Developing a Safety Case for
Autonomous Vehicle Operation on an Airport

John Spriggs
Safety Assurance Consultant, Roke Manor Research Limited,
Romsey, SO51 0ZN U.K.

Abstract
This paper discusses the development of a safety case for the operation of an autonomous vehicle near to an airport's runways and taxiways. It describes an approach to constraining such vehicles to operate only in allowed areas, and highlights some of the problems that may be encountered in constructing the safety argument.

Introduction
In my paper given at the Safety-critical Systems Symposium 2002, [SSS 2002] I discussed some hazards that may be encountered on airport runways. In particular, I reported on some research concerning the automatic detection of debris and foreign objects on airport runways, and suggested that an autonomous vehicle could be used as the sensor-carrying platform. You may recall that I said that we could build such a vehicle now, using today's technology, but I was doubtful that we could persuade the Safety Regulator that a vehicle guided by machine vision would keep to its designated areas, and not wander onto runways or taxiways without the appropriate clearances. It would need to be fenced in somehow.

The autonomous vehicle cannot be fenced in literally, as the only things that can currently be installed above ground near runways are aids to aircraft navigation. Rail guidance would encounter similar problems to fences, so buried wire guidance to complement the machine vision had been proposed as a solution.

Subsequent private venture work has identified a potential solution that does not involve the disruption inherent in digging a trench and installing wires. In principle, it uses existing safety-critical radio navigation infrastructure. In practice, that infrastructure is currently installed at very few airports; it can, however, be expected to be widely deployed in future.

The autonomous vehicle does not have to be a debris monitor, it could be a bird scarer, or a grass cutter, but whatever it is, we will need a safety case for its operation on the airport. This paper uses the vehicle as an example in discussing how we could construct a safety case. It highlights the fact that re-use of a safety-critical item in a new system does not mean that preparing the associated part of the safety argument will be trivial.
What is a Safety Case?

A safety case in this context is defined as:

“A document which clearly and comprehensively presents sufficient arguments, evidence and assumptions that system hazards have been identified and controlled for both engineering and operational areas to demonstrate that a facility, facilities or organisation is/are adequately safe in air traffic service respects.” [CAA 1998]

“An argument is a connected series of statements intended to establish a definite proposition.” [Python 1989]

The statements in a safety argument are often referred to as claims. For example a claim may be, “X is safe”, for which the terms “X” and “safe” will have been previously defined. Safety is not absolute, so the definition of “safe” will employ words like “tolerable”, which must also be defined for a particular application by stating a target level of safety or by stating the degree of acceptability of defined classes of risk.

Evidence is information that is presented to establish the point in question; it supports the claim. If a claim asserts A is true, evidence must be available to demonstrate its truth. Evidence can be brought to support a claim directly, e.g. a safety plan could be presented to demonstrate the claim that all safety activities were planned in advance; but this is not sufficient - backing evidence is also required, e.g. configuration control records and audit reports demonstrating that this is the plan that was implemented.

An assumption is a statement that is believed to be, or taken to be, true for the purposes of the argument. For example, “It is assumed that the existing equipment complies with the pertinent Minimum Aviation System Performance Standards”. Evidence should, where possible, be brought to indicate the validity of the assumptions.

The purpose of a safety case is to provide an assurance that any risks that may be introduced by a change to a system or facility have been minimised, as far as is reasonably practicable, before the change is introduced into operational service. The scope of the change may range from the bringing on-line of completely new systems to a minor modification of operating procedures.

Incremental development is very important to fulfilment of this purpose. It is easier to provide assurance to someone who has observed the development of the arguments, than to someone who is suddenly presented with a hundred pages to read. The initial version of the safety case should just present the proposed structure, i.e. the top-level argument, for approval. Subsequent versions would develop the argument further and populate the structure with references out to the supporting evidence. At each stage of development of the item for which the safety case is in preparation, the evidence with which to demonstrate accomplishments should be available and referenced from the safety case. Furthermore, the plans should be in place to collect evidence of accomplishment in the succeeding stages.

How is a Safety Case Presented?

In general a safety case can be a very large document, so we need strategies to break it up into manageable chunks. The first thing to note is that the evidence element of a safety case is often, but not always, material that is also used for other purposes. For example acceptance test results will be used to show that all requirements are fulfilled, not just the safety ones; production test results can be used in the optimisation of manufacturing processes, not just to demonstrate repeatability.

The evidence must be kept elsewhere; not in the safety case document, but referenced therefrom. The whole must be kept under configuration control with all the rest of the system documentation, so that, for example, if a component is no longer available, its replacement is assessed for impact on the safety case before being authorised for use.

Even when keeping the evidence separate you can end up with a large document. You can build a good case like a Victorian novel and convince yourself of its validity because of the process you went through in constructing it. The purpose of a safety case, however, is to convince others, so proof by
construction does not work here, unless you also went though an iterative approval process. The safety case is not intended to be a static object, however. It has to develop as the system it describes develops. A safety case with monolithic structure can be very expensive to maintain.

One method of partition that can be used is often expressed by the composite claim “it is safe now and it will continue to be safe”, i.e. provide a safety case for entry into service, and one to show how the safety features are preserved in operation. Some authorities explicitly require separate safety case volumes like this.

For our vehicle, we could split the case up into two volumes; the first addressing the development of the safety requirements and their fulfilment in the design, the second addressing the hazards arising from the use of the vehicle and how the mitigations are preserved throughout its life. The first volume is clearly the responsibility of the equipment supplier, whilst the second volume will become the responsibility of the Operators at handover, and will require their input during development.

These volumes address functional safety but, as the designer, there are other aspects that I must consider, for example, the hazards to maintenance personnel, their colleagues and their visitors arising from the vehicle. These are “product safety” considerations, and deserve their own volume. Even though the Regulator is unlikely to ask me about them, the Operators will need the assurance and will take over responsibility for this volume also, unless maintenance is contracted out.

Furthermore, I must ensure that the vehicle is safe to build and test. Production test personnel, their colleagues and visitors, may be open to hazards not encountered in normal use or at first line maintenance because, for example, they may be working on a subassembly rather than the whole thing, and they may be using high power simulated signal sources, etc. In practice, I would slip this topic into the safety case as an extreme form of maintenance, but it has to be explicit, so my top-level set of claims, which define the partition into separate volumes, becomes:

- The vehicle is safe to enter service
- The vehicle remains safe in operation
- The vehicle is safe to manufacture and maintain

These claims can be further decomposed using arguments, to support each claim, that in turn depend on sub-claims. We proceed in an iterative manner to populate each volume of the safety case. We need to address many topics in this decomposition, for example, design processes; quality assurance; test strategies; staff competence; the derivation, validation and verification of safety requirements; configuration control; analyses of unwanted interactions, interference and misuse; the need for special operating procedures...

Right at the bottom of the tree we would have claims that cannot usefully be further broken down and just point to supporting evidence, like:

- The Product Safety Review was completed with no actions arising.
- CE Marking Declarations of Conformity were obtained for Machinery, EMC, RTTE and Low Voltage Directives.

It is not enough to have a sensible decomposition, we need also to illustrate the structure so that the reader can understand it and navigate through it. A cunningly crafted contents list could structure the claims; but this only really works for small systems. A picture is much better at conveying a tree structure than a list; but that is not enough either.

**A Safety Case is Not Just What You Have Done**

The Regulatory Authority will want to know why you have chosen this structure; in particular, they want to know why you think that doing it this way is sufficient to fulfil the objectives that they have set. Decisions need to be justified in the safety case; it is not enough to claim:

- The software was developed to Class C of Standard X

You also need to state why that particular standard is thought appropriate and, in the light of that, why you have chosen to address the objectives of Class C, rather than Class B, say. I once asked why a particular standard had been chosen for a project and was told something like “our avionics
colleagues use this for aircraft control systems, so it must be good enough for our train application”. If you have to justify your choice of standards explicitly, i.e. produce an argument to illustrate how the standard is appropriate, you may think about it more deeply than this; you may even come up with something more cost-effective. Similarly, the use of particular tools needs to be justified and evidence brought to show that they have been verified.

“But the standards and tools were chosen at bid time, whereas the safety case is the last deliverable and has to reflect what has been done; it is a fait accompli!” If you are in the unenviable situation of having to bid for a project to develop a safety-related system, with no intermediate feasibility studies, risk reduction exercises, demonstrators, etc., I suggest that you do not produce the safety plan that the Customer has requested in the tender documents. Instead, produce Issue A of the safety case; it serves the same purpose, but includes justification of the plans.

This first iteration of the safety case is all intentions rather than claims – “it will be safe because…” This gives you the opportunity to build the structure of the claims and the arguments, at least at a high level. Most importantly, it allows you the opportunity to provide design constraints, with justification, to the systems engineers who are developing the architecture and draft design specifications.

I am sure you have met project managers who call for safety arguments to demonstrate that what has been done is adequate for the application. They think it your fault if it turns out to be inadequate; and, of course, it is your fault if you were present at the planning stage and did not consider the impact of the decisions on the safety case, and vice versa.

What this digression illustrates is that we need to state justifications, i.e. arguments of why a claim is thought appropriate, as well as the arguments that link the claims to sub-claims. We also need to represent the relationship between all the various elements of a safety case in a clear manner.

I have looked at using the Ward and Mellor Entity Relationship Diagram [Ward 1987] as a means of capturing the structure of a safety case – the aim was to use existing software tools, and also to help build the safety case in a data base format. This work has been overtaken by events; Ward and Mellor have fallen out of fashion in the software world and, more significantly, special purpose tools and notations have now become available, for example the Adelard Safety Case Editor and the Goal Structuring Notation from York University.

Goal Structuring Notation allows construction of complex safety cases whilst making explicit the logical relationships between the claims (Goals) sub-claims (Sub-goals), strategies, rationales, contexts and evidence. This is a very powerful notation because it captures context information and the assumptions made in developing the argument. The capture of this information opens the way for future re-use of parts of the safety argument, it is key to establishing whether an existing argument may be re-used in a new application.

In the simple example of Figure 1 overleaf, which uses a sub-set of the notation, goals and sub-goals are represented by rectangles; the context information is in rectangles with rounded corners; a rhombus is used for strategy; and sources or types of evidence are circles. Of course, a real safety case would further decompose the sub-goals before appealing to the evidence. There are a number of choices for this decomposition, for example the split could be on the basis of particular rôles and functions; or it could be on the basis of personnel, procedures and platforms; or it could even be to maximise re-use of existing safety arguments.
The vehicle can be used on-site

Operational Concept for the vehicle on this site

Base argument on safety of vehicle and location constraint

The vehicle is constrained to stay in designated area

Definition of “designated area”

Designated area definition data are validated for use

The vehicle is safe

Evidence of constraint

Evidence of validation process

Evidence that the vehicle is safe

We will opt for a functional decomposition of the claim “The vehicle is constrained to stay in designated area”, giving sub-claims:

- The vehicle has a definition of the designated area
- The vehicle has a predefined operational strategy
- The vehicle has access to a high-integrity navigation service
- The vehicle uses received navigation data to direct and bound its operations.

The decomposition of the first point would then go into implementation detail, discussing the definition of the boundary of the area in question plus a guard band defined by protection limits. If the vehicle guidance detects that it is approaching a protection limit, it has to react so that factors like momentum and uncertainty in position do not act to push it over the boundary inadvertently.

**Reusing an Existing Safety-critical Item**

Recall that the constraint keeping the vehicle off the runway was to make use of an existing infrastructure item. What we propose to use are the radio navigation signals from a “blind landing” system, i.e. one that is used in the landing of aircraft when there is insufficient visibility for the pilot to do it “manually”. Some would say that there is no issue here; we have a system certificated to land aircraft with hundreds of passengers automatically, so it must be safe enough to mow the grass!

Well, no, it does not work like that.
You could expect that one of the main thrusts of the landing system safety case would be concerned with the continued ability to keep the aircraft tracks coincident with the centre line of the runway (plus or minus a little bit). This is just what we want the grass cutter not to do. I may be able to appeal to the same body of evidence about the infrastructure, but I certainly cannot use the same argument in both cases.

This is the main lesson I want you to take from this paper. Just because you are re-using part of an existing safety-critical system in your new system, it does not mean that the pertinent part of the safety argument will be trivial. We have an advantage in this particular instance, in that we are re-using an established, well-documented, interface – but that does not stop the analysis from being horrendously complex. I will give an overview to illustrate that point.

In fact, the landing systems are so well defined that any safety case is more likely to argue from the viewpoint of compliance with standards, than it is to start from a requirement to stay on the centre line, or the avoidance of obstacles on approach.

Standardisation of Interfaces for Interoperability

The first thing to note is why the interface that we wish to exploit is well documented. It arises from the nature and structure of the industry and its Regulatory environment. A hierarchy of standards, specifications and characteristics has to be in place before the detailed design, development and entry into service of equipment required to implement a new aeronautical service.

By its very nature, aviation operates across national boundaries; aircraft are required to operate globally in a safe and expeditious manner. Furthermore, different companies produce the equipment for the ground-based and airborne segments; and they do this largely independently, based on the requirements of the standards. International agreements are made apportioning safety performance requirements to the subsystems. In particular, Standards and Recommended Practices (SARPS) are developed under the auspices of the International Civil Aviation Organization (ICAO), a United Nations agency.

SARPS normally address essential air-ground interface parameters, e.g. signal strengths in coverage areas, power output, frequency, tolerances, modulations, signal protocols, integrity and continuity of service. The treatment of the ground segment in distributed air-ground systems is usually more comprehensive and detailed than that for the airborne segment. This emphasis is intended to encourage a worldwide uniformity in the provision of services. It also assists countries with less well-developed infrastructure to procure their ground systems with a high degree of confidence as to their appropriateness to provide an adequately safe and expeditious service.

SARPS are developed through specially constituted specialist panels and working groups. Once representative drafts are available from the iterative development process within the working groups, they are submitted to the panel and, if acceptable, onward for worldwide discussion and agreement at ICAO Divisional meetings. They are published, following a written consultative procedure, in annexes to the Convention on International Civil Aviation. This requires the assent of a majority of member states.

Blind landing systems are considered a sub-set of Telecommunications Systems, and are standardised in Volume 1 of Annex 10 to the Convention [ICAO 1996].

For a typical landing system, there are defined three main parameters relating to safety of operation:

**Continuity of Service**
- It has to be operating throughout the period in which you need to use it, i.e. approach and landing

**Integrity**
- It either has to give you correct information, or tell you that it is not correct

**Accuracy**
- It has to give you the information required for a soft landing at the right place on the runway

Continuity of Service is, in effect, reliability of the navigation service and it does not really affect us in this application. Our argument will be based on the principle that, if the service stops, the vehicle will be commanded to stop and so it remains in its permitted operating area. Continuity of Service is, of course, very important for the landing application, as the aircraft is not in a position to stop.
Procedures define a decision height above which they can elect to abort the landing and go around to begin another approach; below that height, they have to land.

Integrity is important to our vehicle; if it is in one place, but the navigation service suggests that it is somewhere else, it could encroach onto forbidden areas. It would not be a sudden change, as that would be readily detectable, but a gradual drift. Accuracy is also important; if the navigation service tells us where we are plus or minus a metre, then we can accept that; if it is plus or minus fifteen metres, we would need such a large guard band around our operating area that, for example, much of the grass would not get cut.

It is not enough to take numbers from the standard and use them in our arguments. To do that would be to make an implicit assumption that the numbers are appropriate for use in this way. We need really to understand what they mean, and justify their application. I originally assumed, for example, that the Integrity requirement would be the same as that I had encountered in my work on Microwave Landing Systems some years ago, but it is not. Integrity is defined for landing systems as:

“That quality which relates to the trust which can be placed in the correctness of the information supplied by the facility”.

The original Instrument Landing System and the more recent Microwave Landing System are defined to have radiation monitors and functions that are arranged to stop transmission if pre-defined thresholds are exceeded.

Integrity is expressed as one minus the probability of transmission of undetected erroneous radiation. That probability is that of concurrent failures in transmitter and monitor resulting in undetected erroneous radiation. It can be calculated from a knowledge of the Mean Times Between Failure of the items and of the proportion of those failures that can cause the emission of spurious guidance.

The original landing systems used only hardware components in the transmission and monitor paths, and so the techniques of traditional Reliability Analysis can be used for these calculations. Some more recent systems have an element of software in the monitoring functions; as there are no recognised techniques for the development of software to the required integrity levels, additional hardware functions have to be incorporated to apply checks on the results provided by the software components.

The system that we wish to use is the Ground Based Augmentation System, which is also known as the Local Area Augmentation System in some parts of the World. It is different from the original landing systems in that the ground segment does not provide the navigation signals per se; there is an additional, space-based, segment that does that. The ground segment acts as a monitor; but in this case, it does more than just compare against thresholds. It provides corrections and other data needed to produce a dependable navigation solution. These additional data include parameters that are to be used by the aircraft to check the integrity of its navigation solution.

This is a real system; installations are planned or already in place at, for example Frankfurt Main, Chicago O’Hare and Memphis International airports. Many others will follow, especially as the original instrument landing systems approach the end of their design life.

To consider the meaning of integrity of the service provided by the Ground Based Augmentation System, we need to know how it works and what can cause erroneous results.

**Satellite Navigation**

The concept of Satellite Navigation using, for example, GPS\(^1\) or GLONASS\(^2\), is well known; what is probably less well known is that such systems are inadequate for use by commercial air traffic. Although the accuracy obtainable may be adequate for en-route navigation, the Integrity and Continuity of Service performance of these systems leaves a bit to be desired. There are, for example, a number of mechanisms for undetected corruption of the navigation solution. These factors would be problems for “blind landing” too, but the dominant problem there is the fact that the systems

---

\(^1\) The Global Positioning System

\(^2\) The Global Navigation Satellite System
are just not sufficiently accurate, especially in the vertical axis. However, before mitigations of these problems can be discussed, we need to know how the satellite navigation systems work.

GPS and GLONASS allow positions on, or near, the Earth to be estimated by using multilateration to a number of orbiting satellites. The distance to each satellite in view is measured by timing how long it takes for a signal transmitted by the satellite to arrive at the receiver. The distance is then the product of the measured period and the speed of light, which is defined to be $2.99792458 \times 10^8$ m.s$^{-1}$.

The theoretical geometry is relatively straightforward. If the distance from one satellite is known, then all that can be deduced is that the receiver lies somewhere on a sphere centred on the satellite with radius approximately twenty thousand kilometres. Two transmitters bring it down to a circle, and three to a pair of points. Four transmitter distances give an unambiguous result; although three could be sufficient, as one of the pair of points would be inappropriate for an aircraft, e.g. outside the atmosphere, or underground.

In practice, however, four distance measurements do not give an unambiguous result. The distance is being measured by timing, but different clocks are being used at either end of the links; consequently, the spheres do not intersect at a point. The receiver clock will not in general have the accuracy and stability of the satellite system, which in GPS depends on an ensemble of two caesium and two rubidium atomic clocks. However, a single receiver makes all the measurements, and so, for first order effects, there is a single value of "clock error" that needs to be added to each of the measurements to achieve intersection.

Once that correction factor has been determined, the receiver can, in principle, apply it to all measurements from then on. In effect, the receiver clock is now synchronised to satellite time, which has a known relationship to Co-ordinated Universal Time (UTC). In practice, the correction process is usually repeated for each set of range measurements taken, to ensure synchronisation is maintained with varying clock error. A receiver does not use the clock correction to actually correct its clock.

The uncorrected range measurements are called "pseudo-ranges" to indicate that they are measurements that contain errors. In order to identify reference points on the signal for timing measurements, pseudo-random code sequences with excellent autocorrelation properties are modulated onto the carrier. Each GPS satellite has its own code and so they can transmit on the same frequency without interfering with each other. GLONASS is the other way around; all the satellites use the same code, but are each allocated a different transmission frequency.
The navigation solution depends on knowing where the transmitters are as well as “when they are”. Data with which to calculate the position of the satellite when the signal was transmitted are contained in messages superimposed on the pseudo-random codes. These messages also contain the time of transmission, plus data for error reduction and availability data for the satellites. The satellite position problem is simplified by the high altitude. They are well clear of the atmosphere, and so have readily predictable orbits. The ephemeris giving satellite position, with a lower precision almanac of all the satellites, is also transmitted.

In summary, the receiver derives its own position from knowledge of the position of a number of satellites from which it receives signals. Furthermore, it is able to derive a correction factor for its clock. What is usually done in practice is to derive correction factors for all dimensions; the receiver maintains an estimate of where, and when, it is, which is updated as each set of measurements is made. A Kalman Filter implementation is almost exclusively used to maintain the estimates.

As the system depends upon taking measurements, there are errors to be taken into account. There are, of course, errors in the receivers themselves, e.g. imprecise phase measurement, but these are reduced by design in high-quality equipment to affect the navigation solution by less than two hundred millimetres. There are much larger errors arising from our assumption about the transmission path.

Sources of Error in the Signal Path

One source of error should be apparent from the previous description; the speed of light is defined as a particular number. That number is derived from the Système International definition of a metre:

“The length of the path travelled by light in vacuum during a time interval of 1/299792458 of a second”.

The definition acknowledges the axiom of special relativity that says that the speed of light is a constant. That is the speed of light in a vacuum; these signals travel through the atmosphere, and so are slower. The ratio by which they are slowed is the refractive index. One would expect the refractive index to increase along the signal path, as one end is in effective vacuum, and the other is near the base of the atmosphere.

Unfortunately, it is not that simple; the upper part of the atmosphere, the Ionosphere, has an effect on signal propagation, due to the presence of charged particles, that varies over time. The Ionosphere is usually reasonably well behaved and stable in the temperate zones; but near the equator or magnetic poles, it can fluctuate considerably. It has a greater effect during the day than at night; there is also a long-term periodic component, apparently correlated with the sunspot cycle.

Some GPS receivers use a model of the Ionosphere, with parameter data provided by the satellites, to derive a correction. Residual errors in the final result tend to be in the region of two to five metres despite this correction.

Military users of GPS have access to another signal transmitted from each satellite on a different frequency. As the ionospheric delay effect is proportional to the frequency of the signal, tracking both signals allows the delay to be calculated and hence compensated for. There are second order effects; residual errors in receivers using the dual frequency technique are of the order of one or two metres.

Lower down in the atmosphere, the Troposphere has different delay characteristics. These are due primarily to the water vapour content, but there are also temperature and pressure effects on both code and carrier. These are not frequency dependent; but it is feasible to compensate for the effect by measuring these parameters and applying them to a tropospheric model to derive a delay estimate. In practice the tropospheric models have been found to be better than those of the Ionosphere, but there may still be errors in the final solution of the order of a metre.

There are error-producing effects in the system that are more esoteric in origin.

Relativistic Effects

One of the consequences arising from the constancy of the speed of light is that a moving clock appears to run slow with respect to a similar clock that is at rest. The GPS satellites travel in their
orbits at such a speed that their clocks appear to run slow by seven microseconds per day, relative to a similar clock on the Earth’s surface.

General Relativity tells us that a clock at a weaker gravitational potential appears to run fast in comparison to one at a stronger potential. This effect makes the satellite clocks appear to be running fast by forty-five microseconds per day. The net effect is thus that the satellite clock is fast, by thirty-eight microseconds per day, with respect to a clock on the ground. This systematic error is compensated for in GPS satellites by a rate offset introduced into the satellite clock before launch. The master oscillator runs at 10\,229\,999\,9543 MHz, which appears to be the required 10\,23 MHz when in orbit.

The orbits are not exactly circular, so the altitude varies over one revolution, as does the speed. The eccentricity of the orbits gives an effect in addition to that compensated for by the fixed rate offset. Data transmitted from the satellite includes additional coefficients to enable the receiver to model, and compensate for, the effect.

There is a third relativistic effect to be taken into account. A clock on the Earth is not in fact fixed; it is in a rotating frame. The receiver undergoes a displacement during the signal propagation period. This phenomenon, called the Sagnac Effect, can also be compensated for in the receiver.

Other Sources of Error

Another error contribution is due to the signals being reflected off objects in the environment and then to the receiver. If the indirect path is not a lot different from the direct one, it produces an uncertainty in the arrival time measurement. If the path lengths are very different, the effect may be reduced by signal processing. It is also possible to improve multi-path effects by choice of antenna location and arranging it to reject signals from low angles, from where most of the reflections come. It is possible, but very rare, to encounter ranging errors up to fifteen metres due to multi-path effects; this may happen in a scenario where a static antenna is mounted near large reflecting surfaces. The effects are much less pronounced in moving receivers, and one can assume that multi-path effects are very much less for an air vehicle than for a ground-based receiver, however they can increase as the aircraft approaches the runway.

Unlike GLONASS, GPS has intentional loss of integrity designed into the system; the signals available to non-military users, until recently, have been intentionally degraded. This was done by dithering the satellite time value and the position data. This feature, Selective Availability, was turned off by Presidential Decree in 2000, but there is no guarantee that it will not be turned back on again in future. If it were, military GPS users could obtain the “correct” values; however, there would still be errors due to satellite clock drift and orbit perturbations.

One nanosecond error in the satellite clock corresponds to about three hundred millimetres error in the range measurement. The atomic clocks on the GPS satellites drift and can easily accumulate errors of this magnitude. The US Department of Defense has facilities that monitor the satellite clocks and compare them with a master clock comprising an ensemble of very accurate clocks including, for example, hydrogen masers. Correction factors are then transmitted up to the satellite for inclusion in its transmissions. The receiver, in principle, subtracts the reported error from the transmit-time value to arrive at its navigation solution. Both civilian and military users are affected by this error, which can offset the solution by one or two metres.

Similarly, the satellite orbits are monitored and the data contained in the messages are updated accordingly. So called Ephemeris Errors result when the message does not contain the correct satellite location. It is typical that the radial component of this error is the smallest: the tangential and cross-track errors may be larger by an order of magnitude. Fortunately, these larger components do not affect ranging accuracy to the same degree. Even so, this error source can still contribute a few metres of error to the navigation solution.

All the errors discussed above have direct effects upon the measurement of the satellite ranges. The effect of the range errors on the navigation solution depends on the geometry of the situation. If only the four satellites discussed above are used, and they are clustered in the same part of the sky, the position error can be tens of metres for one metre of range error. Conversely, if many satellites are
used, and they are distributed across the sky, then the position errors will be only slightly greater than
the range errors.

**Differential Mode of Operation**

As well as compensating for the various identified errors directly, we can take advantage of the
continuity (in the mathematical sense) of the error effects. If two receivers are relatively close, the
ranging errors due to propagation conditions and the uncertainties in satellite position and clock will
be very similar. If the position of one of the receivers is known precisely, it can calculate what pseudo-
ranges it expects for each satellite in view. It can then measure the pseudo-ranges as received and,
by subtraction, derive the magnitude of the errors.

Correction values can then be supplied to the second receiver with which to improve its navigation
solution. This is more flexible than measuring a position and comparing it with the known position, as
it does not constrain the second receiver to use exactly the same set of satellites as the reference to
calculate its position. This also allows the second receiver to be mobile within the coverage area of
the reference receiver. The error magnitudes change quite rapidly due to satellite motion, and clock
drift, so the correction values have to be continuously updated. This is usually achieved via a radio
link between the systems; but where position is required as part of some later analysis, the pseudo-
ranges and corrections may be recorded, locally to where they are measured, for post-processing “off
line”.

Multi-path and internal receiver errors are local to each receiver, and so cannot be compensated for in
this way. Multi-path dominates for a high quality receiver but, as previously noted, it can be reduced
by signal processing and antenna design. For a fixed reference receiver, known sources of multi-path
may be mitigated using stealth-engineering techniques to lessen their effects.

Individual pseudo-ranges must be corrected prior to the formation of a navigation solution. The
reference receiver therefore needs to track all satellites in view and derive individual pseudo-range
corrections for each of them. Similarly, the remote receiver has to be capable of applying the
corrections to each set of satellite measurements used to form its navigation solution.

This is in principle how the Ground Based Augmentation System, illustrated overleaf, works but, as I
keep on saying, it is not that simple. Variants of this system are defined with two, three, or four
carefully surveyed-in reference stations, rather than just the one. These can perform crosschecks on
each other, as well as providing corrections and other data to the aircraft via a VHF datalink. In
common with the original landing systems, there will be a radiation monitor associated with the
datalink transmitter to improve the integrity of the link.

Some implementations, in which continuous view of four or more satellites cannot be guaranteed,
also employ “pseudolites”, which are ground based signal sources that simulate navigation satellites.
The pseudolite provides continuity for the case in which one of only four satellites in view fails during
a landing operation. There are also other signal sources that may be used by an installation. The
Space Based Augmentation Systems intended for en-route navigation employ geostationary
communications satellites in place of the VHF datalink; these satellites also provide navigation
transmissions conforming to the GPS standards.

**Integrity**

Integrity for this navigation service, then, is not just a property of a ground-based transmitter and a
ground based monitor, as in the previous landing systems. For this system, it is an emergent property
of:

- A navigation satellite constellation, with its own ground-based monitoring and control system;
- The ‘signals in space’, with all their tribulations;
- The ground-based monitors with their navigation software;
- The ground-based processors implementing the alerting functions; and
- The VHF datalink, with its own radiation monitors
The supplier of the ground equipment has a problem. The numbers specified as acceptable for the various integrity-related probabilities are very small; it is not feasible to demonstrate that they have been achieved in the timescales of a normal development programme. They have to adopt other strategies, such as appealing to analysis and simulation. Their safety case has to justify and develop these strategies and provide evidence to validate the simulation results, etc. Furthermore, not only is the integrity calculation more complex than for the original landing systems but also, because of the need to employ software for the Kalman Filters, etc., traditional reliability prediction techniques cannot be directly applied in its verification.

Fortunately, as a user of the service, we can regard this work to have been done. We will state an assumption in our safety case that the evidence seen by the Regulatory Authority, when accepting the landing system for service, was enough to convince them that the safety performance against the pertinent parameters had been adequately demonstrated. Our safety case is thus dependent upon that of another supplier who, in general, will not be willing to show it to us. That is another reason why we cannot re-use parts of the argument in our safety case, and why we need the Regulator to maintain the "web of trust".
For critical infrastructure items, we should not be able to view the safety case even if the supplier had no objections. These security critical documents highlight vulnerabilities in the infrastructure and should remain confidential.

**Elaboration of the Integrity Sub-claim**

Having seen the Ground Based Augmentation System description, we are now in a position to detail the sub-claim stated as:

- The vehicle has access to a high-integrity navigation service

A candidate structure in Goal Structuring Notation is presented for this sub-claim in Figure 4 below. Although use of acronyms in safety cases should be deprecated, the acronym for Ground Based Augmentation System has been used in Figure 4 to reduce the size of the text boxes.

---

**Figure 4 ~ A Breakdown of the High-integrity Sub-claim of Figure 1**

The new sub-claims assert that the vehicle has the means to receive and use the navigation service and that it is constrained to operate within the local area in which the service is available. The certification of the system will apply over a particular volume but it is, of course, concentrated on
aircraft operations. There may be areas on the airport in which we require to operate the vehicle but
to which aircraft would, or could, not go. An airport may be perceived as a wide open flat area, but
there can be some very large buildings producing the same “urban canyon” effects that cause
problems with conventional GPS receivers in cities. Hence the need for signal surveys.

Note that, in Figure 4, the term “designated airport” has been used; this is part of a generic safety
case for the vehicle, not for a particular instance. The signal survey evidence will be plans, including
methods, for the particular type of survey. We have a software tool for predicting the urban canyon
effect, so simple surveys would be used to verify the predictions, rather than having to do a complex
series of measurements.

One of the sub-claims refers to the integrity data; these data were glossed over in the preceding
description. It is not only pseudo-range corrections that are received via the VHF datalink, there are,
inter alia, additional statistical parameters that can be used, by the receiver, to judge the quality of the
signals prior to use and invalidate the guidance data output if necessary.

Conclusions

A safety case should be built and reviewed incrementally to facilitate approval. It also needs to be
presented in such a manner that, in addition to giving confidence to the Regulatory Authority that what
has been done is sufficient, it can:

- Give confidence to the organisation producing it that what they have done is necessary;
- Make it straightforward to assess the impact of future proposed changes to the subject
  system;
- Be easy to maintain; and
- Be used as the basis for future safety arguments in the domain

When budgeting for the safety case development activity, we must not underestimate the amount of
work involved in re-using existing items. Those items that are “owned” by the designer, and already
have arguments developed and represented in a way that preserves context and assumptions, can be
straightforward to assimilate.

However, as illustrated in this paper, incorporation of items that are owned elsewhere, or are to be
used in a different context, can involve a lot of effort. We were fortunate in this case that we were
tapping in to a very well defined interface. It is also a very public interface in that the International Civil
Aviation Organization has published its description. This description has been open to scrutiny by
many experts from around the World, and has been made more robust as a result of their work.

Outlining a safety argument in terms of intentions at bid time will help to identify where in-depth
analyses will be required, and hence will lead to a more robust estimate of the costs involved in safety
case development.

References

[CAA 1998] Civil Aviation Authority: CAP 670: Air Traffic Services Safety Requirements, CAA London,
1998, plus amendments.

~ Aeronautical Telecommunications; Annex 10 to the Convention on International Civil Aviation, Volume 1: Radio

2 of Monty Python’s Flying Circus ~ Just the Words, Methuen 1989.

[SSS 2002] Spriggs J: Airport Risk Assessment ~ Examples, Models and Mitigations, in Redmill F, and
Anderson T: Components of System Safety, Proceedings of the Tenth Safety-critical Systems Symposium,
Springer-Verlag, 2002.