SAFETY CASES FOR GLOBAL NAVIGATION SATELLITE SYSTEMS' SAFETY OF LIFE (SOL) APPLICATIONS

C.W. Johnson [(1)], Amaya Atencia Yépez [(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*
E-mail: aatencia@gmv.com,
+ 34918072257 (Tel.), +34 918072199 (Fax.)

ABSTRACT

Global Navigation Satellite Systems (GNSS) have recently been enhanced to provide additional guarantees for the accuracy, reliability and coverage of their services. These infrastructures are intended to be robust against jamming. They support self-diagnostic error detection and provide end-users with detailed information about precision and integrity. In consequence, they are gradually being introduced into safety-related applications. This paper argues that greater attention needs to be paid to the ways in which these navigation infrastructures are being integrated into the safety cases that support Safety of Life (SoL) applications. In particular, we contrast the significant investments that have been made in analysing the safety of GNSS aviation applications, such as en-route operations and non-precision approaches, with the relative lack of progress in other industries. There is also a need for greater consistency between the safety arguments that support similar GNSS applications. This helps to ensure that safety managers and regulators consider a similar set of hazards when seeking to integrate these new navigation infrastructures into SoL systems. While international aviation organisations have taken important steps to establish communication mechanisms within their industry, the same cannot be said for most other industries. The ad hoc nature of the safety arguments supporting many recent proposals creates a danger that technological innovation will outstrip our commitment to mitigate or avoid future hazards. Unless these issues are address then accidents involving the first wave of SoL applications will further jeopardise the development of GNSS infrastructures.

1. INTRODUCTION

First generation GNSS infrastructures, based around GPS and similar architectures, offered limited levels of accuracy and reliability for civilian users. In consequence, they were not recommended as a primary source of navigation information in safety related applications. A second generation of technologies based on augmentation networks has been developed to support Safety of Life (SoL) applications. These can be seen as an interim stage in the development of third generation GNSS infrastructures that are deliberately intended to support levels of redundancy and reliability across all system components. They will be robust against jamming and support self-diagnostic error detection. This paper argues that we must transfer lessons both within and between industries to ensure consistency in the identification and mitigation of GNSS related risks.

2. SOURCES OF ERROR IN GNSS

Early GNSS applications were heavily influenced by ground-based architectures, such as the differential signal processing used within LORAN during the 1940s. Many of these early concepts were carried forward into the 1950s when Doppler effects were demonstrated for early satellites. By 1960, the US Navy had begun to demonstrate the feasibility of satellite navigation systems using their Transit prototype to provide navigation fixes once every sixty minutes. This led to the creation of the US Defense Navigation Satellite System (DNSS) and Navstar-GPS programme that provided different levels of support for military and civilian users. In 2000, President Clinton disabled the artificially generated errors in the GPS-Selected Availability signal improving the accuracy from 200 to around 30 meters for civilian users.

First generation GNSS infrastructures did not meet the safety requirements of many potential users. For example, The International Civil Aviation Organization (ICAO) created Required Navigation Performance parameters in terms of:

Accuracy. How correct is the aircraft 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;
Continuity. The probability that an operation once commenced can be completed.

Early GNSS infrastructures suffered from significant limitations across each of these dimensions. Regulators acted to limit their role as a primary source of safety-related navigation data. These concerns can be illustrated by the loss of all GPS signals to a Continental trans-Atlantic flight over New Jersey during December 1997. It was initially believed that the signal interruption was caused by intentional jamming, however, it was later found to be the unintended side effect of a US military test. A 200-kilometer "interference zone" was created by a GPS antenna with a 5-watt signal, stepping through frequencies. These concerns over jamming were exacerbated by the lack of signal authentication in first generation GNSS infrastructures. This makes them vulnerable to spoofing through the broadcast of fake GNSS-like signals or through rebroadcast of valid GNSS signals (Kendall et al, 2007). In addition to the security concerns that limit accuracy, integrity, availability and continuity, GNSS architectures also suffer from a number of known error sources (Köhne and Wößner, 2010):

• Satellite Geometry. In simple terms, higher accuracy is derived from GNSS in which the satellites are widely spread relative to the receiver. If all the satellites are closely grouped together then the benefits of differential signal processing will be reduced. If the satellites are positioned in a line then the plane of intersection of possible positions from their respective signals becomes elongated and the fixes are less accurate. In practice, satellite geometry tends to act as a multiplier for the errors that are induced from other sources.

• Satellite Orbits. A small source of error can be introduced by gravitational forces that create subtle changes in the orbit of the satellites within a GNSS constellation. Corrections can be made to these orbits by analyzing the ephemeris data that is sent by each satellite. Ephemeris data can be thought of as a table giving the coordinates of a 'celestial body' at specific times during a given period. The scale of the error attributable to these effects is typically less than 2 meters.

• 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.

• Atmospheric effects. 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. The resulting delays are well known in standard conditions and can, therefore, be compensated by the receiver. However, most end users do not correct for unforeseen changes such as variations introduced by strong solar winds (Köhne and Wößner, 2010). Different concentrations of water vapour in the troposphere also introduce uncertainty into transmission times to ground based receivers. The uncertainty of these effects means that although they are less significant than ionospheric influences, they cannot be eliminated in any simple computation.

• Clock inaccuracies and rounding errors. Each message exchange helps to synchronize the receiver's clock. However, inaccuracies still leave an error of around 2 meters with an additional 1 meter being due to rounding and calculation problems.

• Relativistic effects. 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. These factors combine to ensure that the receivers' clocks would slow by around 38 milliseconds per day compared to the satellites'. This corresponds to a location error of around 10 km per day. This potential problem is compensated by running the space-based clocks at a frequency that is slightly slower than those in the ground-based components. However, further small relativistic effects stems from the movement of the received on the surface of the earth at up to 500m/s. These are so small as not to be generally compensated in most applications but can be significant for some safety related applications.

3. SAFETY OF LIFE GNSS ARCHITECTURES

These concerns over accuracy, integrity, availability and continuity have not prevented the increasing use of GNSS technology even within safety-related applications. End users often ignore the warnings from suppliers and regulators that these infrastructures should **not** be relied on a primary source of navigation information. In consequence, we have seen a significant number of accidents in which GPS systems have been identified as or contributory causal factors (Johnson, Holloway and Shea, 2008). It is for this reason that satellite based augmentation systems have been developed to specifically support Safety of Life (SoL) applications. These include the North American Wide Area Augmentation System (WAAS) and the Asian Multi-functional Satellite Augmentation System (MSAS). The following paragraphs use the architecture of the European Geostationary Navigation Overlay Service (EGNOS) to illustrate key concepts behind these architectures.

EGNOS uses a network of approximately 40 ground stations and 3 geostationary satellites. The ground stations 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 four master stations that broadcast deviation corrections using the geostationary network. End users then apply these corrections to location information derived from the GPS of GLONASS networks. In particular, it is possible to use this architecture to map out and then compensate for the atmospheric delays described in the previous section. The net effect is to improve the accuracy of the satellite location information from 17-20 meters accuracy in conventional approaches to Global Navigation Satellite Systems to around 2 meters in the augmented approach.

Redundancy supports the reliability of the EGNOS infrastructure. For instance, each of the four master stations rotates from being the Master to a Hot-Back-Up and a Cold-Back-Up. EGNOS provides three different services:

1. **The Open Service** – a free service that offers improved accuracy over conventional GPS applications. It came on-line during the end of 2009.

2. **EGNOS Data Access Server (EDAS).** This is a terrestrial commercial data service that is being tested at present. It disseminates EGNOS data in real time so that it can be integrated into a range of applications, for example to support atmospheric or tectonic research as well supporting the differential GPS professional market.

3. **Safety-of-Life Service (SoL).** The final aspect of EGNOS is intended to support safety-critical industries. Most of the work focuses on demonstrating that the underlying architectures are sufficiently resilient to meet certification requirements. The safety work is largely driven by the Single European Sky/SESAR initiatives within aviation, for example to support approaches with vertical guidance. It is hoped that EGNOS will be certified against the Single European Sky regulations during 2010. In order for this to happen, safety arguments must be made to demonstrate the adequacy of guarantees for message broadcasts and transmission etc. These arguments must convince regulators that the service will be robust against jamming and will be capable of supporting self-diagnostic error detection within seconds.

Augmentation systems, such as EGNOS, provide a stepping stone to third generation GNSS architectures. Rather than extending the existing GPS or GLONASS constellations, future GNSS infrastructures are being deliberately developed to support a wide range of civil, commercial and military SoL applications. There has yet to be a definitive technical description of the integrity mechanisms that support the Galileo infrastructure. However, it is likely that the satellites will broadcast data on the accuracy of error estimations and a guarantee that the error itself is below a threshold value. The SoL user can then assess the risk that the accuracy falls below the threshold and hence can help them to determine whether or not it is 'safe' to rely on Galileo services.

The aim of SoL services is to deliver an alarm when the error for any location solution exceeds a pre-determined limit. This warning must be provided within a particular and with a probability that is greater than the integrity risk. Ideally, the user of any GNSS would like the position error to be less than the alarm limit. However, because the true position cannot be known the position error cannot be calculated. EGNOS and Galileo both derive 'surrogate' values or estimates for these measures. EGNOS uses the external ground stations to augment the satellite signals. Receivers use this data to continuously estimate predicted position errors, known as the Vertical Protection Level (VPL) and the Horizontal Protection Level (HPL), for each position solution. In contrast, the Galileo Ground Segment will monitor the satellite health and upload data for subsequent broadcast to users via the mission uplink stations. Integrity is supported because Galileo Sensor Stations monitor the constellation and broadcast information about the health of the satellites. In contrast to the VPL and HPL, Galileo always calculates a single estimate of integrity risk for a given alert limit. Whenever the derived integrity risk at the alert limit is larger than the allowed integrity risk, the users' equipment raises an alert. In EGNOS, it is assumed that under nominal conditions, the protection levels are guaranteed to over-bound the integrity risk. However, this cannot always be guaranteed. Error sources that are not captured by EGNOS, such as multi-path transmissions, must be accounted for at the receiver. Hence, for aeronautic applications this architecture has been extended to include, Receiver Autonomous Integrity Monitoring (RAIM).

The two approaches raise a range of issues for the end users of GNSS data. In most applications, there is little need to distinguish between vertical and horizontal accuracy. Both components are critical in aviation. However, this is not always the case. In most maritime transport applications the focus is on horizontal rather than vertical accuracy. Further concerns for the end users stem from the lack of independent accuracy measures. In other words, second and third generation GNSS infrastructures rely on error corrections that are themselves calculated from those infrastructures (Pecchioni, Ciollaro and Calamia, 2007). It is for this

reason that considerable care must be taken when developing the safe case arguments that support the use of particular GNSS infrastructures within safety-critical applications.

4. SAFETY CASES IN AIR TRAFFIC MANAGEMENT

GNSS infrastructures are widely used in aviation. Some applications have been informal and ad hoc. For instance, a number of accidents have occurred because General Aviation pilots have relied on mass market GPS devices retrofitted into their cockpits (Johnson, Holloway and Shea, 2008). There are more successful examples. Many accidents continue to involve Controlled Flight into Terrain (CFIT), in spite of the introduction of Minimum Safe Altitude Warning (MSAW) and Terrain Awareness and Warning System (TAWS) applications. The Flight Safety Foundation (2000) has argued that almost 40% of accidents or incidents on approach or landing include elements of CFIT. Boeing (2002) found that around 50% (n=200) of heavy air transport accidents involving hull loss or fatalities over a ten year period involved elements of CFIT. One reason for the prevalence of these accidents is that flight crews must assimilate barometric and radio altitude instruments, the vertical speed indicator, ground proximity warning systems, terrain depiction systems, and navigation information from the flight management computer (FMC) and navigation charts. The difficulty of forming a coherent mental picture of the vertical situation is complicated when there may be uncertainty both about the accuracy of altitude data and also about the presence of surrounding obstacles. In consequence, a number of companies have sought to use GNSS services to support vertical guidance during instrument approach procedures. The interfaces to these applications provide powerful symbology intended to simplify navigation tasks.

GNSS tools cannot be certified as primary navigation tools unless the underlying technological infrastructures meet the ICAO Required Navigation Performance parameters (Vanni, 2008) with the following specific safety targets:

- Integrity risk (probability that an alarm will not be given) = 2 x 10{-7}
- Time to alert = 6 seconds
- Vertical Protected alarm Limit = 20 meters.
- Horizontal Protected alarm Limit = 20 meters.
- Vertical Aircraft Navigation System Error = 7.7 meters.
- Horizontal Aircraft Navigation System Error = 7.7 meters.
- Continuity risk (probability that an operation once commenced cannot be completed) = 8x10{-5}.

The EGNOS development team proceeded with 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. In the Galileo architecture, unexpected values support fault detection and exclusion algorithms. In contrast, EGNOS assumes fault free performance from the GPS/GLONASS constellation in calculating the VPL and HPL measures. 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).

The EGNOS safety case is a key component in the certification of this infrastructure within the European aviation industry. This provides the structure for the technical documentation that demonstrates compliance with both ICAO and the EC Single European Skies requirements. As can be seen from the RAIM example, however, safety concerns about the introduction of GNSS services stretch from the underlying space and ground based segments to receiver-based fault detection through to the integration with end user applications. Figure 1 shows how the EGNOS safety case arguments have been separated into several components:

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.

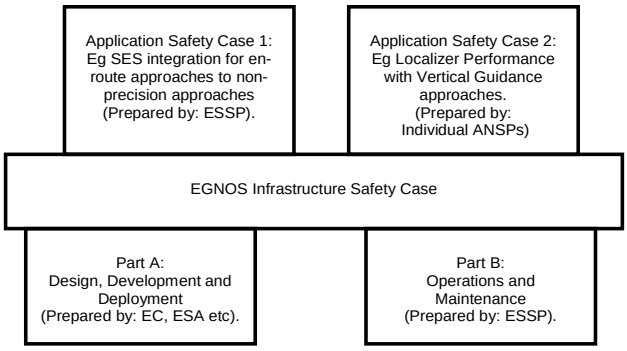

Figure 1: Overview of the EGNOS Safety Case Structure for Air Traffic Management

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 element of the supporting documentation.

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. For instance, ESSP are responsible for developing a safety argument supporting the integration of EGNOS information during en-route operations through to non-precision approaches. The aim of each application safety case is to demonstrate that the target level of safety is met by potential applications. This is done through the argument that the safety of EGNOS applications will be at least equivalent to GPS-based operations that have already been approved.

A further example of application level safety arguments is provided by Localizer Performance with Vertical Guidance (LPV) approaches. These are similar to conventional Instrument Landing Systems with the addition of GNSS receivers. Greater accuracy and reliability enables pilots to descend as low as 200 ft AGL before executing a missed approach (APV-I). LPV systems can be used at airports that have not previous been equipped with ILS technology. Within the EGNOS certification process, it is the responsibility of individual Air Navigation Service Providers to develop the safety cases that justify the use of these technologies within particular approaches. However, EUROCONTROL have developed a generic argument for Approach Procedures with Vertical guidance (APV) using EGNOS that is intended to provide a template for member states. This is illustrated in Figure 2. Individual service providers, shown as ANSP X and ANSP Y, must instantiate the generic safety case for their own operating environment. However, Figure 2 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.

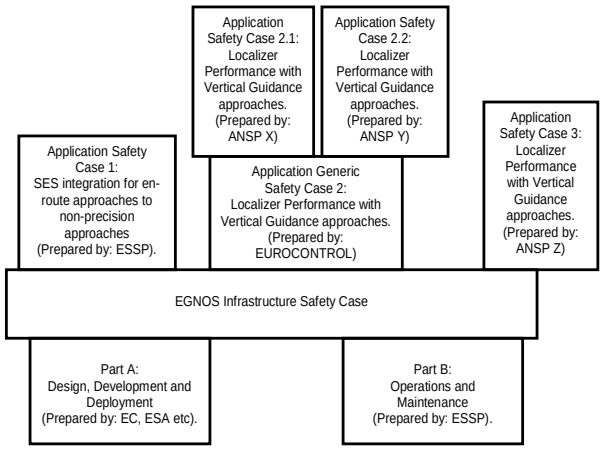

Figure 2: Overview of the EGNOS Safety Case Structure for Air Traffic Management

All of the safety cases mentioned above assume that it is possible to demonstrate EGNOS will meet the targets established for ICAO Required Navigation

Performance. Studies were required to provide the evidence of conformance that supports the underlying arguments in the safety case. 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).

The modular approach in Figure 2 is essential if costs are to be minimised in ensuring that aviation applications based on GNSS are acceptably safe. However, it creates a number of concerns, including but not limited to the following:

Dependencies between Levels? The development of safety cases in a modular approach implies that any underlying weaknesses in 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. If hazards are found in the underlying infrastructures then the architecture illustrated in Figure 2 assumes that those hazards will be adequately addressed in the Part A or Part B arguments. 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 at a higher level.

Consistency within Levels? The modular composition of safety arguments raises concerns about the interdependencies that exist within each level. For instance, if ANSP X found a safety concern then they should immediately inform EUROCONTROL to ensure that the hazard did not stem from an omission in the generic safety case. Alternatively, if the problem stemmed from their interpretation of the template then they should inform ANSP Y to ensure that they too did not misinterpret the common template. This situation becomes more complex in the case of ANSP Z; it is unclear who should be notified of potential problems identified in their safety case? This assumes that service providers are willing to share common safety concerns once they have identified them and corrected them internally.

Modular Safety Cases Limit Shared Understanding? 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 some 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, such as those identified by ICAO. It is also important to stress that the particular approach that is adopted by engineers will have a profound impact on the relationships that must be formed between safety teams and infrastructure providers. For example, in Figure 2 it is clear that ANSP X and Y must have strong interactions with the EUROCONTROL EGNOS teams as they refine their generic safety case. However, they may have considerably less interaction with ESA and ESSP than ANSP Z who has elected not to use the LPV safety case template.

Separation of Ownership and Experience? Application users will gain direct operational experience of common infrastructures. There is a danger that any potential hazards identified in operational use will only inform the safety arguments at the application layer. It is, therefore, critical that some feedback mechanisms are identified to ensure that operational data is also fed back to ESA and ESSP as well as EUROCONTROL. This is particularly important because if any accidents occurred from the integration of EGNOS in Air Traffic Management, it is likely that public and political concern would focus on the general infrastructure and not just the particular application in which it was embedded.

The Reality of Modularity? Experience in the development of safety cases for other ATM systems has shown that the boundaries are never as clear as they might seem in Figures 1 and 2. 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 would undermine safety arguments across all of the components illustrated in these high-level architectures.

5. SAFETY CASES IN SEARCH AND RESCUE

The second case study in this paper focuses on GNSS applications in search and rescue applications, including disaster management. In such situations, there is a pressing need to generate accurate data events in particular locations and times. It is also important to coordinate the distribution of information amongst multiple agencies. During 2006, the Federal Emergency Management Agency (FEMA) and representatives from the New York City administration worked with several commercial US carriers to test a broadcast system for texting warnings about natural disasters, terrorist attacks, chemical explosions, fires and other life-threatening events across a number of US States. This

system was able to send messages to users in particular geographical regions using only a small portion of the bandwidth available for other phone services. The US trial followed the successful implementation of a national cellular emergency broadcast system for South Korea during May 2005. There are, however, a number of limitations that affect the use of cellular systems for disaster management applications. In particular, the networks of base stations and service centres are often damaged in natural disasters, including Tsunamis, or are overwhelmed by public demand in large scale terrorist attacks. The European Space Agency, therefore, developed the ALIVE concept to provide GNSS support during a wide range of emergencies (Ventura-Traveset, Gauthier, Toran, de Lesthievent, and Bedu, 2005). In order to understand some of the benefits of this approach it is important to recall that EGNOS provides the ability to broadcast information to its users. This information is used to provide the corrections to location information that supports the accuracy gains for augmentation based systems. However, this same approach enables the communication of critical information to anyone equipped with a suitable GNSS receiver.

The ALIVE architecture is illustrated in Figure 3. As can be seen, Disaster Management Centres collate information about an adverse event and store them on redundant disaster management servers located in each of the four existing EGNOS Master Control Centres (MCC). This information is used to generate messages that must first be converted into an appropriate format via the EGNOS computing platform (CPF) for transmission by the satellite based augmentation system (SBAS). The information is broadcast using the same satellite infrastructure that provides correction information to location information within the augmentation system. The messages can be associated with particular locations in the same way that corrections reflect local errors detected by the augmentation infrastructure. In this way, regional and national civil protection agencies can target the messages that they send to their population through the disaster management centres indicated in Figure 3. In return, the EGNOS Data Access System can be used by the Disaster Management Centres to verify that the information has been sent with the EGNOS guarantee of service that is built into the architecture using Internet Protocol connections or other conventional communications links.

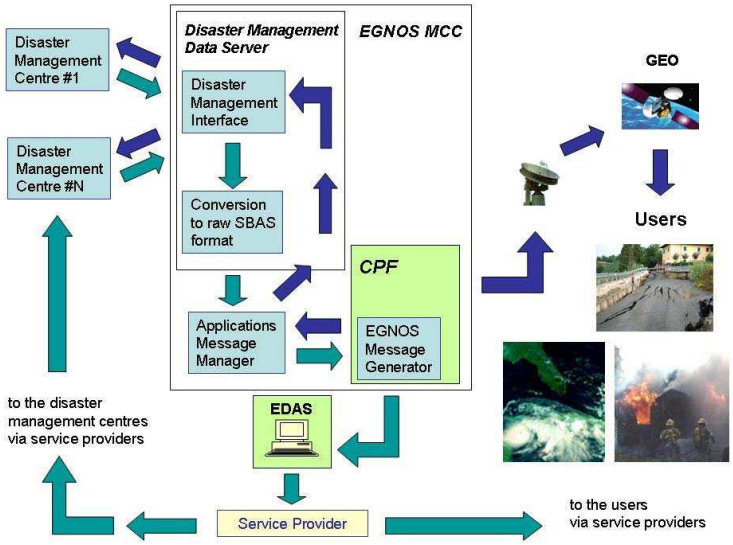

Figure 3: THE ESA ALIVE Architecture (Acknowledgment: Ventura-Traveset et al, 2005)

The applications data managers within the disaster management centres are responsible for defining an ordering over the messages that is passed on to the data server so that critical information can be communicated before less important messages. Once the ordering is defined and the messages have been converted for transmission, they are included in the EGNOS up-link and down-link loop in the same way as other messages. Any user equipped with an EGNOS receiver is made aware of the problem, for example using the same warning techniques that might be used to indicate a loss of integrity for normal location updates.

The general approach developed by the ALIVE architecture, described above, has been applied in recent projects that use EGNOS to support the Corpo Nazionale Soccorso Alpino e Speleologico (CNSAS), the Italian Alpine Rescue Team (Dominici, Defina, and Dovis, 2006). The activities of this Search and Rescue (SaR) team provide a detailed example of the type of tasks that might be supported by wider disaster management services proposed for satellite based augmentation systems. At present, the team spends considerable amounts of time in manually

communicating the position of rescuers to a Control Centre. Each rescuer is equipped with a VHF radio transceiver that can be used to communicate on a reserved frequency. In some cases, they are also equipped with a personal GPS receiver. These are used to augment traditional navigation using map and compass techniques. The VHF reports are then logged on a map. However, this is an error prone process. Individuals may forget to make reports. Verbal slips lead to ambiguity and confusion over precise locations. In the worst case, these problems can lead to a number of hazards. The search team may waste valuable time by searching the same location twice, delaying aid to the individuals and groups in distress; Ambiguity over the locations that have already been search may cause teams to overlook locations where casualties are to be found; Problems in identifying the location of rescuers can increase risks for the SaRs team, especially in poor weather where exposure and hypothermia are likely to occur over prolonged rescue operations; Concerns over the risks to rescuers and anxiety over the location of team members, described in the previous point, can exacerbate a sense of risk aversion in which command teams take premature decisions to bring the SaRs team 'off the hill' in circumstances where they might have continued operations if there was greater certainty in team coordination and location.

Dominici et al (2006) describe EGNOS based SaRs applications that distinguish between User Terminals and Local Elements. The User Terminals are portable devices based around a Personal Digital Assistant (PDA). These use standard GPS receivers to communicate the raw pseudo-ranges back to the Local Element using protocols built on top of the analogue VHF equipment that is proven to work in the mountain environment where there is intermittent cellular coverage. The Local Elements can be thought of as control centres that communicate with the User Terminals over the VHF infrastructure. They log location information in a database that replicates aspects of the paper maps that are used at the moment. In addition, the Local Element can apply EGNOS location corrections to the fixes that are radioed back from each of the User Terminals. The Local Element can obtain these corrections either directly from the satellite infrastructure if they are equipped with a suitable receiver or they can download the corrections over the Internet from the European Space Agency's SISNeT server. Figure 4 provides an overview of the architecture behind the CNSAS system.

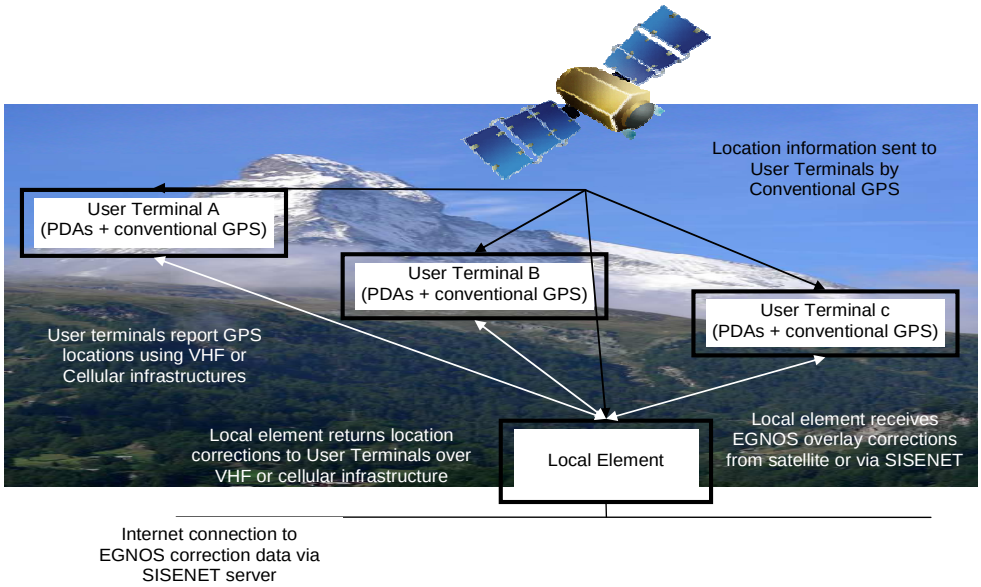

Figure 4: The CNSAS Architecture for SaRs Applications

The Local Element's Internet connection provides access to EGNOS corrections in situations where the User Elements cannot access the EGNOS signal, for instance, when satellites are occluded by the mountain range. The introduction of the EGNOS corrections at the Local Element level allows the rescuers to be equipped with simple mass-market receivers that do not have to receive the EGNOS signal. This meets the critical requirement of limiting system cost but at the same time increasing the accuracy of the location information that could, if necessary be communicated back to the SaRs teams using the UHF links. The power/battery requirements for the User Terminals are reduced since they do not have to acquire the EGNOS signal in mountainous terrain, when there can be significant delays in signal capture.

Once the rescuers' position has been determined it can be displayed using digital mapping software. This provides coordinators with a dynamic view of their personnel as they move across the search area. This graphical view can also show historic data to indicate the trail of the team as they move across the mountains over time. The database can also record information about the time that each member has been engaged in the search as well as the distance that they have travelled to provide high level data to inform risk assessment for the rescue operations. Much of this information can also be transmitted back over the VHF links to the PDA's that run the User Terminal Software. Individual team members can obtain accurate fixes on the other members of their organisation.

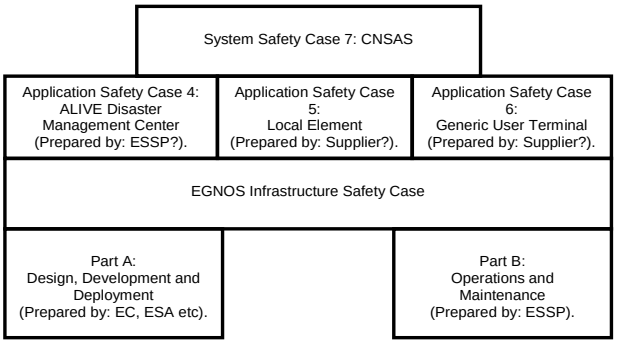

Figure 5: Overview of Possible EGNOS Safety Arguments for CNSAS SaRs Applications

The CNSAS and ALIVE architectures have not been supported by the detailed safety cases that are required within the Single European Skies initiative. Figure 5, therefore, provides an overview of the potential safety case architecture that might support disaster management/SaRs activities in the same way that the EUROCONTROL safety case architecture was illustrated for Air Traffic Management in Figures 2 and 3. As can be seen the Safety Case must consider arguments that both the Local Element and the User Terminal's are acceptably safe. This functional decomposition can then be used to support overall arguments about the CNSAS application as a whole. Figure 5 also opens the opportunity for links between the Local Elements within the SaRs application and the Disaster Management Centres in the ALIVE architecture. However, a number of caveats can be raised.

Who will develop the safety arguments? Previous sections have described how international agencies, including ICAO and the European Commission, have worked together to establish responsibilities for developing the arguments that are intended to support the introduction of SBAS into controlled airspace. ESA, ESSP, EUROCONTROL and individual service providers are all responsible for developing different aspects of the assurance framework that helps to mitigate risks that might arise from the introduction of EGNOS. These responsibilities are far less clear in the domains of Disaster Management or SaRs even though the associated risk exposure is arguably at least as great for those whose lives depend upon these services.

Functional decompositions are appropriate? Figure 5 differs from the ATM safety case architectures because it relies on a functional decomposition of the CNSAS system by distinguishing between local elements and user terminals. Arguments about the safety of interaction are gathered in the system safety case (7). Although the CNSAS safety case architecture does not refer to implementation details, it may be that these distinctions are overly prescriptive. Services may be blurred between these elements – for example when VHF and cellular transmissions are interrupted then user terminals may have to mimic functionality that would otherwise be provided by the local elements. This might imply a more service oriented structuring of the safety cases dealing with location information provision. Such uncertainty reflects the lack of expertise in the development of argumentation to support safety applications of second and third generation GNSS architectures. It also reiterates the importance of sharing experience between application domains such as ATM and Disaster Management.

Can we support information sharing between ATM and other domains? For example, previous sections have described the requirement for Receiver Autonomous Integrity Monitoring (RAIM) within the detailed safety cases for SBAS in Air Traffic Management. However, this need for this functionality has not been considered within disaster management or SaRs applications. This might be a deliberate omission; given that GNSS are likely still to be an adjunct to manual navigation in most of the envisaged rescue scenarios. However, there is a danger that the importance of such integrity techniques has also been overlooked as the infrastructure is being extended from one domain to another. The potential transfer of ideas from the cases in Figure 2 to Figure 5 remains a topic for further work.

Previous sections have explained the powerful guiding influence that aviation applications have had upon second generation GNSS infrastructures. This partly explains the progress that has been made in identifying safety requirements for the integration of location services into Air Traffic Management applications. The questions and caveats about structuring techniques for safety cases in Disaster Management and SaRs applications equally can be argued to illustrate the need

for more sustained work in this area. It seems clear that technological innovation leveraged by EGNOS and similar architectures seems to have outstripped the analysis of safety requirements within some potential application areas.

6. CONCLUSIONS

First generation Global Navigation Satellite Systems (GNSS) have had a profound impact on many different domains ranging from military navigation through to mass-market in-car navigation applications. However, these infrastructures provide few guarantees about the availability of signals, or the accuracy of location predictions or the integrity of the underlying systems. In consequence, satellite based augmentation systems, such as EGNOS, have enhanced first generation architectures such as the GPS and GLONASS constellations to provide additional levels of accuracy, reliability and coverage. These infrastructures are intended to be robust against jamming. They support self-diagnostic error detection and provide end-users with detailed information about the precision and integrity of the services that they provide. In consequence, they are gradually being introduced into Safety of Life (SoL) applications.

This paper argues that greater attention needs to be paid to the safety cases that support the use of novel GNSS architectures. In particular, we have contrasted the investments in the safety analysis of aviation applications with the relative lack of progress in other industries. Such contrasts should not be surprising given that EUROCONTROL and the FAA helped to lead the development of second generation GNSS infrastructures. However, this creates a danger that other domains may rush to use the new SoL services without investing the same levels of care and expertise in the development of associated safety cases.

The closing sections of this paper argue for greater integration between the safety cases that support the use of GNSS services within safety-related applications. In particular, it is important to ensure close cooperation between the infrastructure providers and the developers of SoL systems. It is also important to ensure consistency between organisations developing safety arguments for similar applications in different countries around the globe – for instance, to ensure that everyone considers a similar set of hazards for the use of GNSS data. While international aviation organisations have taken important steps to establish communication mechanisms within their industry, the same cannot be said for most other application domains. There is a danger that technological innovation will outstrip our commitment to mitigate or avoid future hazards. Unless these issues are address then accidents involving the first wave of SoL applications will further jeopardise the development of GNSS infrastructures.

References

Boeing, Vertical Situation Displays, Aero, Number 20, 3-10, October 2002.

F. Dominici, A. Defina, and F. Dovis, An Augmented GPS/EGNOS Localization System for Alpine Rescue Teams Based on a VHF Communication Infrastructure. IEEE PLANS 2006 (Position Location and Navigation Symposium), 25-27 April 2006, San Diego,CA (USA).

European Commission, DG-TREN, Galileo Briefing to ICAO, March 2009. Last accessed April 2010, available on: http://ec.europa.eu/transport/air/international_aviation/european_community_icao/doc/galileo_pres/status_of_egnos_certification.pdf

European Space Agency, EUROCONTROL Clearing the Hurdles for EGNOS, EGNOS News, Volume 8, Issue 1, 2009.
Flight Safety Foundation, ALAR Briefing Note: 7.2 Constant Angle Non-Precision Approaches, FSF Digest, 2000.

M. Hernández-Pajares, J.M. Juan, J. Sanz and S. Soley, ESTB performance under the October 30th 2003 geomagnetic super storm, Journal Space Communications,(20)1-2:7-16, 2005.

E. Herraiz-Monseco, A.M. Garcia, M.M. Merino, P. Romay, A. B. Martin, A New System Level Integrity Concept for Galileo: The Signal In Space Accuracy, Proceedings of the 14th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GPS 2001), Salt Lake City, UT, September 2001, pp. 1304-1316

C.W. Johnson, C. Shea and C.M. Holloway, The Role of Trust and Interaction in GPS Related Accidents: A Human Factors Safety Assessment of the Global Positioning System (GPS). In R.J. Simmons, D.J. Mohan and M. Mullane (eds.), Proceedings of the 26th International Conference on Systems Safety, Vancouver, Canada 2008, International Systems Safety Society, Unionville, VA, USA, 2008.

A. Kendall, A. Vidal, F. Boulette, P. Campagne, B. Panefieu, Say Hello to Galileo's PRS: Making the Case to Security Minded User Communities, Inside GNSS, Autumn, 2007. Available on: http://www.insidegnss.com/auto/igm_050-054.pdf

A. Köhne and M. Wößner, Sources of Error in the GPS System, KOWOMA, Last Accessed February 2010, http://www.kowoma.de/en/gps/errors.htm

J. Oliveira and C. Tiberius LANDING: Added Assistance to Pilots on Small Aircraft Provided by EGNOS. IEEE/ION PLANS 2008 (Position Location and Navigation Symposium), 5-8 May, Monterey, California 2008.

C. Pecchioni, M. Ciollaro and M. Calamia, Combined Galileo and EGNOS Integrity Signal: a multisystem integrity algorithm. In 2nd Workshop on GNSS Signals & Signal Processing - GNSS SIGNALS'2007, European Space Agency, 2007.

P. Vanni, EGNOS Project, Concepts and Operations, ENAV/Italian Flight Safety Association, Italy, November 2008.

J. Ventura-Traveset, L. Gauthier, F. Toran , C. de Lesthievent, J.Y. Bedu, EGNOS Status, Performance and Planned Evolutions (2006-2010), European Navigation Conference 2005 – Munich. European Space Agency 2005.