DOCUMENT CONTROL SHEET

	ORIGINATOR’S REF. NLR-TP-2003-300		SECURITY CLASS. Unclassified

ORGINATOR

National Aerospace Laboratory NLR, Amsterdam, The Netherlands

TITLE

Air transport, from privilege to commodity

A COTS enabled paradigm shift

PRESENTED AT

The World Congress Aviation in the XXIst Century, Kyiv, Ukraine, 14-16 September 2003

AUTHORS	DATE	PP	REF
E. Kesseler	June 2003	16	13

DESCRIPTORS

SECURITY
SERVICE-BASED ARCHITECTURE
SOFTWARE CERTIFICATION

ABSTRACT

One hundred years ago air transport started as a technical challenge. Once the enchantment was over, the practical advantages were swiftly recognised, providing privileges for the affluent. Due to the inherent dangers and the early mishaps, a self-improving safety system evolved. The safety of current air transport testifies to the success of this approach.

The current business trend is the integration of independent companies into an Internet based virtual enterprise, delivering seamless customer support. As air transport has become a commodity, these service-based architecture techniques will be applied. The impact of the myriad, not harmonised safety rules on such integrated software will be discussed.

Recently security concerns have risen. It is described how the common criteria could provide a framework for systematic application of security to software.

Nationaal Lucht- en Ruimtevaartlaboratorium
National Aerospace Laboratory NLR

NLR-TP-2003-300

Air transport, from privilege to commodity
A COTS enabled paradigm shift

E. Kesseler

This report is based on a presentation held at the World Congress Aviation in the XXIst Century, Kyiv, Ukraine, 14-16 September 2003.

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
	June 2003

Approved by author: 6/6/2003	Approved by project manager: 20030606	Approved by project managing department: 4/8/3

Summary

One hundred years ago air transport started as a technical challenge. Once the enchantment was over, the practical advantages were swiftly recognised, providing privileges for the affluent. Due to the inherent dangers and the early mishaps, a self-improving safety system evolved. The safety of current air transport testifies to the success of this approach.

The current business trend is the integration of independent companies into an Internet based virtual enterprise, delivering seamless customer support. As air transport has become a commodity, these service-based architecture techniques will be applied. The impact of the myriad, not harmonised safety rules on such integrated software will be discussed.

Recently security concerns have risen. It is described how the common criteria could provide a framework for systematic application of security to software.

Contents

(16 pages in total)

1 Introduction

Nearly one century after the first powered flight the need for a quantum leap in air transport improvement became apparent on both sides of the ocean. The European vision for 2020 [1] states “an air transport system responding to society’s needs despite a three-fold increase in air traffic because aircraft are cleaner, safer, quieter and air traffic is efficiently managed”. The imperatives are safer, cleaner and quieter (in this order) resulting in stated goals including a five-fold reduction in the average accident rate, a seamless European Air Traffic Management (ATM) system, integration of air transport into an efficient multimodal transport system and halving the time-to-market for new products.

In the US the Anyone, Anything, Anytime, Anywhere vision [2] states a number of breakthrough capabilities including, tripling air transport capacity by 2025, reducing fatal accident rate by 90%, reducing aircraft noise and emissions by 90% and reducing time-to-market from decades/years to months/weeks. Information Technology (IT) tops the list of potential breakthrough enablers. Reducing the time-to-market requires solving the airborne equipage problems. As the current certification process remains a major issue [2] proposes a paradigm shift.

This paper shows how an actual project, predating these vision documents, tries to combine innovative IT concurrent enterprise concepts with ATM practises to address the challenges mentioned above. Based on some observations of the European COOPATS (Co-operative Air Traffic Services) concept chapter 2 proposes a prototype infrastructure as realised in the TALIS project. Given the ambitious safety objectives, safety will become even more important, so chapter3 discusses current certification practises. Chapter 4 summarises the findings.

2 Air transport innovation

2.1 New ATM concepts

In busy airspace the current working methods are approaching their limits, resulting in safe but uneconomical flight execution with delays on the ground and in the air. The current ATM concept certainly cannot cope with the three-fold increase required by [1] and [2]. To improve this situation the COOPATS concept [3] has been conceived. COOPATS' 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 data exchange. The result is improved situational awareness for both pilot and controller, enabled by intelligent flight-phase dependant services. Figure 1 provides an overview of the proposed COOPATS services.

The US Distributed Air-Ground Traffic Management (DAG-TM) considers three parties: pilot, AOC (Airline Operations Centre) and air traffic controller, and defines 14 services. As these services are not fully defined and validated, for both COOPATS and DAG-TM considerable evolution in the amount and content of these services is to be expected. This supports the need for a time-to-market in the order of months to 1 year. An example how integrated services can benefit noise reduction objectives is Continuous Descent Approach (CDA) where an aircraft descends with idling engines. Currently this induces capacity loss because ATM cannot accurately predict the resulting arrival time and has to allow for larger slots. This noise abatement is not effective, as it is only possible at low traffic densities.

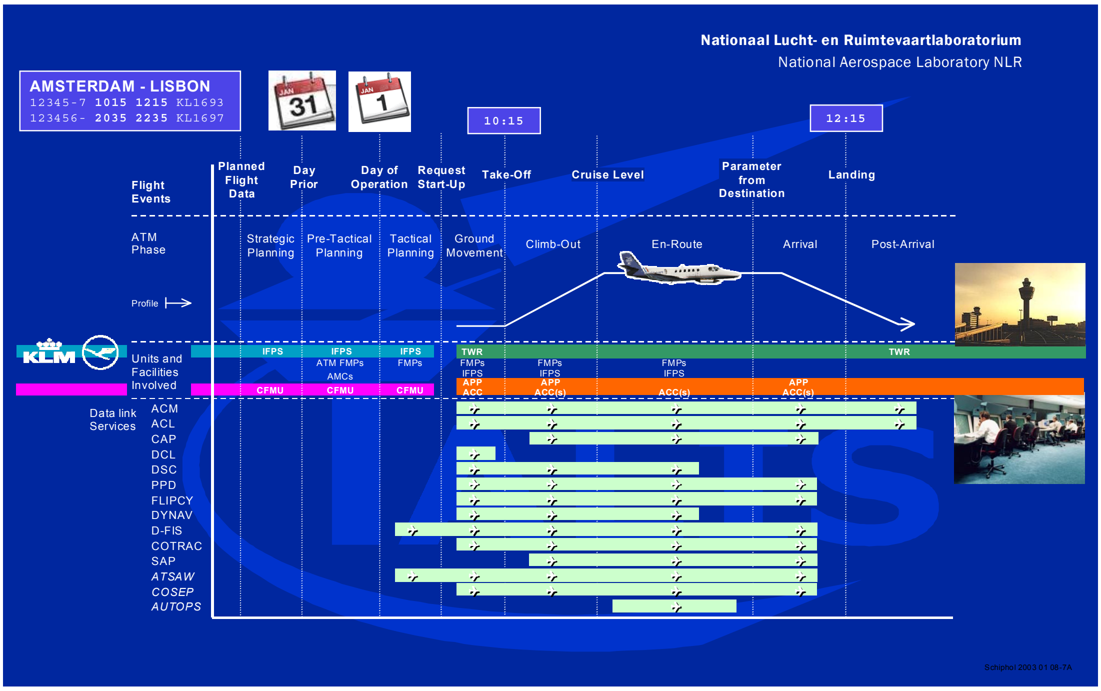


Figure 1 Overview of Co-operative Air Traffic Services (COOPATS)

2.2 TALIS solution

COOPATS and DAG-TM only consider three parties although actually more parties are involved as shown in figure 2.

The concurrent enterprise concept is to provide an IT infrastructure enabling a company to use services provided by other companies to create more advanced services. The success of this business model in other industries demonstrates its viability. The TALIS (Total Information Sharing for Pilot Situational Awareness Enhanced by Intelligent Systems) project [4] provides a supporting architecture for COOPATS and similar concepts and their innovative services. The TALIS architecture (figure 3) should also integrate the existing systems of yet other actors like the authorities (figure 2). 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.

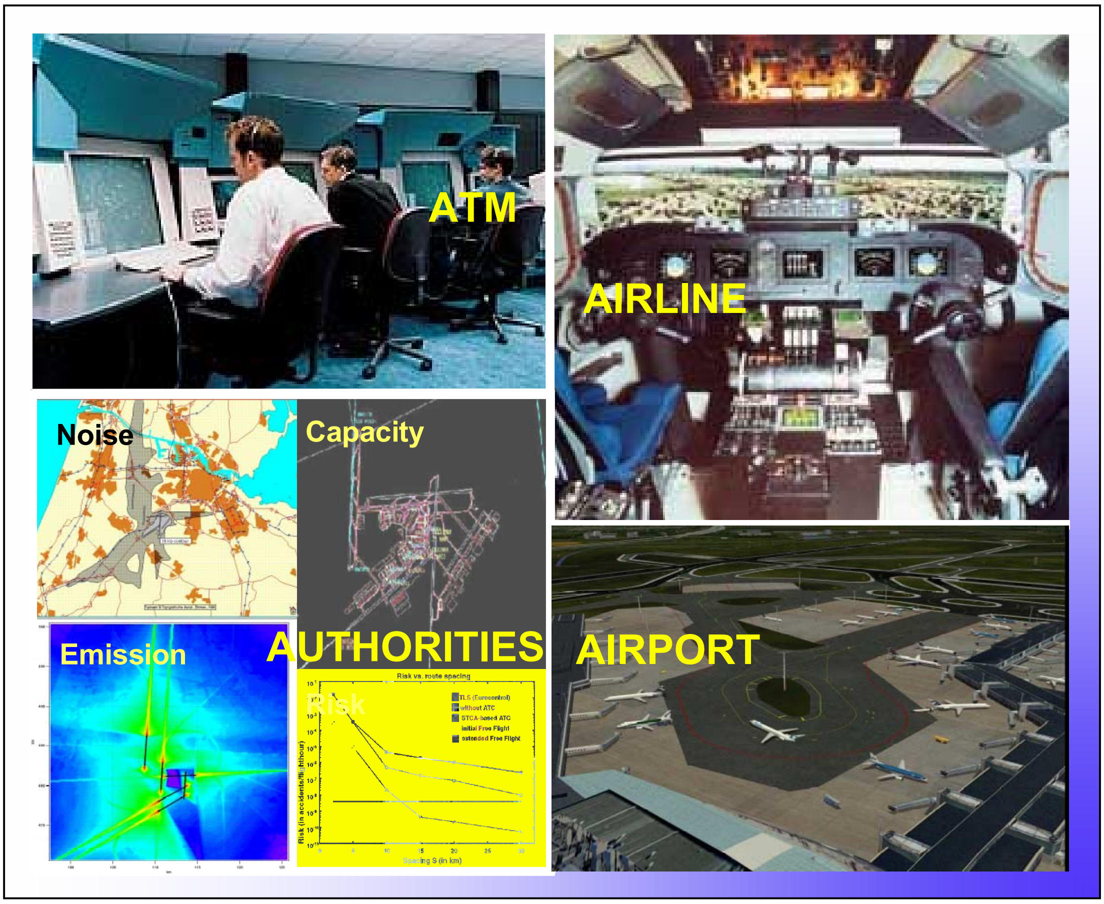
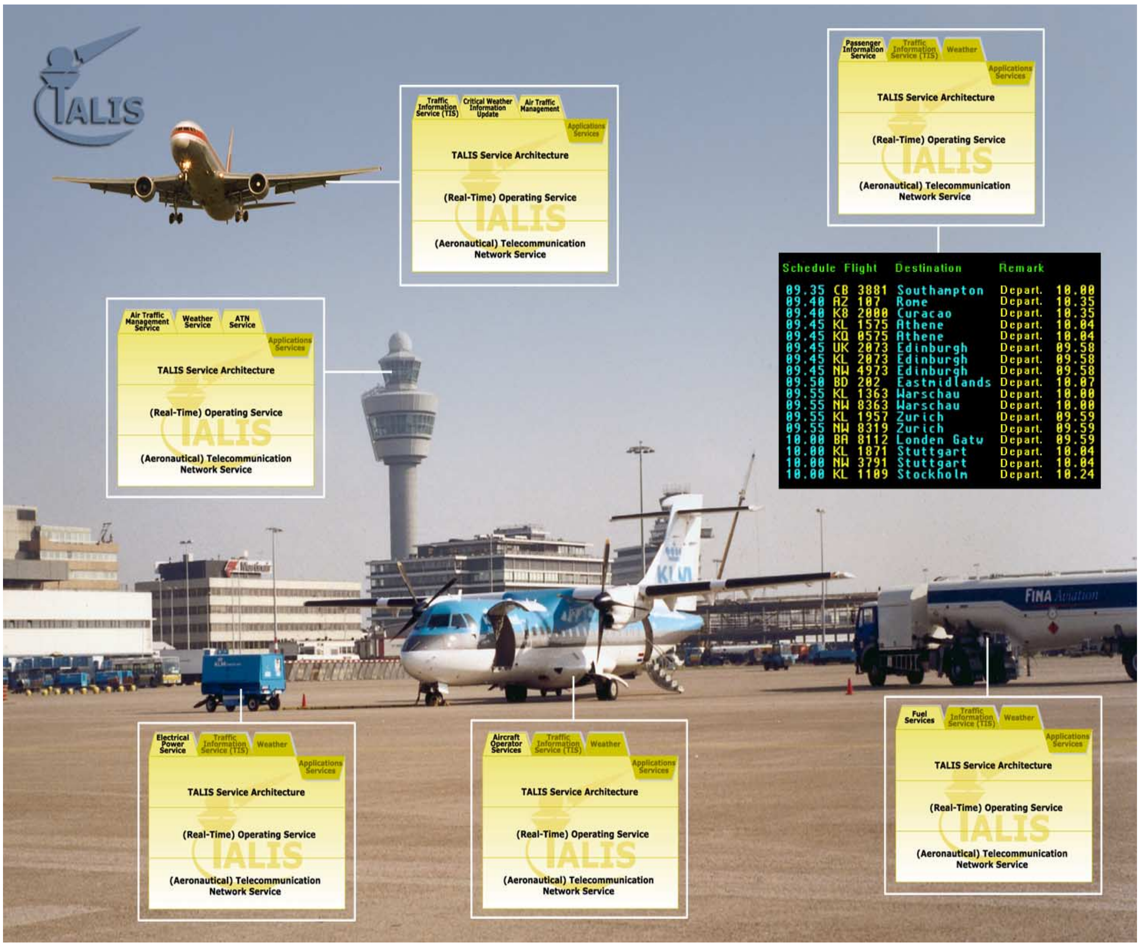


Figure 2 Overview of air transport parties

By basing the TALIS prototype on Java, services can be uploaded dynamically. Once a service is certified, immediate fleet-wide deployment can be achieved, reducing the time-to-market for new services (or products as they are called in references [1] and [2]). As the concurrent enterprise and Java are COTS (Commercial Off-The-Shelf) products, significant benefits from exploiting COTS can be accrued. Since the start of the TALIS project, Jini has been superseded by Openwings, which considerably extends connectivity to many affordable COTS hardware platforms. For Java work has started on a DO-178B certifiable real-time kernel in the Open Group [5] in collaboration with the Java Community Process. Once completed this will reduce the challenge to certify the software implementing new services. TALIS will realise two services with two iterations plus the infrastructure in 2½ years, demonstrating a time-to-market of around one-year. The concurrent enterprise facilitates seamless ATM and its integration into a multimodal transport system. Consequently the TALIS choice for the concurrent enterprise and COTS solutions pays off.


TALIS
Traffic Information Service (TIS)
Critical Weather Information Update
Air Traffic Management
Applications Services
TALIS Service Architecture
(Real-Time) Operating Service
TALIS
(Aeronautical) Telecommunication Network Service
Passenger Information Service
Traffic Information Service (TIS)
Weather
Applications Services
TALIS Service Architecture
(Real-Time) Operating Service
TALIS
(Aeronautical) Telecommunication Network Service
Air Traffic Management Service
Weather Service
ATN Service
Applications Services
TALIS Service Architecture
(Real-Time) Operating Service
TALIS
(Aeronautical) Telecommunication Network Service
Electrical Power Service
Traffic Information Service (TIS)
Weather
Applications Services
TALIS Service Architecture
(Real-Time) Operating Service
TALIS
(Aeronautical) Telecommunication Network Service
Aircraft Operator Services
Traffic Information Service (TIS)
Weather
Applications Services
TALIS Service Architecture
(Real-Time) Operating Service
TALIS
(Aeronautical) Telecommunication Network Service
Fuel Services
Traffic Information Service (TIS)
Weather
Applications Services
TALIS Service Architecture
(Real-Time) Operating Service
TALIS
(Aeronautical) Telecommunication Network Service
KLM
FINA Aviation

Schedule	Flight	Destination	Remark	
09.35	CB 3881	Southampton	Depart.	10.00
09.40	AZ 107	Rome	Depart.	10.35
09.40	K8 2000	Curacao	Depart.	10.35
09.45	KL 1575	Athene	Depart.	10.04
09.45	KQ 0575	Athene	Depart.	10.04
09.45	UK 2073	Edinburgh	Depart.	09.58
09.45	KL 2073	Edinburgh	Depart.	09.58
09.45	NW 4973	Edinburgh	Depart.	09.58
09.50	BD 202	Eastmidlands	Depart.	10.07
09.55	KL 1363	Warschau	Depart.	10.00
09.55	NW 8363	Warschau	Depart.	10.00
09.55	KL 1957	Zurich	Depart.	09.59
09.55	NW 8319	Zurich	Depart.	09.59
10.00	BA 8112	Londen Gatw	Depart.	09.59
10.00	KL 1871	Stuttgart	Depart.	10.04
10.00	NW 3791	Stuttgart	Depart.	10.04
10.00	KL 1109	Stockholm	Depart.	10.24

Figure 3 TALIS architecture

3 Air transport safety standards

For the various systems and services depicted in figure 3 different safety standards apply, some of which are discussed below.

3.1 Airborne software safety standard DO-178B

For all software in an aircraft DO-178B [7] 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.

Table 1: DO-178B/ED12B overview

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	-

DO-178B provides up to 66 detailed requirements, with all required for level A. 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 the IT industry, which is the reason several real-time operating systems vendors are certifying their products according to this standard [6]. This reduces the amount of software needed for an application while increasing the choice of target hardware.

Figure 4 provides an overview of DO-178B software development and certification process. DO-178B defines an abstract software lifecycle. 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 authority prior to actual software development. Subsequently, the developer needs only to comply with the agreed PSAC. Optional industry standards define the functions that must exist in certain avionics units (e.g., flight management system).

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.

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.

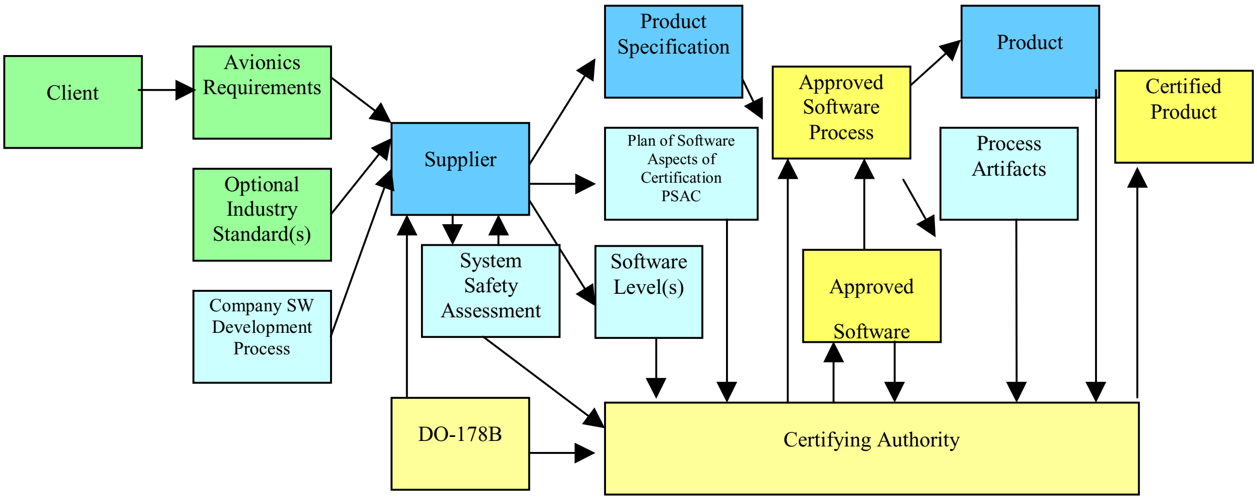


Figure 4: Overview of airborne software safety standard DO-178B

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 [8]. Substantial benefits can be accrued when each nation accepts the certifications of all accredited ICAO member states. A system of accreditation should enforce the standard equally 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 can not statistically justify compliance to DO-178B requirements. Like all other software safety standards, evidence on the utility and effectiveness of each of the 66 DO-178B requirements is lacking. They are based on a consensus on engineering judgement.

3.2 US Air Traffic Management standard DO-278/ED109

For Air Traffic Management (ATM) ground (and satellite) systems, the USA has extended DO-178B into a new standard DO-278 [9]. 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.

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 no failure may occur for a continuous period of 8760 hours of representative use. 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.

Table 2: DO-278/ED109 overview

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

3.3 EUROCONTROL draft Air Traffic Management standard

The European Organisation for the Safety of Air Navigation (EUROCONTROL) has set up a safety management software ad hoc task group under the European Air Traffic Management Programme (EATMP). Based on the EUROCONTROL Safety Regulatory Requirement ESARR 4 [10], the task group is drafting a software standard. This, as yet unnamed, standard will combine DO-178B, IEC 61508, and the Capability Maturity Model [13] into a combined safety and quality assurance document. The software classification provided in Table 3 has not yet been fixed. The Standard is based on ESARR4, 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 covers operational use and maintenance phases, an extension to DO-178B.

Table 3: EUROCONTROL EATMP software assurance level

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

3.4 Electronic flight bag AC 120-76

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 FAA AC120-76 [11] 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 is classified as a:

- Class 1 portable COTS device without data link connectivity to the aircraft and not connected to the aircraft power system or an aircraft mount;
- Class 2 portable COTS device mounted to the aircraft, can connect read-only to the aircraft data link and can connect to Airline Operational Control (AOC) information in receive/transmit mode;
- Class 3 installed equipment and consequently DO-178B applies in full.

For Class 1 and 2 equipment DO-178B compliance is not required. To illustrate the usefulness of Class 1 and 2, AC120-76 lists sixty-four sample applications for Class 1 and seventeen for Class 2. Class 2 mentions Internet connectivity, but for data only. Consequently a key TALIS requirement like uploading Java applets is prohibited.

Compliance to AC120-76 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. Even within AC120-76, 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 a specific period of time. This profusion of standards, regulations, etc, is typical for integrated systems like TALIS.

The four discussed standards, which are not harmonised and could have different national interpretations, support the conclusion in [2] that innovation in certification is needed. Although [2] proposes a shift to process versus current product standards, more objective evidence on the relevance of the provided test evidence with respect to the safety claims is needed.

4 Security certification

After the tragic September 11 (2001) events security has become even more of a concern for air transport. Especially network-enabled systems, like TALIS, are vulnerable to attacks and hence need protection. The ISO-15408 [12] is an international standard that includes security requirements and can provide certifications for complying products. 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 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).

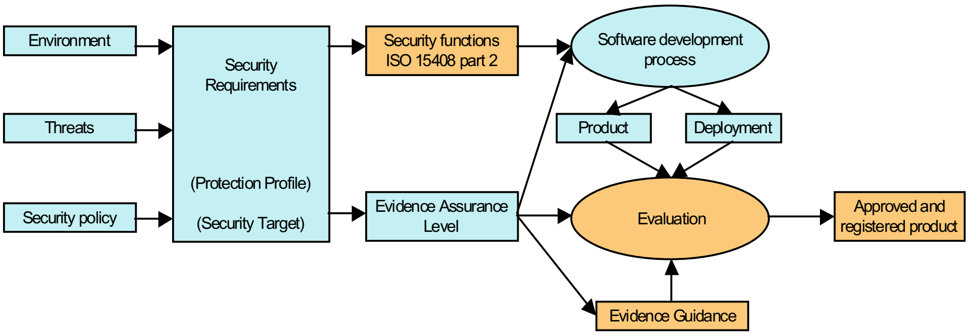


Figure 5 Overview of security standard ISO 15408

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 the security functions of the system are chosen from the extensive listing of possible security functions in the ISO-15408 Part 2. Separately the protection level is determined, which determines the amount of implementation effort and evaluation effort. Table 4 provides an overview of the Evaluation Assurance Levels (EALs). The amount of COTS products in the register at the time of writing (May 2003) illustrates that ISO-15408 is rapidly being accepted.

Table 4: ISO 15408 Evaluation Assurance Level and number of complying COTS products

EAL	**Description**	**# of COTS products**	
		Certified	In evaluation
1	Functionally tested, security threats not serious	11	0
2	Structurally tested, low to moderate assurance	19	13
3	Methodically tested and checked, maximum assurance without infringing sound development practise	16	2
4	Methodically designed, tested and reviewed, maximum assurance compatible with good commercial practise	40	20
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	87	35

ISO-15408 adds further requirements on the software development process, so harmonisation with the safety requirements is advantageous. As air transport does not have a tradition is software security certification, it can benefit of the military and commercial domains through this more advanced standard.

5 Conclusions

- A century after the first powered flight, air transport is in need of major improvements. Both Europe (Vision 2020) and the US (Anyone, anytime, anywhere, anywhere) have set ambitious targets for capacity, safety, environmental issues and flexibility (reduced time-to-market). To achieve these goals IT is a key enabling technology.
- By deploying the concurrent enterprise concepts and the supporting COTS technology, the TALIS prototype has demonstrated the technical viability of an IT infrastructure for seamless ATM involving all actors integrated into a multimodal transport system.
- For non-critical services TALIS has shown the time-to-market can be reduced to a year by deploying IT innovations like COTS, component technology, connector technology. To achieve the week/month timeframe further innovation is needed.
- For critical services certification is a major obstacle to achieve the required time-to-market. The various non-harmonised safety standards compound these problems, as do national re-certification requirements. Objective evidence linking safety requirements and provided evidence is needed.
- For security COTS products complemented by an internationally recognised certification scheme offer an affordable promise to improve air transport.

References

[1] Report of the group of personalities, European Aeronautics: A vision for 2020, (January 2001), http://europa.eu.int/comm/research/growth/aeronautics2020/pdf/aeronautics2020_en.pdf

[2] Commission on the future of the US aerospace industry, Anyone, anything, anytime, anywhere, (December 2002), http://www.asme.org/gric/engineeringpolicy/Images/piscopo.pdf

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

[4] Ernst Kesseler, R. Grosmann, R. Ehrmanntraut, Integrating navigation and communication systems for innovative services, (2002 May 27/29), 9th St. Petersburg International conference on integrated navigation systems

[5] Open Group certifiable real-time Java, (June 2003), http://www.opengroup.org/rtforum/rt_java

[6] J. Ganssle, A battle for hearts and minds, (May 2003), Embedded systems programming

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

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

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

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

[11] FAA AC120-76, Guidelines for the certification, airworthiness and operational approval of electronic flight bag computing devices, (September 2002), FAA AC120-76

[12] ISO/IEC 15408, Information technology, Security techniques, Evaluation criteria for IT security, (August 1999), http://www.commoncriteria.org/cc/cc.html

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

Acronyms

AL	Assurance Levels
AOC	Airline Operations Centre
ATM	Air Traffic Management
CDA	Continuous Descent Approach
COOPATS	Co-operative Air Traffic Services
COTS	Commercial Off-The-Shelf
DAG-TM	Distributed Air-Ground Traffic Management
EAL	Evaluation Assurance Level
EATMP	European Air Traffic Management Programme
ESARR	EUROCONTROL Safety Regulatory Requirement ESARR 4
EUROCONTROL	European Organisation for the Safety of Air Navigation
FAA	Federal Aviation Administration
JAA	Joint Aviation Authority
PSAC	Plan of Software Aspects of Certification
IT	Information Technology
PP	Protection Profile
ST	Security Target
TALIS	Total Information Sharing for Pilot Situational Awareness Enhanced by Intelligent Systems

Acknowledgement

This work has been partly 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.