Nationaal Lucht- en Ruimtevaartlaboratorium
National Aerospace Laboratory NLR

NLR-TP-2003-378

Consistent safety objectives and COTS versus fragmented certification practices and good safety records

Air transport dilemma in need of innovation

E. Kesseler

This report is based on a presentation at the 3rd IEEE Conference on Standardization and Innovation in Information Technology SIIT 2003, Delft, The Netherlands, 22-24 October 2003.

This report may be cited on condition that full credit is given to NLR and the authors.

Customer:	National Aerospace Laboratory NLR
Working Plan number:	I.1.D.2
Owner:	National Aerospace Laboratory NLR
Division:	Information and Communication Technology
Distribution:	Unlimited
Classification title:	Unclassified
	August 2003

Approved by author: 5/8/2003	Approved by project manager: 20030805	Approved by project managing department: 5/8/2003

Abstract

Air transport has evolved into a safe infrastructure due to a comprehensive set of safety standards covering all relevant aspects of flying. However, each standard has evolved independently and imposes specific, historically motivated, requirements that are not necessarily compatible.

New challenges arise, such as punctuality and cost consciousness. General information technology trends, such as COTS and network-centric solutions, offer new opportunities to improve responsiveness and reduce time-to-market.

The applicable air transport software safety standards for a specific integrated system are discussed. A comparison is made with software safety standards from the process, nuclear and medical industry, focussing on lessons-learned.

The air transport case illustrates the need for and an opportunity to innovate software safety standardisation and certification and provides guidance for such standard innovation.

Contents

(24 pages in total)

1 Introduction

A century after the first powered flight, air transport has evolved into a safe infrastructure connecting all places around the globe. Air transport safety standards have evolved into a comprehensive set, covering all relevant aspects of flying. Incident and accident investigations focussing on lessons learnt instead of apportioning blame contribute to a self-improving safety system. The impressive air transport safety record testifies to the success of this approach. However, each standard has evolved independently and imposes specific, historically motivated, requirements, which are not necessarily compatible.

The transformation of air transport from a privilege of the few into a mass-market commodity imposes new challenges such as punctuality and cost consciousness while at the same time reinforcing the need for continuous safety improvements. General Information Technology (IT) trends such as deploying Commercial-off-the-shelf (COTS) components and network enabling of existing systems offer new opportunities to improve responsiveness, reduce time-to-market for new passenger services such as in-flight e-mail, and to improve the quality of passenger service by seamless airport check-in procedures, etc.

The nature of air transport implies that the supporting services have to be world-wide interoperable i.e. need to be standardised. The resulting global competition requires a uniform interpretation of these standards and resulting certificates to prevent safety degradation from occurring in specific nations, the unwanted equivalent of cheap flag countries for ships.

Chapter one provides some background on the integrated air transport system. This integrated system, also referenced as a system-of-systems, illustrates the various applicable air transport software safety standards that are discussed in the subsequent chapter. In order to learn from other domains, an overview from the safety standards of the process, nuclear and medical industry is provided in the next chapter. Differing approaches or incompatible requirements of these standards, which aim for similar safety objectives, will be highlighted, resulting in a number of recommendations for software safety standards. For COTS to be viable, a safety product needs to be allowed to operate in these differing domains without undue additional certification effort per domain, i.e. the common safety objectives should result in mutually recognised standards and certificates.

Recently heightened security concerns provide an opportunity to apply a security standard to the same integrated system. A dedicated chapter describes this standard’s approach, providing further material for the conclusions in the closing chapter.

2 Air transport case description

2.1 Current practise

Currently the various aircraft systems are highly integrated to optimise the aircraft flight within the applicable safety limits. However, as aircraft are not connected to ground-based air traffic management systems, other then via an old-fashioned voice link between pilot and air traffic controller, this optimisation does not take into account the other traffic.

The justification of Air Traffic Management (ATM) is to prevent collisions between aircraft. Aircraft operate in conditions (e.g. flying through clouds) where the pilots can not do this themselves. Traditionally air traffic management is a national responsibility, where use of civil airspace and airports is optimised to achieve maximum traffic flow within national constraints like military airspace.

As in any safety-related industry, both aircraft and air traffic management systems tend to have a conservative approach to innovation. These systems are custom made for a very small market, compared to the general domain, resulting in comparatively low investment and a correspondingly low innovation rate. Strict domain-specific safety rules prevent the use of Commercial off-the-Shelf (COTS) software, reducing the innovation rate even further.

Currently the design of a new aircraft, like the Airbus A380, or the Joint Strike Fighter, is a major effort that takes well over a decade from initial idea to a flying and certified product. Even on the ground, Air Traffic Management systems take a similar time to produce and get operational.

Airlines fly aircraft within the limits set by the aircraft and the airspace, optimising for commercial profit. As a result their automated support systems posses yet other information and optimise for different objectives.

National authorities are responsible for the environment by limiting noise, emissions, third party risk etc. This is yet another perspective, yielding different information and information systems.

2.2 New concepts

In busy airspace the current way of working is approaching its limits, resulting in safe but uneconomical flight execution with delays on the ground and in the air. To improve this situation in the COOPATS (Co-operative Air Traffic Services) concept [EUROCONTROL, 2000] concept has been conceived. Co-operative Air Traffic Services combine global satellite based position services with global satellite based communication services and terrestrial air traffic management. COOPATS's high-level objective is to support air traffic controllers, pilots, and all potential ATM users, in all phases of flight by progressively implementing fully seamless communication, data exchange and automation capabilities. The key principle is improved situational awareness for both pilot and controller, enabled by intelligent systems. Figure 1 provides an overview of the proposed services per flight phase.

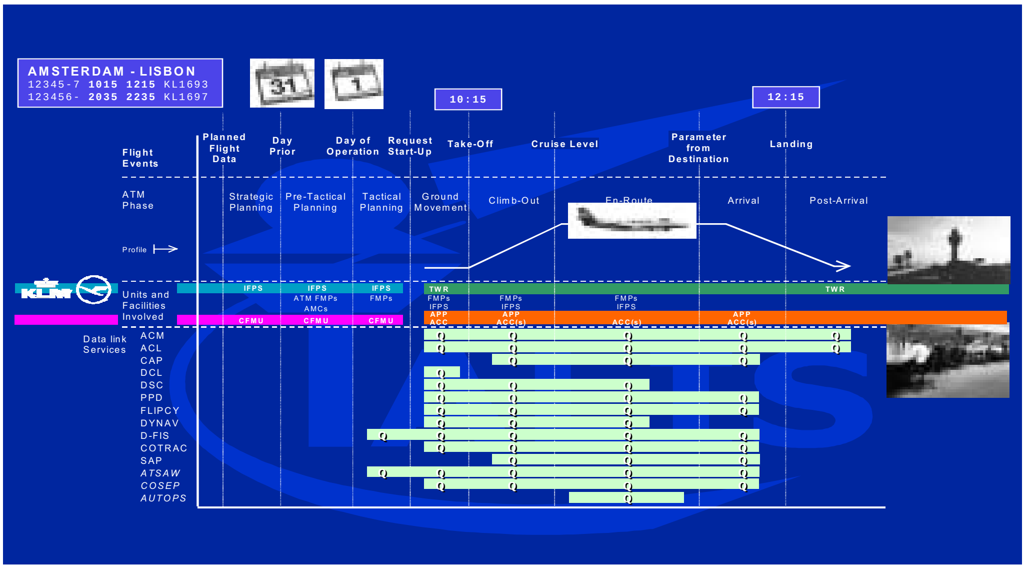

Figure 1: Co-operative Air Traffic Services concept

2.3 Service example

In order to illustrate the kind of optimisation that the Co-operative Air Traffic Services concept aims to support, the pilot-oriented sample service of figure 2 is described.

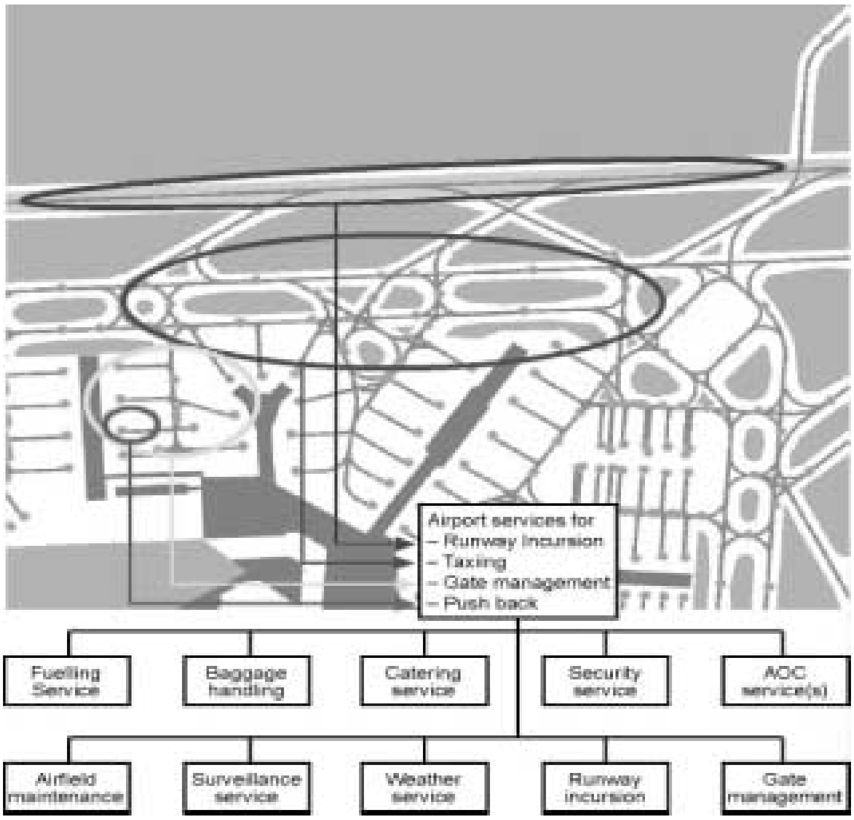

Figure 2 Pilot-oriented sample service

At an airport the pilot information-needs are time dependent. A co-ordinated pushback service will allow the pilot to improve the reliability of on-time pushback. The pilot needs amalgamated information from, e.g., fuelling services, baggage-handling services, catering services, security services, gate personnel and Airline Operations Centre (AOC) about transfer passengers. This pushback service optimises utilisation of the taxi-way linking the various gates and prevents aircraft from blocking each other or ending up in the wrong take-off order. Subsequently taxi-services guide the aircraft to the correct runway, optimised for the other airfield traffic, its departure timeslot and taking possibly adverse weather or airfield maintenance restrictions into account. Finally, runway incursion services, using surveillance services, improve the safety during take-off.

2.4 TALIS solution

The TALIS (Total Information Sharing for Pilot Situational Awareness Enhanced by Intelligent Systems) project provides a supporting architecture for the Co-operative Air Traffic Services concept and its innovative services. Furthermore the TALIS architecture should integrate the existing systems of yet other actors like the authorities. The authorities are responsible to determine capacity, regulate and monitor collision risk, noise, emissions and third party risk. The TALIS architecture provides the middleware to integrate the existing systems. By combining the strengths of the individually provided services the time-to-market for new services can be reduced significantly and competitiveness can be increased resulting in better service at lower costs. Figure 3 provides an overview of the TALIS architecture. [Kesseler, 2003] contains more information on TALIS.

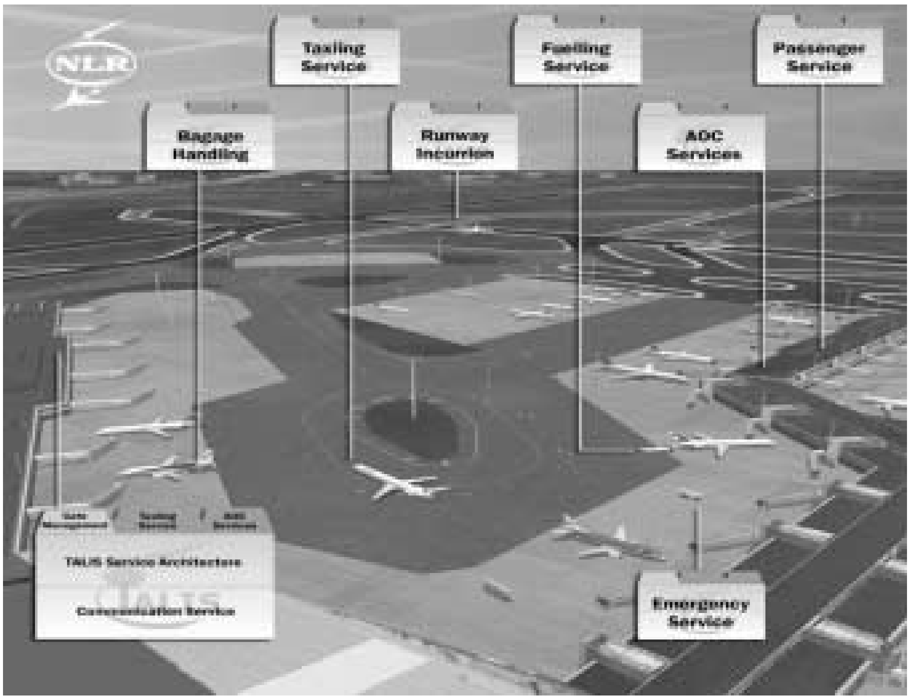

Figure 3: TALIS architecture

For the various systems and services depicted in figure 3 different safety standards apply, which are discussed in the next chapter. Some [Jensen, 2003] even state that modernising the ATM infrastructure would be relatively easy. The certification process poses the major problem.

3 Air transport safety standards

All discussed standards share the notion that software has to be classified according to the system hazards (loss of life, aircraft damage) the software failure would cause or contribute to. This information is obtained from the Functional Hazard Analysis (FHA) plus the (Preliminary) System Safety Assessment (P)SSA. Based on this information, the software will be classified. For each software class a number of standard specific requirements have to be satisfied. Usually, an independent authority checks compliance with the requirements and approves complying products as fit for use. This paper will concentrate on the software part.

3.1 Airborne software safety standard DO-178B/ED12

For all software in an aircraft [DO-178B, 1992] applies. As one of the oldest software safety standards it influenced other software safety standards. Based on the system level FAR/JAR AC-25-1309 the following five software levels are defined by DO-178B. For convenience in Table 1 the quantified FAR/JAR failure-probability definition is included.

Level	**System failure**	**Failure description**	**Probability description**	**FAR/JAR definition per flight hour**
A	Catastrophic failure	Aircraft loss and/or fatalities	Extremely improbable	.. < 10^{-9}
B	Hazardous / Severe major	Flight crew can not perform their tasks Serious or fatal injuries to some occupants	Extremely remote	10^{-9} < .. < 10^{-7}
C	Major failure	Workload impairs flight crew efficiency Occupant discomfort including injuries	Remote	10^{-7} < .. < 10^{-5}
D	Minor failure	Workload within flight crew capabilities Some inconvenience to occupants	Probable	10^{-5} < ..
E	No effect	No effect	Not applicable	-

Table 1: DO178B/ED12 overview

Detailed requirements are provided for each level. As it is not possible to measure actual failure rates at the required low rates, strict process guidance is provided. Complying with this process is considered sufficient. The excellent air transport safety record up to date does not repudiate this assumption. Many consider DO-178B as the toughest standard in industry.

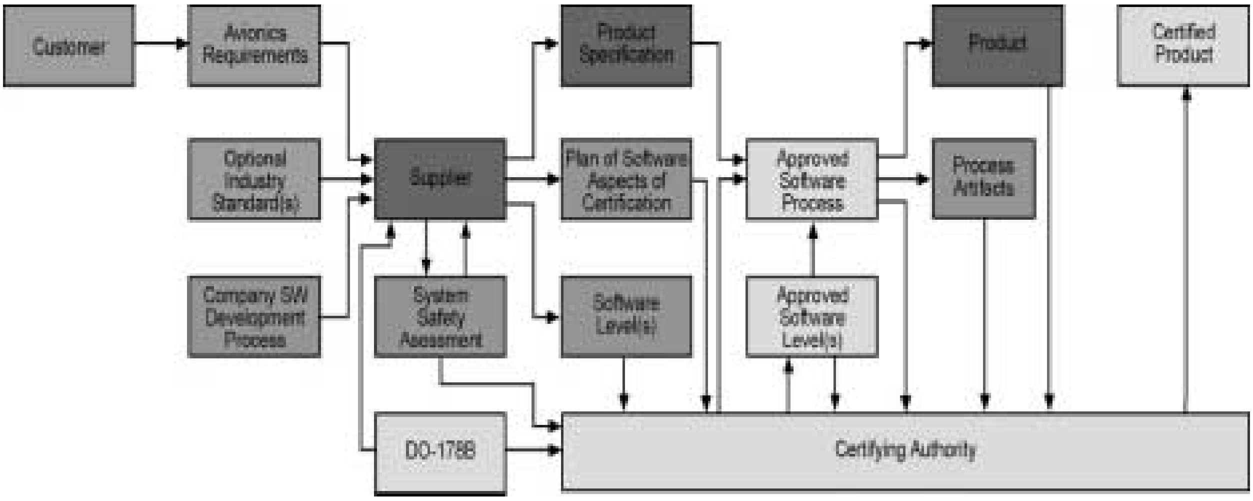

Figure 4: Overview of airborne safety standard DO-178B

Figure 4 provides an overview of the DO-178B software development and certification process. DO-178B has an abstract lifecycle defining four generic phases (software requirements process, software design process, software coding process and software integration process). A developer must map its software processes onto those required by DO-178B. This is described in a special document called the Plan of Software Aspects of Certification (PSAC). This document should be negotiated between the developer and certifying authorities prior to actual software development. Subsequently, the developer needs only to comply with the agreed PSAC document.

DO-178B specifies 66 detailed requirements for the four software development processes complemented by the software planning process and integral processes. For each level the applicability of each requirements is defined, with all required for level A.

Industry standards define the functions that must exist in certain avionics units (e.g., flight management system). Developers can further enhance such units with client-based requirements. Consequently, most avionics units are custom made, though the mandating of core functionality does provide a basis for reuse.

To date, there is usually only one software application assigned to a hardware unit, although the Integrated Modular Avionics (IMA) industry standard will allow several fixed and pre-defined applications to run on a single hardware unit. This illustrates how DO-178B trails current real-time and embedded systems development practices.

Commercial off-the-shelf (COTS) products are officially allowed by DO-178B, however, no requirements are waived. Consequently, only COTS products that have been developed specifically taking all DO-178B requirements into account can be used. Note that navigation services like [WAAS, 2003], [EGNOS, 2003], [MSAS, 2003] and the European Galileo effort, all take DO-178B into account but deviate on details. These deviations are predicated upon cost-benefit analyses, in that various requirements may be more expensive than justified by the relative usage of the navigation service by a particular domain. These deviations must be shown to the conservative certifying authority not to materially distract from the safety goals of DO-178B.

Certification involving new software techniques such as object-orientation tends to be troublesome for the first applicant trying to certify its use since DO-178B tends to trail the current state-of-the-art in embedded software engineering. The first applicant bears the full burden to convince the justifiable conservative certifying authorities.

Certification is required from each nation where an airline wants to acquire an aircraft for civil use. Airbus has obtained its initial 13 type certifications over the last 10 years from the European Joint Aviation Authority (JAA), complemented by another 13 from the U.S. Federal Aviation Administration (FAA) plus 130 from other nations. Boeing obtained 200 additional certificates in the same period, after the initial FAA certification [Holderbach, 2001]. Substantial benefits can be accrued when each nation accepts the certifications of all accredited ICAO member states. A system of accreditation should enforce equal enforcement of the standard in all nations concerned. Currently mutual certification recognition involves a lengthy negotiation between the two certifying authorities involved, leading to a bilateral agreement. Air transport's good safety record does not repudiate the claim that DO-178B compliance provides the safety objectives. However catastrophic failures (level A) are fortunately so rare, that the absence of software induced catastrophic failures does not statistically justify DO-178B claims. Like all other software safety standards, evidence on the utility of effectiveness of each of the 66 requirements is lacking. They are based on a consensus on engineering judgement.

3.2 Airborne software safety standard DO-278B/ED109

For Air Traffic Management (ATM) ground (and satellite) systems, the USA has produced a new standard [DO-278, 2002] by extending DO-178B. Table 2 provides an overview of the six Assurance Levels (AL) defined in DO-278. Note that unlike DO-178B, neither a definition of the assurance levels nor an indication of the allowed failure probability is provided. DO-278 adds an assurance level by splitting level C. DO-178B added an level by splitting level II from it predecessor DO-178A into level B and C. Consequently any software safety standards should provide sufficient grading.

In contrast to DO-178B, DO-278 acknowledges the use of independently developed (pre-existing) COTS, by defining processes for planning, acquisition, verification, configuration management and quality assurance. It must be demonstrated that unused COTS capabilities do not adversely effect the ATM system. An important extension to DO-178B is that COTS service experience may be used, thereby obviating the need to apply a DO-278 compliant development process for some assurance levels. However, the restrictions on service experience are quite severe. The information on service experience is included in Table 2. In the table, “one year” means that for a continuous period of 8760 hours of representative use no failure may occur.

Additionally, all in-service reports originating from all users of the COTS have to be evaluated for their potential adverse effects on the ATM system.

DO-178 level	DO-278 assurance level	COTS service experience
A	AL 1	Not allowed
B	AL 2	Negotiate with approval authority
C	AL 3	One year
	AL 4	Six months
D	AL 5	Typically not needed
E	AL 6	Not applicable

Table 2: DO-278/ED109 overview

3.3 EUROCONTROL Recommendations for Air Navigation Services

The European Organisation for the Safety of Air Navigation (EUROCONTROL) has produced the Recommendations for Air Navigation Services (ANS) [EUROCONTROL, 2003]. These recommendations combine DO-178B, IEC-61508, and the Capability Maturity Model [Paulk, 1993] into a combined safety and quality assurance document. The software classification is provided in Table 3. The classification is based on the EUROCONTROL Safety Regulatory Requirement [ESARR 4, 2003], while inserting an additional level identical to Level B of DO-178B. The requirements on the evidence that needs to be provided depend on the assurance level. The standard also covers operational use and maintenance phase, a useful extension to DO-178B.

Software assurance level	ESARR4 severity (Class, effect)		ESARR 4 occurrence likelihood	software occurrence likelihood (operational-hour)
1a	1	Accidents	Improbable	N/A
1b		DO-178B level B	N/A	DO-178B Extremely Remote 10^{-9} < .. < 10^{-7}
2	2	Serious incidents	Remote	10^{-6} < ... < 10^{-5}
3	3	Major incidents	Occasional	10^{-5} < ... < 10^{-4}
4	4	Significant incidents	Probable	10^{-4} < ... < 10^{-3}
5	5	No immediate effect on safety	N/A	N/A

Table 3: EUROCONTROL EATMP software assurance levels

3.4 Electronic Flight Bag AC120-76A

The electronic flight bag is a COTS-based hardware platform that supports many independent software applications, possibly even simultaneously. As such the electronic flight bag is well suited for the airborne part of the TALIS system. The electronic flight bag can be part of the aircraft and so DO-178B applies. However, it can also be used outside the aircraft, so a special document on the safety and certification [AC120-76A, 2003] is available. The electronic flight bag could either be a portable device like a slate laptop or personal digital assistant, or be installed in the aircraft.

The electronic flight bag software is classified as:

- Type A: applications that include pre-composed, fixed presentations of aviation data. Type A software needs Flight Standards District Office (FDSO) approval. 71 example applications are provided;
- Type B: applications that include dynamic applications that interactively manipulate and present aviation data. Type B software additionally needs evaluation by the Aircraft Evaluation Group. AC120-76A lists 17 applications. A six-month operational evaluation is needed, during which a (paper) back-up of the application is required.
- Type C: all other applications. Full DO-178B approval is needed.

All user-modifiable software is type C. Consequently a key TALIS requirement like dynamically uploading applications remains cumbersome. Positive is the guidance provided on usability or human factors.

Compliance to AC120-76A implies compliance to 103 sections of 5 parts of the US Code of Federal Regulation (CFR) relating to airworthiness plus 45 additional sections of 4 parts of the operating regulations plus 20 advisory circulars plus 10 other FAA regulations. Even within AC120-76A, some parts relate to activities performed only once for the approval of software, while other parts mention an operational approval valid for a specific operator for six months. This profusion of standards, regulations, etc, is typical for integrated systems like TALIS. Consequently, there is a need for a different approach to certification, which ensures the safety, but omits the many un-harmonised standards. Note that possible different national interpretations further complicate certification without increasing safety.

3.5 ESA DRD 920, a DO-178B based standard

For the European Geostationary Navigation Overlay System description (EGNOS) programme, the European Space Agency (ESA) has produced a specific standard that combines the standard European space quality assurance practises PSS05 with DO-178B, [DRD 920, 1999]. DRD 920 addresses issues arising from the use of subcontractors and the reuse of existing software. Interestingly, ESA acts both as customer as well as certifying authority. Consequently, for EGNOS additional certification activities need to be performed once EGNOS becomes operational in any ESA member state.

An annex to DRD 920 provides the PSAC (Plan for Software Aspects of Certification, a DO-178B required document). The annex states that forty DO-178B requirements are satisfied by the standard, while a further three are partially satisfied, twenty-six are not satisfied and for four requirements the status is unclear. For the unsatisfied requirements the contractor has to comply by other means. Human Machine Interface testing and specialised tools are specifically mentioned by DRD 920.

Procured software is approved by ESA. For COTS software "certification material" is needed to satisfy the DO-178B objectives. If modifications of reused software exceed 20% of the code, it is considered new code. A virus check for COTS is required, merging safety and security concerns.

An idealised software life cycle ignoring iterations, deployment, maintenance and decommissioning is described by DRD 920. Despite a few useful innovations, DRD 920 does not materially differentiate itself from pre-existing standards (e.g. DO-178B).

3.6 UK CAA Air Traffic Management approach

The approach for safety assurance of Air Traffic Management (ATM) systems typically differs from the approach for aircraft. For the latter, a single certification is done, after which all aircraft of the same type are certified airworthy (in the country issuing the certificate). For services provided by ground systems, typically the national regulator issues a license to operate for a fixed period of time. After expiry of the license a periodic review is held and this license is extended for the same time. Unfortunately for ATM systems, as discussed above, no standard is (yet) internationally recognised. Even on a European level, harmonisation is not complete.

As the UK practise is advanced and informative, it is discussed below. The UK CAP-670 contains all safety-related regulations. The excerpt "Regulatory objective for software safety assurance in air traffic service equipment" [SW01, 1998] focuses on software. The Standard defines Assurance Evidence Levels (AEL), to identify the type, depth and strength of evidence to be provided by the software development process to the assessor. In this way, the developer may use any standard to provide the evidence. Based on the ESARR 4 safety classification (see Table 3), one AEL is defined for each class. Three types of evidence are acknowledged: test, field service and analytic. Every type of evidence can be either direct or backing, with requirements provided for each type.

This goal-oriented approach is a more modern approach than that used with the other standards discussed here. It means that the supplier has to provide the software classification, the type of evidence that is needed, the evidence itself, and justification that the evidence is adequate. This way of working would be more suitable for integrated systems like TALIS than the profusion of the myriad standards currently available. This approach should be complemented by a mutual recognition scheme, which means that approval in one country would be recognised by other countries, preferably world wide, but at least within Europe. The merging of the authorities of the European Union member states into the European Aviation Safety Agency (EASA) is a step in the right direction.

The [Commission on the future of the US aerospace industry, 2002] states that the current product-based FAA certification process hampers innovation in several ways. It proposes to shift from the current practises to an approach that fosters innovation to make aviation safer and more secure. Such an approach would certify manufacturing organisations, who are then trusted to design and produce safe products, under what is called process certification. The FAA would focus on the most critical safety aspects and safety oversight. The commission also states an objective to reduce the aviation fatal accident rate by 90 percent by 2025. Given the lack of evidence for the current safety requirements, a lot of standard innovation is needed to accomplish these two objectives.

4 Other domain safety standards

The following overview of software safety standards from other domains is provided:

- To learn from their approach. Consequently this chapter will focus on the differences
- To assess COTS. For COTS to be viable the air transport market it too small. Both Boeing and Airbus only produce a few hundred aircraft per year, with the number of processors involved in safety critical tasks in the tens. Consequently for COTS to pay off, these products should be deployable in other safety conscious markets as well.

4.1 Process industry IEC-61508

From the general software safety-critical domain [IEC-61508, 1998] is available which originated in the process industry. Four Safety Integrity Levels (SIL) are defined. IEC-61508 states that safety can be quantified and assessed using reliability prediction techniques only for hardware. For software, only qualitative techniques and judgements are possible. The Standard explicitly states that failures rates lower then 10^{-9} per hour (i.e., level A according to DO-178B or DO-278 AL1) can not be achieved for complex systems. Note that every programmable system is considered complex. IEC-61508 defines its own software safety lifecycle, based on the general V-model, described in many textbooks like [Broekman, 2003]. The IEC-61508 life cycle does include operations, maintenance, repair, retrofit and even decommissioning procedures, a useful extension to DO-178-B. The railway industry is converting to IEC-61508 by providing domain specific extensions to IEC-61508, in line with the intention of this standard.

Part 7 of the standard aims to provide an exhaustive list of techniques for each process phase, including recommendations on their use (or avoidance) for each SIL. This part of the standard will need regular updates to remain in-line with information technology innovations. It is possible to certify COTS for a certain level, when an IEC-61508 compliant development process is followed. An independent party will perform the certification. Table 4 provides an overview of the four SIL levels.

Safety Integrity Level (SIL)	Failure probability per hour (systems active > once per year)	Failure probability per demand (systems active < once per year)
4	10^{-9} Ò ... < 10^{-8}	10^{-5} Ò… < 10^{-4}
3	10^{-8} Ò ... < 10^{-7}	10^{-4} Ò… < 10^{-3}
2	10^{-7} Ò ... < 10^{-6}	10^{-3} Ò… < 10^{-2}
1	10^{-6} Ò ... < 10^{-5}	10^{-2}Ò … < 10^{-1}

Table 4: IEC-61508 Safety Integrity Levels

Using service experience is allowed, but in practice hardly possible for higher SIL levels. An example from the standard states that for a SIL 1 system, 95% confidence in correct functioning requires 300 hours of relevant service experience. For a SIL 4 system, 99.5 % confidence requires 690 000 years of service experience.

4.2 Nuclear industry IEC-60880-2

In the nuclear industry [IEC-60880-2, 2000] is applicable. IEC-60880-2 is based on the software classification provided in [IEC-61226, 1993], see table 5. The basic single-failure criterion requires the assembly of safety systems to remain functional despite any random failure. This single-failure criterion is not applicable for software, as a software failure can cause a system with multiple hardware units to fail. As a consequence IEC-60880-2 devotes an appendix to the pros and cons of multiple diverse software implementations. Multiple software versions can only cover some fault classes, so incorrect or ambiguous specifications remain single point-of-failure.

Category	Description	Excerpt assignment criteria
A	Principal role in achieving safety	• Mitigate to prevent significant sequence • Failure could result in significant sequence
B	Complementary role to category A	• Control process variables within safety limits • Alert staff of Category A failure • Continuously monitor category A function
C	Auxiliary or indirect role	• Enhance category A performance • Monitor and mitigate internal hazards an natural events • Ensure personnel safety
Unclassified	No direct safety role	• Not significant to safety

Table 5: IEC-61226 Overview

IEC-60880-2 distinguishes between software tools that can introduce errors and tools that fail to detect them. The requirements for the former category are strict. Compilers (called translators) are acknowledged to be too large to demonstrate their correctness. They are trusted under certain restriction, unlike DO-178B where binary code needs to be verified for the highest level.

The compiler may not introduce dead code, which is code that is not traceable to requirements (e.g., error handling). Operating experience may compensate for some lack of design documentation.

IEC-60880-2 allows for COTS. There are strict requirements on the evaluation of functions, design documentation etc. In case operating experience is used, there are requirements on the operating history data. Also after acceptance of the COTS, all subsequent error and failure information has to be assessed for its potential impact on the approved system.

Unlike DO-178B, the evidence provided by formal methods is deservedly recognised.

4.3 Medical industry FDA-1252

For software in medical devices in the USA [FDA-1252, 1998] applies. The software is classified into three "levels of concern," see Table 6. FDA-1252 states that as the probability of software failure cannot be measured, only the severity of the software failure consequences is used to determine the level. A table listing 12 documents describes for each level of concern what type of information is needed, if any. No specific software life-cycle model is prescribed, but a general V-model for verification is provided. Verification needs to be performed at module, integration and system levels.

Level of concern	Severity description
Major	Software failures that could cause, directly or indirectly, to death or serious injury of the patient and/or the operator
Moderate	Software failures that could cause, directly or indirectly, to non-serious injury of the patient and/or the operator
Minor	Software failures are not expected to cause injury to patient and/or operator

Table 6: FDA-1252 Level of concern

Even though FDA-1252 states that artificial neural networks are impossible to verify, they are allowed for all levels of concern. Consequently the assumptions and the training of the neural network need to be verified, but no guidance is provided.

According to FDA-1252, embedded and real-time systems pose unique concerns, but only the use of techniques, simulators and emulators to analyse timing of critical events is mentioned, but not imposed. The importance of human factors is acknowledged without enforcing verification and validation requirements. In the same spirit, security is raised, but no requirements ensue. Consequently the air transport domain can not learn much from FDA-1252. However, in order for COTS to become commercially viable, COTS needs to be deployable in various safety critical domains. This implies recognition of DO-178B by the medical domain and a scaling of its levels to the FDA-1252 levels of concern.

5 Security ISO-15408

After the tragic September 11 (2001) events security has become a major concern for air transport. Especially network-enabled systems, like TALIS, are vulnerable to attacks hence need protection. The trend to make systems network-enabled will also become relevant for the safety critical systems in the other domains mentioned. This implies that standards are not only needed for safety but also for security. The [ISO-15408, 1999] is an international standard which includes security requirements and can provide certifications for complying products. ISO-15408 is the civil variant of the Common Criteria (CC) from the military domain and will follow all updates of the Common Criteria. As such it is discussed in this paper on standards. The ISO-15408 aims to provide objective evidence about the product security level. Qualified and officially recognised assessors perform the objective and repeatable evaluation, much like DO-178B for safety certification. The evaluation can lead to a certificate, which is currently recognised by 16 countries, the USA, Canada, Australia, New Zealand and twelve European countries.

The ISO-15408 considers three security objectives aiming to prevent:

- Damaging disclosure of the service to unauthorised recipients (loss of confidentiality);
- Damage through unauthorised modification (loss of integrity);
- Damage through unauthorised deprivation of access to the asset (loss of availability).

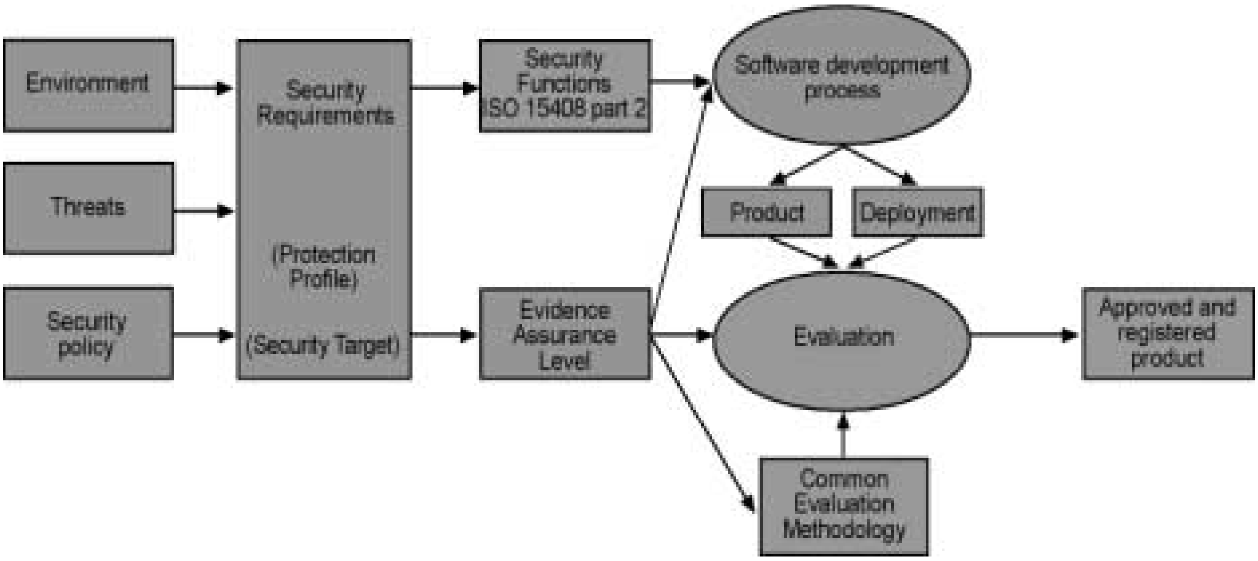

Figure 5: Overview of security standard ISO-15408

Figure 5 provides an overview of the ISO-15408 view on the realisation of security functions. The security environment provides the context of the asset. Combined with the perceived threats and the security policy the security requirements can be derived. These requirements consist of a reusable Protection Profile (PP) and an asset specific Security Target (ST). Based on these

requirements and the extensive listing of possible security functions in the ISO-15408 Part 2, the security functions of the system are determined. Separately the protection level is determined, which determines the amount of implementation effort and evaluation effort.
Table 7 provides an overview of the Evaluation Assurance Levels (EAL). The amount of COTS products in the register at the time of writing (August 2003) illustrates that ISO-15408 is rapidly being accepted.

EAL	**Description**	**# of COTS products**	
		Certified	In evaluation
1	Functionally tested, security threats not serious	11	1
2	Structurally tested, low to moderate assurance	22	12
3	Methodically tested and checked, maximum assurance without infringing sound development practise	17	2
4	Methodically designed, tested and reviewed, maximum assurance compatible with good commercial practise	44	19
5	Semiformally designed and tested, maximum assurance with moderate security engineering	1	0
6	Semiformally verified design and tested, protect high value assets against significant risk	0	0
7	Formally verified design and tested, extremely high risk situations and/or high assets values	0	0
	Total # of COTS products	95	34

Table 7: ISO-15408 Evaluation Assurance Level

The ISO-15408 adds further requirements on the software development process, so harmonisation with the safety requirements is advantageous.
Note that whereas DO-178B unjustifiably does not recognise the verification evidence from formal methods, ISO-15408 requires it for the highest level. As air transport does not have a tradition in software security certification, the industry can benefit of the military and commercial domains through this more advanced standard. This would constitute innovation through standardisation.

6 Conclusions

For air transport, safety is of prime concern. To demonstrate its safety, all systems need to comply with the relevant safety standards.
For software this had led to a profusion of standards with different, sometimes even non-compatible requirements. Those differences are hard to justify, as they derive from common safety concerns. No standard is clearly superior. For integrated systems that have to rely on

COTS, like TALIS, the current certification practise is hampering innovation hence improvement is needed.

To improve software safety and its certification the following attributes are recommended for inclusion in software safety standards and certification schemes:

- Certification is to be performed by an independent third party.
- A trusted party or organisation must accredit the independent third party.
- Certification should be performed in accordance with objective standards.
- There should be objective guidance for the reviewers. (e.g. like for DO-178B and the ISO-15408)
- The standard should provide maximum freedom for the software processes being used and the deployed techniques in order to exploit information technology innovation.
- The software cannot be tested to high levels of safety; instead many standards have to rely on process requirements.
- The standard should allow a grading of software with sufficient nuances for less safety critical applications.
- The standard should recognise COTS products. This should be done in a timely and cost effective manner, to preserve the advantages of deploying COTS.
- As air transport has many integrated systems, inevitably the constituent parts will come from various domains so there should be mutual recognition of the various standards/certificates
- Research is needed on the effect of software safety requirements so that each requirement can be justified for the intended safety level.
- The current state-of-the-art does not (yet) allow large systems (as used in air transport) to be formally verified. For tractable subsystems, the evidence provided by formal methods should be recognised.
- It would be convenient if software standards covering various non-related properties, like safety and security, would impose compatible requirements.

Standard innovations like the goal-based approach, which states the objective, the evidence and the reasoning seem to be beneficial if current safety standards are to be maintained or even improved. This approach may comply with the objective of the US aerospace committee to shift to a new software certification paradigm.

7 References

AC120-76A (July 2003), *Guidelines for the certification, airworthiness and operational approval of electronic flight bag computing devices*, FAA

Broekman B, Notenboom E, (2003), *Testing embedded software,* Addison-Wesley

Commission on the future of the US aerospace industry (November 2002), *Anyone, anything, anywhere, anytime*, www.ita.doc.gov/aerospace/aerospacecommission

DO-178B/ED12B (December 1992), *Software Considerations in Airborne Systems and Equipment Certification*, RTCA & EUROCAE

DO-278 (March 2002), DO-278/ED109 *Guidelines for the communication, navigation surveillance, and air traffic management (CNS/ATM) systems software integrity assurance,* RTCA & EUROCAE

DRD 920 (August 1999), *GNSS-1 Programme implementation phase, EGNOS software engineering standard*, to be obtained from the EGNOS programme office

EGNOS (2003) *European Geostationary Navigation Overlay System description* http://www.esa.int/export/esaSA/navigation.html

ESARR4 (October 2002), *ESARR 4, Software in ATM Systems,* EUROCONTROL, http://www.eurocontrol.be/src/html/deliverables.html

EUROCONTROL (November 2000), *Towards Co-operative ATS, The COOPATS Concept*, EUROCONTROL DIS/ATD/AGC/MOD/DEL 01

EUROCONTROL (March 2003), *recommendations for Air Navigation Services,* SAF.ET.ST03.1000.GUI-01-00, to be obtained from the EUROCONTROL Safety Management group

FDA-1252 (May 1998), *Guidance for FDA reviewers and industry guidance for the content of pre-market submissions for software contained in medical devices,* http://www.fda.gov/cdrh

Holderbach, H. (2001) *Type certification of commercial aircraft call for enhanced international rules*, ICAO Journal 2

IEC-60880-2 (December 2000), *Software for computers important to safety for nuclear power plants, Part 2, software aspects of defence against common cause failures, use of software tools and of pre-developed software*, http://ww.iec.ch

IEC-61266 (May 1993) *Nuclear power plants - instrumentation and control systems important for safety - Classification*, http://ww.iec.ch

IEC-61508 (December 1998), IEC-61508 *Functional safety: safety related systems,* 7 parts, http://ww.iec.ch

Jensen D., (January 2003), *Industry transformation*, Avionics magazine January 2003

ISO-15408, (August 1999), *Common criteria for security evaluation, Version 2.1*, also known as the Common Criteria, http://www.commoncriteria.org/cc/cc.html

Kesseler E., (June 2003*), Transforming air transport to a concurrent enterprise, Technical, safety and security perspectives*, 9th International Conference on Concurrent Enterprising, ICE2003, 16-18 June 2003, http://www.ice2003.org/

MSAS (2003), *MTSAT Satellite- based Augmentation System description* http://www.mlit.go.jp/koku/ats/e/mtsat/miss/03.html

Paulk, M. C., Weber C. V., Garcia S. M., Chrissis M. B., Bush M. W., (February 1993), *Key Practices of the Capability Maturity Model, Version 1.1, Software Engineering Institute*, http://www.sei.cmu.edu/cmm/obtain.cmm.html

SW01 (April 1998), CAP 670 *ATS Safety Requirements*, UK CAA http://www.caa.co.uk/docs/33/CAP670.pdf

WAAS (2003) *Wide Area Augmentation System description*, http://gps.faa.gov/programs/index.htm

8 Abbreviations

ACC	Area Control Centre
ACL	ATC Clearance and Information
ACM	ATC Communications Management
AMC	Airspace Management Cell
AOC	Airline Operations Centre
APP	Approach Control
ATC	Air Traffic control
ATM	Air Traffic Management
ATSAW	Air Traffic Situation(al) Awareness
AUTOPS	Autonomous Flight Operations
CAP	Controller Access Parameters
CFMU	Central Flow Management Unit
CFR	(US) Code of Federal Regulation
COSEP	Co-operative Separation Assurance
COTS	Commercial-off-the-shelf
COTRAC	Common Trajectory Co-ordination
DCL	Departure Clearance
DFIS	Digital Flight Information
DSC	Downstream Clearances
DYNAV	Dynamic Route Availability
EAL	Evaluation Assurance Levels
EASA	European Aviation Safety Agency
EATMP	European Air Traffic Management Programme
EGNOS	European Geostationary Navigation Overlay System description

ESA	European Space Agency
ESARR	EURCONTROL Safety Regulatory Requirement
FAA	Federal Aviation Administration
FAR	Federal Airworthiness Requirement
FLIPCY	Flight Plan Consistency
FMP	Flight Management Position
IFPS	Initial Flight Plan Processing System
JAA	Joint Aviation Authority
JAR	Joint Aviation Requirement
MSAS	MTSAT Satellite- based Augmentation System
PP	Protection Profile
PPD	Pilot Preferences Downlink
SAP	System Access Parameters
ST	Security Target
TALIS	Total Information Sharing for Pilot Situational Awareness Enhanced by Intelligent Systems
TWR	Tower Control Service
WAAS	Wide Area Augmentation System

Acknowledgement

Part of this work has been 50% funded by the European Commission, DG Information Society Technologies as project IST-2000/28744. The EUROCONTROL Experimental Centre leads the consortium of Lido, NLR, Thales Avionics and Skysoft.