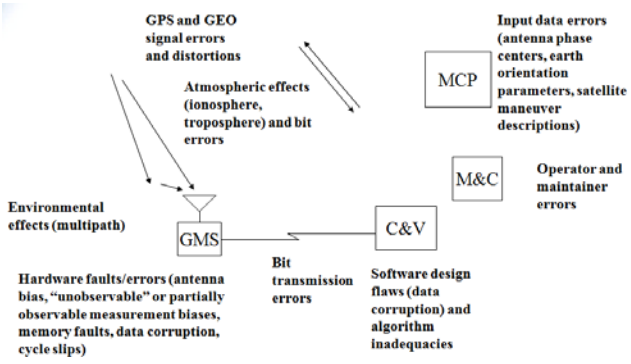

Figure 1: Integrity threats to satellite-based augmentation systems

Figure 1 (Fernow, 2005) provides an overview of the various sources of error in satellite-based augmentation system (SBAS) architectures, including signal errors from the space based components through to hardware and software failures on the ground based segments. Mitigations must be introduced to ensure that the SBAS infrastructure remains within the PHMI limits established by the regulators.

2.1 Analysing Error Distributions

The safety assessment for SBAS architectures has been driven by a need to over-bound range error distributions. As mentioned, EGNOS and WAAS rely on ground stations to estimate satellite ranging errors that are then used to broadcast corrections to mobile users. These corrections cannot easily anticipate errors that have a different impact on the fixed ground stations compared with mobile end users. The SBAS, therefore, also broadcasts confidence limits on navigation accuracy that try to over-bound these less predictable errors. End-users apply this information to calculate an 'error buffer' around their estimated location.

The calculation of the confidence interval falls into two different tasks. First, it is necessary to identify the core of the error distribution that represents possible biases under routine operations. Secondly, it is necessary to identify the tails of the distribution. These small probabilities are in the order of 10-7 (Rife, Walter and Blanch, 2004). They represent receiver dependent errors that are the result of less predictable effects including ionospheric and tropospheric gradients, radio interference etc.

Computing range error distributions is complicated by a lack of operational data. Regulatory organisations have, therefore, commissioned studies to gather evidence about the core and the tails of the error distributions experienced by aviation users. Further problems arise because it is hard to distinguish between different sources of error in direct observations. This is necessary to determine which hazards can be predicted during particular operational conditions.

If a source of error can be anticipated then mitigations can be introduced to exclude it from the PHMI. The WAAS PHMI cannot be averaged over conditions that are unknown but constant or repeatable over time (Blanch, Walter and Enge, 2007). In addition, the WAAS teams used analytical techniques to characterise the tails of the error distribution. This introduced elements of subjectivity: domain experts had to identify the threat mechanisms that could contribute to low probability events. The limited amount of direct data meant that extrapolation was used throughout the analysis. The resulting threat models covered ionospheric errors, tropospheric delays, and multipath issues. The intention was to place a bound on the worst case impact of these threats and to assign probabilities to them.

2.2 Risk Assessments

In addition to the position and range errors from secondary effects, such as tropospheric gradients, it was also necessary to identify the failure modes that might affect WAAS and

EGNOS architectures. These included software errors as well as hardware/processor failures for the ground based stations.

In both the United States and in Europe, Failure Modes Effects Analysis was used to support hazard identification. Fault Trees then helped to assess mitigations. There are, however, contrasts between the safety assessment methods used in both projects. For example, the EGNOS team took steps to mitigate human errors that might lead to a loss of integrity (Johnson and Atencia Yepez, 2010). The WAAS team did not explicitly include maintenance failures within their systems level fault tree analysis: "WAAS design is such that the WAAS operator and maintainer cannot cause HMI" (Fernow, 2005). These risk assessments were supported by the static analysis of PHMI algorithms. These studies identified a number of what the EGNOS team termed 'feared events' and the WAAS groups called 'system threats' (Fernow, 2005). Threat models and detection algorithms were developed for each of the hazards. These were then used to drive an estimation of their contribution to the PHMI.

2.3 Receiver Autonomous Integrity Monitoring

Receiver Autonomous Integrity Monitoring (RAIM) provides techniques for mitigating many of the hazards that can arise for GNSS architectures. Europe Aviation Safety Agency (EASA) requirements AMC 20-4 and JAA TGL10 and ICAO's Performance-Based Navigation (PBN) Manual, Doc 9613 have encouraged the use of RAIM when satellite based systems provide primary navigation aids. RAIM detects faults with redundant GNSS measurements. Additional signals that are not used in calculating the receiver's location, for instance from other satellite arrays, are used to confirm the fixes derived from the main system.

In the Galileo architecture, RAIM techniques can be used to exclude data from satellites that provide unreliable signals. This is not, typically, possible in augmentation systems that have less control over the underlying satellite networks. EGNOS and WAAS assume fault free performance from the GNSS constellation in calculating the protection level. In the case of EGNOS, these satellites are outside the control of the immediate infrastructure operators. However, the system assurance and monitoring techniques described in previous sections offer a level of confidence that justifies the omission of RAIM within these SBAS core architectures.

RAIM techniques can, however, be introduced by the end users of EGNOS and WAAS services. Reliability tests are conducted in real time on the aircraft to validate satellite signals against model predictions. Detection, Identification and Adaptation 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).

2.4 WAAS and Process Based Safety Assurance

The application of risk assessment and mitigation techniques has been supported by process based approaches to system safety. This was embodied within the Safety Assurance Requirements Process (SARP) of the WAAS programme. The SARP was supported by the application of a range of process based standards, including RTCA DO-178B. These assurance processes were developed in response to earlier criticisms from the US Government Accountability Office (GAO, 2000). The GAO identified a need for greater supervision and audit across the WAAS initiative. The requirements process provided guidelines for the peer and external reviews that were intended to ensure the system architecture and design mitigated the PHMI related hazards. The key inputs to SARP were documents including, but not limited to, the detailed plans that described how various software and hardware standards would be applied within the project. They also included specifications, requirements and design documents for sub-systems and the meta-level architectural components as well as system safety assessments, component implementation guides, system integration documentations and the outcome of acceptance testing (FAA, 2005).

A series of assertions were developed to characterise both internal and external failure modes within the WAAS architecture. External assertions stemmed from reliability requirements for the GPS infrastructure. These were of obvious concern not only to the FAA but also to EUROCONTROL and the European Space Agency (ESA) as they sought to develop EGNOS on top of the same GPS architecture. The exchange of WAAS information about common failure modes had to be mediated with the US Department of Defense. The internal assertions identified by the WAAS teams included proprietary information related to the implementation techniques used by contractors. Proprietary concerns, therefore, created some additional barriers to the exchange of integrity lessons between WAAS and EGNOS.

The process-based approach to safety assurance within the WAAS program used a wide range of additional techniques. The analysis of the PHMI algorithms was supported by an assessment of input-output relationships for the processors used within the ground based segments. Timings were verified using latency analysis. These diverse analytical techniques were essential given the reliance on software components and stochastic systems that could not be completely verified using exhaustive testing techniques.

One of the most significant differences between the European and North American approaches was the degree of integration between the infrastructure safety assessments and those that were developed at the application level. EUROCONTROL worked with ESA to introduce a degree of separation between

these complementary activities. In contrast, the FAA supported a more bottom-up approach in which there was a close integration between the safety assessments on the infrastructure and those that guided the development of initial aviation applications.

The contractor, Raytheon, drove the initial infrastructure analysis that led to the identification of the assertions, mentioned in previous paragraphs. These were then used to support the development of more detailed application-level fault trees. These diagrams were then reviewed by the FAA and their subcontractors. The reliability analysis focused on non-precision, Lateral Navigation (LNAV) and Vertical Navigation (VNAV) approaches. LNAV approaches tend to involve 'non-precision' incremental descents rather than following a fixed glide slope with electronic slope guidance down to a decision altitude. The LNAV accuracy required by the FAA was greater than or equal to 36 meters with a PHMI of less than 1×10^{-7} per hour.

The drafting of fault trees that capture both infrastructure and application hazards reflects close cooperation between WAAS infrastructure developers and system integrators. The hazard analysis for LNAC and NVAN approaches directly supported SBAS avionics development following DO-229C, TSO-C145/146. A similar approach was adopted during the development of SBAS localizer performance with vertical guidance (LPV). These rely on GNSS receivers at airports without Instrument Landing Systems. Pilots use WAAS to descend under vertical guidance to decision altitudes as low as 250 feet above the runway. This illustrates a further important feature of WAAS development. 'In service' experience has been used to justify changes in the safety assessments. In March 2006, some three years after the initial LPV certification, the FAA extended its operation down to decision altitudes as low as 200 feet above the runway.

2.5 EGNOS and the Role of Safety Cases

Previous sections have identified the similarities that exist in the safety assurance processes behind both the EGNOS and WAAS SBAS programmes. Both have used process based techniques that are consistent with existing aviation development standards to structure the integration of model based analysis with limited operational data. However, it is possible to identify significant differences in the approaches that have been adopted in Europe and North America.

As we have seen, there was a tight integration between infrastructure and application development within the US programme. This was an inevitable consequence both of the pioneering nature of the augmentation system but also arguably was a consequence of the influence exerted by critical GAO reports. These had urged closer oversight and cooperation to ensure the delivery of usable systems within the WAAS programme (GAO, 2000). In other work we have reviewed the unintended technical consequences of such political and administrative interventions (Johnson, 2009).

In contrast, the European initiatives developed a more modular approach based around safety cases. This was intended to simplify the future application of EGNOS to a wide range of applications. The safety case structures the technical documentation that demonstrates compliance with both ICAO and the Single European Skies requirements. Figure 2 shows how the EGNOS safety arguments have been separated into several components.

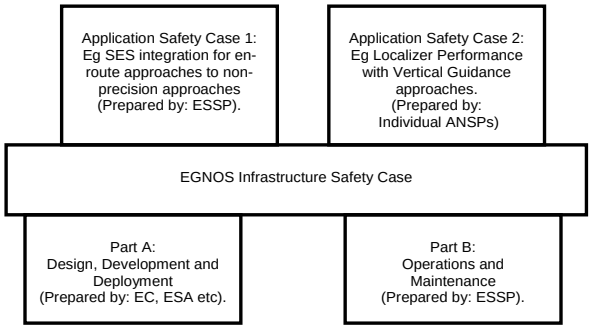

Figure 2: Overview of the EGNOS Safety Case Structure for Air Traffic Management

Part A: EGNOS Design Safety Case explains why the system has been 'designed, developed and deployed' in a manner compliant to ICAO Standards and Recommended Practices (SARPS). This part was coordinated by the EC with support from the European Space Agency as the lead body in the initial design of the EGNOS architecture. It resembles many elements of the internal and external safety assessments developed during the initial WAAS programme.

Part B: Operations Safety Case provides further arguments and evidence to show that the EGNOS system will be operated and maintained to meet the requirements identified in Part A. The commercial operator for the augmentation system, European Satellite Services Provider (ESSP), is responsible for this component of the supporting documentation. Elements of this safety argument are covered within the internal safety assessments for the US WAAS programme. The EGNOS Part B safety case also builds on monitoring techniques that resemble those used in North America. Operational studies continue to provide evidence of conformance to ICAO Required Navigation Performance. The in-space monitoring was coordinated by EUROCONTROL, firstly by reviewing the existing EGNOS datasets and then by harmonizing the aggregation of the available performance data. Their concern was not simply to demonstrate performance levels using optimal equipment but to assess integrity, availability etc replicating a 'minimally equipped' aviation user at different locations in the EGNOS service area (ESA, 2009).

Application Safety Cases. Parts A and B provide the arguments that the EGNOS infrastructure will be acceptably safe for integration within European Air Traffic Management. Additional safety cases are then required for each of the applications that are built on top of this architecture. ESSP

are responsible for developing safety arguments that support the integration of EGNOS information during en-route operations and non-precision approaches. The aim of each application safety case is to demonstrate that the target level of safety can be met. This is done by demonstrating that the safety of EGNOS applications will be at least equivalent to those GPS-based operations that have already been approved.

The EGNOS approach can also be illustrated by LPV approaches. As mentioned, these are similar to conventional Instrument Landing Systems (ILS) with the addition of GNSS receivers. Within the EGNOS certification process, it is the responsibility of individual Air Navigation Service Providers (ANSP) to develop the safety cases that justify the use of these technologies for particular approaches. This illustrates a second explanation for the modular approach adopted by the European application of SBAS within Air Traffic Management. Differences between the Standard Operating Procedures and technical infrastructures provided by different member states create particular problems in developing a single safety argument that could be used across all nations.

There is a danger that member states may use inconsistent and potentially contradictory arguments in their various safety cases. There is no guarantee that hazards mitigated by one ANSP will be addressed in the same way by a neighbouring service provider. EUROCONTROL have, therefore, developed a generic argument for Approach Procedures with Vertical guidance (APV) using EGNOS. This high-level safety case is intended to provide a template for member states and is illustrated in Figure 3 (Johnson and Atencia Yepez, 2010). Individual service providers, shown as ANSP X and ANSP Y, must instantiate the generic safety case for their own operating environment. Figure 3 also shows that other Service Providers, illustrated as ANSP Z, may reject the template and instead construct their safety arguments directly on top of the safety cases developed by ESA and ESSP.

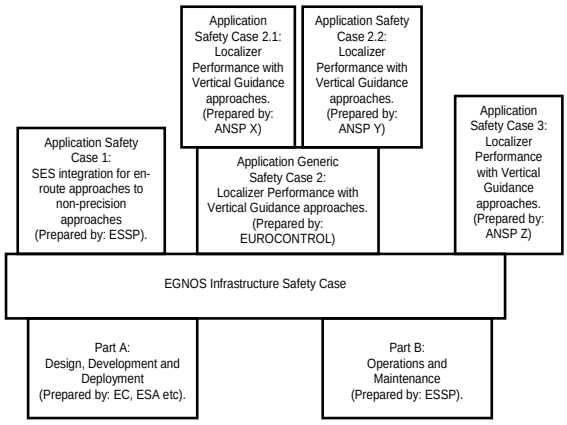

Figure 3: EGNOS Safety Case Structure for approaches

This structure raises further concerns. The development of modular safety cases implies that any underlying weaknesses in EGNOS parts A or B will be propagated into the applications that depend upon them. ANSP X and Y must trust the arguments used for the two underlying levels. The architecture illustrated in Figure 3 assumes that any SBAS hazards will be adequately addressed by arguments in Parts A or B. However, it may also be possible to introduce additional protection into the application level safety cases. This will be difficult when many of the hazards addressed in lower levels of the argumentation structure may not be visible to the engineers working on end-user development. The WAAS approach avoids some of these concerns because the same contractors helped to develop safety arguments for the infrastructure and applications.

There is a danger that the safety managers who develop the arguments used to justify higher level applications may not accurately understand the evidence or constraints that limit claims about the safety of underlying infrastructures. There is some confusion amongst GNSS users about the integrity concepts that support augmentation systems. This creates significant concerns when the properties of those implementations have a profound impact on reliability attributes.

These communication problems were minimised during WAAS development because the GAO reports urged closer and closer integration between infrastructure and application development. External and internal assertions were accurately embedded within the integrated WAAS fault trees. The boundaries between safety arguments are seldom as clear as they might seem in Figures 2 and 3. In practice, it is likely that the generic and application level safety arguments will make reference to evidence used in lower levels of the infrastructure safety cases. This creates concerns about common vulnerabilities where the refutation of a particular non-functional requirement or assertion would undermine safety arguments across all of the components illustrated in these high-level architectures.

A final area of concern for both the WAAS and EGNOS approaches is that SBAS are intended to support a wide range of applications. The previous development of these infrastructures has been tailored towards aviation applications. In consequence, many of the concerns over consistency in the case of EGNOS and of modularity/reuse in the case of WAAS can be overcome through a myriad of personal, professional and regulatory connections between the infrastructure operators and end users.

The next six months will see the extension of EGNOS support to SoL applications well beyond the aviation examples cited in this paper. It remains to be seen whether the threats and hazards, the constraints and assertions that have informed existing safety arguments will be adequately considered by end users in everything from rail transportation through search and rescue applications to the process industries. The EGNOS SoL infrastructure will only enter into service during the second half of 2010. We, therefore, lack direct operational evidence about the commonality and differences between the safety arguments required in different application

domains. It is difficult to determine whether or not the safety arguments will be different between various Air Navigation Service Providers. Previous studies have shown that significant differences arise from the mitigations that can be used to address potential hazards from the failure of SBAS systems (Johnson and Atencia Yepez, 2010). For example, ground based safety net applications that exist in some countries are not available in neighboring countries or even in other regions within the same state. Only the future will tell whether these differences within the field of Air Traffic Safety Management are even more marked in the safety cases that support SBAS applications across other industries.

3. Conclusions

Concerns over the accuracy, availability, integrity and continuity have previously limited the integration of GNSS for safety-critical applications. More recent augmentation systems, such as EGNOS and WAAS address these concerns. Augmentation architectures build on the existing GNSS infrastructures to support location-based services in Safety of Life applications.

This paper has identified strong similarities between the safety assessment techniques used in Europe and North America. For example, both have relied on hazard analysis techniques to derive numerical estimates for the Probability of Hazardously Misleading Information (PHMI).

The paper has also identified differences between the approaches adopted in application development. Integrated Fault Trees have been developed to consider both infrastructure hazards and their impact on non-precision RNAV/VNAV approaches using WAAS. This approach has been facilitated by close cooperation between the FAA and their sub-contractors. However, problems can arise when proprietary information is embedded within the safety assertions that support the internal design of SBAS. It may be difficult to provide competitors with the same level of detail as they try to extend the application of WAAS into further application areas. National security concerns also limit the exchange of external reliability information with the EGNOS development teams.

EGNOS applications have been supported by a more modular approach to safety-case development. This is intended to reduce complexity. Developers can build upon the infrastructure safety analysis without necessarily following every aspect of the underlying safety cases. This approach also supports the development of generic safety arguments by EUROCONTROL that can then be instantiated by individual Air Traffic Management organisations in different European states. However, problems can arise when operational insights and lessons learned might not be communicated back to the agencies that maintain the underlying safety cases. Further problems stem from the maintenance of appropriate interfaces between modular safety cases when application concerns may rely on detailed timing issues in the underlying infrastructure.

References

J. Blanch, T. Walter and P. Enge, ‘Understanding PHMI for Safety of Life Applications’, Stanford University, CA, USA, Institute of Navigation National Technical Meeting, San Diego, CA, January 2007.

Federal Aviation Adminstration. ‘System Certification (Safety Assurance) of WAAS’, Satellite Based Augmentation Systems Workshop, FAA, Washington DC, USA. 2005.

Federal Aviation Administration. Global Navigation Satellite Systems Library - Fact Sheets, Washington DC, USA. http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/library/factsheets/ [accessed April 2010].

J.P. Fernow. *WAAS Integrity Risks: Fault Tree, “Threats” and Assertions*. Centre for Advanced Aviation Systems Development, Mitre Corporation, Bedford, MA, USA, 2005.

United States General Accounting Office. *The National Airspace System: Problems Plaguing the Wide Area Augmentation System and the FAA’s Actions to Address Them*, GAO/T-RCED-00-229, 2000.

C.W. Johnson. ‘Politics and Patient Safety Don't Mix: Understanding Failure in Large-Scale Software Procurement for Healthcare Systems’. In P. Casely and C.W. Johnson (eds.) *4th IET Systems Safety Conference*, London, 2009.

C.W. Johnson, C. Shea and C.M. Holloway. ‘Trust and Interaction in GPS Related Accidents: Human Factors Safety Assessment of the Global Positioning System’. In R.J. Simmons, D.J. Mohan and M. Mullane (eds.), *Proc. 26th Int. Conf. on Systems Safety*, Vancouver, Canada 2008, Unionville, VA, USA, 2008.

C.W. Johnson and A. Atencia Yepez. ‘Safety Cases for Global Navigation Satellite Systems' Safety of Life Applications’. In *Proc of Int. Association for the Advancement of Space Safety*, Huntsville Alabama, NASA/ESA, 2010.

Maritime New Zealand Investigation Report. *Accident Report, Kathleen G Grounding, North side of Double Bay on 30 May 2004*. Maritime New Zealand REPORT 04 3484, 2004.

J. Oliveira and C. Tiberius. ‘Added Assistance to Pilots on Small Aircraft by EGNOS’. *IEEE/ION Position Location & Navigation Symposium*, Monterey, California, May 2008.

J. Rife, T. Walter and J. Blanch, ‘Overbounding SBAS and GBAS Error Distributions with Excess-Mass Functions’. T*he 2004 International Symposium on GNSS/GPS*, Sydney, Australia, 6–8 December 2004.