Practical Implementation of Satellite Navigation Safety Assessment

Jean Pierre Magny

This, and the following three papers, were first presented at GNSS 2000, the Third European Symposium on Global Navigation Satellite Systems held in Edinburgh, Scotland from 1st to 4th May 2000.

This paper presents the methodology and a practical implementation approach to perform GNSS Safety Assessment and Certification with due consideration of the satellite navigation system users. It places Galileo GNSS in a total system that includes vehicles, on-board equipment, crews and traffic controllers and defines the necessary organisation for implementing safety analyses right from the early design phases of navigation systems. Civil aviation has very demanding requirements based on objectives for air navigation safety. It is much better organised on a worldwide basis than other GNSS users and is considered in this paper as the leading study case. Some methods are then proposed to build a bridge between all user organisations and to set up a common approach to certification.

KEY WORDS

1. GNSS. 2. Safety. 3. Design.

1. BACKGROUND. Safety refers to the probability of accidents, death and injuries. Safety of a navigation system refers to the probability of accidents related to the use of the navigation system. Evaluation of the safety-critical aspects of GNSS anomalies must be a mandatory process throughout system design and operational use. The effect at the user/vehicle level requires consideration of the vehicle equipment, the environment, crew procedures and skills, training and traffic control interactions. For Galileo GNSS, a rigorous *risk management* process must be organised within the overall engineering effort to provide the optimisation of each sub-system to the benefit of the whole.

The main problem is the difficulty of setting up an organisation linking several communities with different cultures and long-established procedures. They will have to work together with commonly agreed rules and methods throughout the life cycle of Galileo.

Within the well-structured civil aviation community, linking Air Traffic Control with aircraft designers, crew and satellite systems providers is already a challenge. Beyond that, a global agreement between all possible users' communities for Galileo becomes a necessity with the ambitious objective to set up a common safety assessment and certification process.

2. THE TOTAL SYSTEM CONCEPT. The key issue is to design and build a Global Satellite Navigation System and demonstrate that it is safe for all applications and that it remains safe throughout its life cycle. For aviation, this means that no navigation-related event more probable than 10^{-7} per flight, will lead aircraft

to hit defined protection limits. Collision Risk Models define a protection limit, or a protection surface, with consideration of the risks of collision with the ground or between aircraft. The hazardous nature of a navigation failure depends on the aircraft or vehicle navigation system and procedures; many failures are transparent, and others may be misleading but deadly. For example: one satellite may cease to broadcast; depending on the remaining performance and geometry of the others, the vehicle's receiver may still be capable of providing a full service. By contrast, a satellite may continue to broadcast but anomalies such as interference may mislead the receiver and cause it to produce erroneous navigation information. The consequence of such errors depends on the vehicle systems, its failure detection capability, integrity monitoring, smoothing capability (for example, augmentation with an Inertial Navigation System (INS)), the phase of flight and crew reaction. A satellite navigation system may suffer a general system breakdown or encounter complete jamming in a limited area. Operational and safety consequences will be limited if an INS or a terrain reconnaissance system or any other means of navigation back-up is available in the aircraft, particularly if the crew is trained to react immediately to well identified difficulties of this type.

Complex interactions must be part of the analysis of the total system including the GNSS, its control segment, the signal-in-space, Air Traffic Control, the aircraft and on-board equipment, crew and procedures. Responsibility for the various sub-systems and elements belong to different communities not (yet) linked by a specific organisation or institutional link. These links have to be created with consideration of global system methodology and organisation. The *total system concept*, and associated total system engineering effort, must be flexible enough to sort out these interactions and safety issues between sub-systems and elements and between the organisations involved.

Optimisation of any element to the benefit of the whole concerns basic engineering and safety. For example, some safety issues may be easier to solve by user equipment modifications or crew procedure amendments than by satellite design changes. This requires engineering procedures and organisational methods that are capable of co-ordinating the navigation architecture.

Programme constraints have also to be considered. It is clear that performing a safety assessment just before Galileo is ready for operational use will reveal problems that may take too much time to correct and so cause delay in system deployment and could be very costly. Therefore a continuous programme for safety analysis and risk reduction must be set up as early as possible in the design.

3. ENGINEERING METHODS AND TOOLS FOR SAFETY ANALYSIS AND RISK REDUCTION DURING SYSTEMS DESIGN.

3.1. *End-to-end process.* Failures of a GNSS, affecting the signal-in-space (SIS), may propagate through the receiver to the navigation solutions of the aircraft and so affect the aircraft flight path. The first engineering task should be to perform a Failure Modes and Effects Analysis (FMEA) at the SIS level. It is then possible to assess:

(a) the possible effect of SIS anomalies on the receiver,
(b) the possible effect on aircraft systems,
(c) the possible effect on aircraft position,
(d) the possible effect on information provided to ATC,

(e) the criticality of anomalies with consideration of vehicle systems, the procedures for various phases of flight and the Air Traffic Systems configuration.

This analysis linking SIS anomalies with aircraft position and its possible operational effect is one of the basic methods for safety evaluations and risk reduction action during development. It has the aim of achieving as low a risk level as is reasonably achievable and at least better than the ICAO TLS (Targeted Level of Safety). The analysis may reveal that it is cheaper and safer to solve some integrity events with on board augmentation (such as INS) rather than increasing the complexity of the GNSS. Safety evaluations and certification constraints can thus drive design and management decisions.

The above process should run several times during development of Galileo GNSS and be fully traceable in the corresponding 'Design Justification File' as the corner stone for technical certification. The last iteration provides the necessary elements to establish a protection surface for various phases of flight. In this logic, vehicle systems with lower performance will end up with a wider protection surface leading to higher minima that will reduce the operational benefit but still satisfy the required level of safety. Without such rigorous analysis and evaluation, there may be unknown and possibly misleading and dangerous behaviour that could lead to situations of high risk, unless margins have been taken for such ignorance.

Demonstration at a high confidence level that a system is free of low probability failures (integrity anomalies $< 1{\cdot}10^{-8}$/h) cannot be done by tests. Specific engineering methods and validation techniques must be applied. The aircraft and nuclear power industries are experienced in designing and certifying their products with even more severe requirements. Their practices must be adapted to Galileo GNSS in order to build a redundant and fault-tolerant system, to analyse any possible accumulation of failures corresponding to the probability imposed by requirements, to refine the design by eliminating hazardous failures and – at the end – to demonstrate the robustness of the design to failures.

3.2. *Implementation example for Instrument Approach and Landing*. Precision Approach is probably the design driver that requires specific attention. The designers of Galileo GNSS must provide a complete identification of all events (failures, anomalies and external phenomena) that could affect the SIS. The designers of receiver equipment must provide a rigorous effect analysis of the above-mentioned events on the receiver and co-ordinate with the designer of the aircraft systems to analyse any failure propagation from the receiver to the various aircraft elements: FMS, pilot displays etc. They must also evaluate the subsequent pilot and autopilot reactions in flight simulators. Different aircraft configurations will need to be considered. Each one can lead to a specific error profile corresponding to specific operational minima. For instance, an aircraft with an INS that improves continuity and integrity could be authorised for approaches in lower visibility.

Adverse conditions such as severe wind gradients, marginal visibility and other on-board failures will need to be simulated. At Decision Height (DH), tests must also evaluate the feasibility and safety of the transition from instrument to visual flight to ensure a safe landing. As stated earlier, it is essential to perform this kind of analysis and simulation right from the early development phase to support key architecture/design trade-offs and decision making. Of course, simulations have practical limits.

Flight tests are necessary to validate simulation models and to raise confidence as early as possible and certainly before the final Galileo SIS is available. Flight tests could be started soon using computed navigation system errors resulting from architecture studies and reproduced in test aircraft installations, and by further experiments using existing SIS such as EGNOS.

Once the Galileo GNSS design has been reasonably refined, the remaining profile of acceptable Navigation System Errors (NSE) will permit evaluation of Flight Technical Error (FTE) and Total System Error (TSE) and so provide data for establishing collision Risk Models for precision instrument approaches.

3.3. *Programmatic aspects*. The *total system* engineering loop from Galileo GNSS design to operational use on aircraft, as described above, has to be run several times in all design phases. Design tools and simulators will need to be progressively updated to take care of design progress before completion of real flight tests. Early flight tests can bring additional benefits such as training the various communities involved in the *total system concept* to work together on practical matters and to better prepare for the certification phase.

Flight tests will include navigation data stored in an aircraft database and so provide their contribution to a database integrity assessment. It is recommended that all procedures and associated data should be flight-tested before publication. Again experience shows that only end-to-end testing is capable of detecting data errors or interface, compatibility or integration anomalies. Flight testing will certainly have to be performed during the operational phase for timely assessment of instrument approaches in their environment (calibration like flights) and for validating new or modified procedures.

4. ORGANISATIONAL STRUCTURE. To ensure success, several institutions, communities and organisations (designers and users) belonging to several cultures and outlooks must work together. This applies to the Galileo GNSS designers, the avionics and aircraft industry, pilots and air traffic controllers. Real-time, inter-active cooperation and engineering could enable delivery of fault-free systems right from the beginning of operations. However, the user communities are not all organised to perform engineering studies of their traffic system and user applications. They may not be ready to ensure the engineering interface with GNSS studies so forcing Galileo designers to use default data or assumptions. Cooperation is a very challenging goal in terms of organisation, multi-cultural communication and technical effort. The fundamental issues are:

(a) to create an organisation that has to work in real time and is acceptable to all communities,
(b) to ensure the organisation has the will and decision-making authority when apportioning risk reduction effort between the various elements.

4.1. *Minimum required structure*. Three upper layers would appear to be necessary. The first two will deal with the *total system concept*. The 'top institutional layer', beyond its funding role, has the main mission to link together national and international bodies, regulation units, operators and to arbitrate between sub-systems and communities. In Europe, the European Commission takes this position and ensures the coherence between other European and International bodies such as ICAO and IMO. The 'industrial architecture layer' has the main mission to control

and optimise the engineering effort at industry level between the GNSS SIS, receivers, aircraft and on board equipment, Air Traffic Control, crew and procedures. It must determine all necessary trade-offs with regard to users, co-ordinating requirement allocation, development and validations. The 'sub-systems layer' is where industrial partners, closely linked to the 'industrial architecture layer', will develop Galileo GNSS, user receivers, on-board equipment as specified by the *total system concept* studies.

4.2. *Skills and resources*. Both the 'top institutional layer' and the 'industrial architecture layer' have the difficult task of making the cultural link between all parties and rigorously co-ordinating the *total system concept* engineering effort. This requires enough background in all the cultures and user communities to have the credibility and capability to arbitrate and to convince. This goes well beyond the mere capacity to set up and to control such a complex organisation.

4.3. *Methods*. Systems engineering and safety management methodology are the necessary basis for success, but dealing with so complex an environment requires many other methods, resources and skills that would require development beyond this paper. In particular, it would be a miracle if such a difficult organisation worked from the beginning; there will need to be a built-in 'learning and adaptive process' with a view to learn from any problem and to correct. This paragraph does not pretend to give a precise recipe for success but simply to highlight the need for this unusual category of organisation with responsibility for co-ordinating institutions and industrial partners. This huge 'orchestra' will require outstanding 'conductors'.

5. INTERNATIONAL STANDARDS FOR CERTIFICATION.

Safety assessment is the main technical issue for certification. Legal recognition by institutional bodies can be a purely administrative matter if the 'technical findings' are sorted out. The credibility of a new navigation system, such as Galileo GNSS, depends on the manner in which safety assessment is performed. The level of safety is an integral part of the system's performance and is clearly an interoperability matter. Significant progress has been made over the past two years within GNSS-P and RTCA in defining satellite SIS failure modes with the view to making integrity monitoring resistant to these failures. It is now possible to generate design requirements and test cases for demonstrating the robustness of GNSS integrity.

However, this first step is not sufficient. The global nature of a GNSS is such that practical safety evaluation rules cannot be left to National Authorities, as they are for ILS or VOR, where liability is local. It is therefore recommended that safety evaluation methods be defined by additional ICAO standards and recommended practices (SARPS) to make evaluations and results comparable from one GNSS to another.

6. FROM AIR NAVIGATION TO THE OTHER GNSS USERS.

Identification of differences and commonalties in culture, engineering and standards has already started. Most differences are due to the different vocabulary and definitions used, and the wide variety of requirements in the very large number of applications. For example, it is clear that using GNSS will not prevent a car driver staying on the road visually or avoiding collision with other vehicles. Therefore, integrity and continuity of service – as defined by ICAO – may have less interest for road applications but may look meaningful for maritime users when navigating in the

fog. A common core of performance requirements, of engineering and certification justifications can be defined for all users and can be complemented by special requirements for specific applications, ending up with a 'modular structure of requirements' associated with a sub-part called 'modular safety and certification requirements'. This would avoid duplication of certification work but requires initial analysis and harmonisation, and some communities may take time to set up an organisation capable of responding. The effort goes much beyond defining the core performance requirements; it is touching safety culture and safety demonstration methodology and has to be performed with respect to project planning that calls for requirements to be available in the early design phase. This is another challenge for the two top layers in the organisational structure that will most probably have to rely on a specific task force of experts capable of supporting the required analysis with the various user communities.

7. CONCLUSION. Galileo GNSS certification must be based on safety demonstrations that require a specific organisation involving designers and users from various communities. This paper has presented the *total system concept* that creates the framework for organisation, resources allocations, methods and standards. Its main objective was to draw attention to the required multi-cultural, safety, system engineering competencies and schedule constraints. Only the visible part of the 'iceberg' has been presented.