International Journal of Engineering Business Management
Special Issue: The Next Generation of Aircraft Servicing
and Logistics Operations – Opportunities and Challenges

OPEN ACCESS
ARTICLE

A Methodology to Integrate Security and Cost-effectiveness in ATM

Regular Paper

Francesca Matarese[1,*], Patrizia Montefusco[1], José Neves[2] and André Rocha[2]

1 SESM Scarl, A Finmeccanica Company, Italy
2 GMV SKYSOFT, Portugal
* Corresponding author E-mail: fmatarese@sesm.it

Received 11 April 2013; Accepted 1 September 2013

DOI: 10.5772/56958

Abstract The objective of this paper is the definition of a new methodology for carrying out security risk assessment in the air traffic management (ATM) domain so as to enhance security awareness and integrate secure and cost-effective design objectives.
This process is carried out by modelling the system, identifying the assets, threats and vulnerabilities, prioritizing the threats and proposing cost-effective countermeasures for the weaknesses found.
ATM security is concerned with securing ATM assets in order to prevent threats and limit their effects on the overall aviation network. This effect limitation can be achieved by removing the vulnerability from the system and/or increasing the tolerance in case of component failures due to attacks.
The security risk assessment methodology proposed is based on what is currently being done by the industry (the International Civil Aviation Organization (ICAO) and the International Standard Organization (ISO), etc.).

Keywords Security, Risk, Methodology, ATM

1. Introduction

Concerns about security have been raised in the past, but the tragic events of 9/11 thrust the issue of security into public domain as never before and set in motion responses that are re-shaping transportation in unforeseen ways.

Physical security of airports has been the focus of security concerns for many decades. Hijacking aircraft came to the fore in the 1970s, when terrorist groups in the Middle East exploited the lack of security to commandeer planes for ransom and publicity. Refugees fleeing dictatorships also saw the taking over of aircraft as a possible route to freedom. In response, the airline industry and the international regulatory body, the ICAO, established screening procedures for passengers and bags. This process seems to have worked in the short-run, at least, with reductions in hijackings, although terrorists changed their tactics by placing bombs in un-accompanied luggage and packages (as for example in the Air India crash off Ireland in 1985 and the Lockerbie, Scotland, crash of Pan Am 103 in 1988).

Because passengers were being routed by hubs, the numbers of passengers in transit through the hub airports grew significantly. Concerns were being raised by some security experts, but the costs of improving screening and the need to process ever larger numbers of passengers and maintain flight schedules caused most carriers to oppose tighter security measures.

The situation was changed irrevocably by the events of September 11, 2001. Security involves many steps, from restricting access to airport facilities and fortifying cockpits, to the more extensive security screening of passengers. Screening now involves more rigorous inspections of passengers and their baggage at airports. The imposition of these measures has come at a considerable cost. The purchase of improved screening machines and the re-designing of airport security procedures have been important cost additions. These measures have also had a major influence on passenger throughputs. Clearing security has become the most important source of delays in the passenger boarding process. Security issues have had a negative effect on the air transport industry, as costs have increased with delays and inconveniences to passengers increasing as well. [1]

In addition, cyber security[1] has become an issue for many civil aviation organizations, because they rely on electronic systems for critical parts of their operations, and for many organizations their electronic systems have safety-critical functions.

There are a number of reasons why the risks to civil aviation from malicious cyber activity are increasing, though principally because:

- Much of the new IT technology being introduced raises potential security issues that are unfamiliar in the civil aviation industry; and
- IT systems are becoming increasingly interconnected and interdependent, so organizations are exposed to risks caused by security weaknesses in other people's systems.

Today, air traffic is controlled using instructions issued from the ground by radio, with aircraft position determined by radar, and things have not substantially changed for 70 years. With increasing air traffic, today's ATM system is beginning to hit its physical limits, particularly in terms of the number of aircraft that can be managed by human controllers within a given airspace. The industry has designed solutions to automate the routine part of ATM, which if put into place would greatly increase the number of aircraft that can be managed within a given airspace. This would leave the air traffic controller with the executive role rather than having to issue all the routine control instructions, which would be produced automatically by the system.

The expected widespread use of unmanned aerial vehicles (UAVs) in the near future also raises new issues due to the increased importance of remote linkages and ground control stations.

These and other air traffic control issues are being addressed by the introduction of new communication methods and technologies, which includes the use of internet-based solutions. The use of these increases the role of cyber security and exposes numerous vulnerabilities that do not exist in today's more closed, proprietary, civil aviation systems. These cyber security vulnerabilities have the potential to jeopardize civil aviation safety and efficiency. [2]

In this complex scenario, it is crucial to be aware of the interaction between security, safety and cost-effectiveness.

The setting and implementation of security measures come at a cost that must be assumed by ATM operators and, eventually, by costumers. It has been estimated that an increase of 1% in the costs of air transport would cause a decrease in flows within the range of 2% to 3%. However, security-based measures could increase total costs between 1% and 3%.

Since the early 1990s, cost-effectiveness has become an increasing priority. However, since the terrorist attacks of September 11, 2001, people have been paying more attention to facility security and safety issues. Security measures, such as those for anti-terrorism, must be considered not only with regard to the level of protection deemed appropriate, but also while emphasizing the integrated design process, identifying areas of synergy and potential conflicts between safety and security approaches, and highlighting cost-effectiveness opportunities within certain security and safety strategies. Given budgetary and other constraints, integrating secure/safe and cost-effective design objectives oftentimes requires compromise and trade-offs. [3]

DORATHEA (Development Of a Risk Assessment meTHodology to Enhance security Awareness in ATM) is a research project co-funded by the European Commission Directorate-General of Home Affairs, in the frame of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme, with the aim of developing a common

[1] The protection of electronic systems from malicious electronic attack and dealing with the consequences of such attacks is encompassed by the term 'cyber security'. It comprises managerial and technical activities, and relates to the electronic systems themselves and to the information held and processed by such systems.

methodology for carrying out risk, threat and vulnerability assessments for ATM protection. It is envisaged that only a common methodology can provide the necessary basis for a coherent implementation of measures to protect European ATM critical infrastructure and clearly define the respective responsibilities of all relevant stakeholders.

DORATHEA aims at increasing the awareness of ATM operators through an innovative security risk assessment methodology for ATM systems that:

- Can be adopted either by state-of-the-art ATM systems as well as legacy/proprietary systems, allowing for the assessment of the new risks that their interconnection may (and, indeed, will) introduce.
- Is based on existing and well-established security standards already in use by the industry, including the ICAO [7], the CC [8] and the ISO 27005 [9], and extend them to cover the ATM security scenario.
- Is complementary with the risk assessment methodology currently being developed within SESAR and other EU projects in ATM security.

2. The Need for a DORATHEA Security Risk Assessment Methodology

Recent vulnerabilities that have been discovered and attacks that have been executed (e.g., refer to [4]) prove that the security of ATM systems is always under the spotlight, which is also confirmed by public entities (e.g., refer to [5]). Furthermore, the increasing complexity of ATM systems due to the pervasiveness of emerging technologies and the growing number of daily flights creates the conditions for the rise of unpredicted threats that may, potentially, turn into dramatic events. This is also driven by the on-going update of legacy/proprietary systems with new technologies and their connection to innovative systems, which creates a new environment with new threat vectors, for which these systems were not prepared when they were designed. As such, given that the ATM plays a critical role in supporting the overall airspace/aviation system, the security risk assessment of ATM should be a major concern and a top priority.

Presently, the ICAO Security Manual for Safeguarding Civil Aviation, one of the main references for threat and risk assessment in the ATM domain, offers little help in identifying and prioritizing threats according to time and budget constraints. On the other side, new guidelines are on the way, such as those currently being developed in the Sub-work Package (SWP) 16.2 of the Single European Sky ATM Research (SESAR) project, which focuses on ATM security frameworks, methodologies, tools and best practices.

The proposed methodology is an extension of the ICAO ATM security guidelines and is based on the strong points of the Safety Assessment Methodology defined by EUROCONTROL.

It comprises three phases (see Figure 1):

- **SecFHA (Security Functional Hazard Assessment)** aims at evaluating how secure the system needs to be in order to achieve a tolerable risk. It is a process that, by evaluating system functionalities, identifying potential security hazards and assessing the consequences of their occurrence for the system, produces the system security objectives.
  Therefore, SecFHA inputs comprise the system functionalities, while knowledge about security hazards' consequences and SecFHA outputs are the security objectives of the system.
- **PSSecA (Preliminary System Security Assessment)** aims at evaluating whether the proposed architecture is expected to achieve a tolerable risk. It is a process that produces system requirements related to security (security requirements) in order to satisfy all the security objectives defined in SecFHA process.
- **SSecA (System Security Assessment)** is a process to demonstrate that the system as implemented achieves a tolerable risk (i.e., satisfies the security objectives identified in the SecFHA) and that the system elements meet the security requirements specified in the PSSecA.

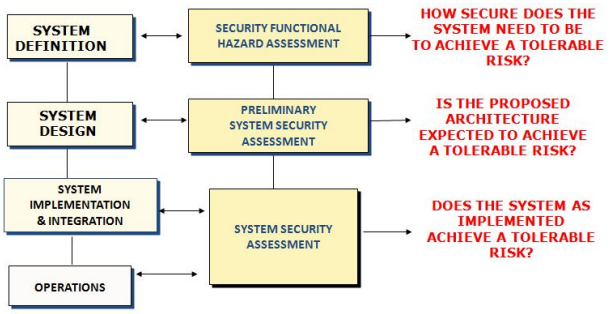

Figure 1. DORATHEA Security Risk Assessment Methodology Overview

2.1 Security Functional Hazard Assessment (SecFHA)

SecFHA is a top-down iterative process, starting at the beginning of the development or modification of an air navigation system and which aims to *determine how secure the system needs to be.*

The steps to be performed during the SecFHA are:

- To identify all potential security hazards associated with the system;
- To identify security hazard effects on system functionalities;

- To assess the impact of security hazard effects;
- To derive a security objective, in terms of maximum tolerable likelihood of occurrence of a security hazard.

2.1.1 Identification of all Potential Security Hazards

The identification of all potential security hazards is performed through the:

1. Identification of all the functionalities that the system under evaluation is expected to provide;
2. Definition of a sub-set of functionalities containing only those system functionalities that are relevant from a security point of view (i.e., the functionalities that have to be protected).
   The selection of these functionalities will take into account:
   - How critical the functionality is from a security point of view (i.e., the loss or the corruption of such functionality due to an attack would have a high impact on people, equipment and procedures).
   - How "attractive" the functionality is from an attacker's point of view: an attacker could decide to attack a functionality on the basis of the effort needed to perform the attack in terms of costs, the time needed to prepare the attack, the skills required to achieve the attack, the equipment required to be able to perform the attack, and the likelihood of being identified during the attack.
3. Definition of all the potential security hazards as any condition, event or circumstance that could lead to the loss or corruption of such functionalities.

2.1.2 Identification of a Security Hazard's Impact

All the possible consequences of the security hazard on the system will be identified and the impact of these consequences will be established.

This impact is represented by a number from 1 to 5, as reported in Table 1. To obtain this evaluation, the impact of the security hazard's effect(s) must be evaluated on each of the SESAR security impact areas (refer to [6]). A comparison should not be made between impact areas - they should be evaluated independently.

The final impact value for each security hazard's effect will be the maximum impact level from this evaluation.

2.1.3 Security Objectives' Identification

The security objective specifies, for each identified security hazard, the maximum tolerable likelihood of its occurrence, given its assessed impact.
In particular, it will be linked to the likelihood of a loss or corruption of functionality due to an attack.

For each identified security hazard, the security risk associated with it will be evaluated as follows:

$$\textbf{\textit{Security Risk}} = L_{sh} * I_c \quad (1)$$

	5	4	3	2	1
Impact Areas	**Catastrophic**	**Critical**	**Severe**	**Minor**	**No impact / NA**
IA1: Personnel	Fatalities	Multiple severe injuries	Severe injuries	Minor injuries	No injuries
IA2: Capacity	Loss of 60%-100% capacity	Loss of 60%-30% capacity	Loss of 30%-10% capacity	Loss of up to 10% capacity	No capacity loss
IA3: Performance	Major quality abuse that makes multiple major systems inoperable	Major quality abuse that makes the major system inoperable	Severe quality abuse that makes systems partially inoperable	Minor system quality abuse	No quality abuse
IA4: Economic	Bankruptcy or loss of all income	Serious loss of income	Large loss of income	Minor loss of income	No effect
IA5: Branding	Government and international attention	National attention	Complaints and local attention	Minor complaints	No impact
IA6: Regulatory	Multiple major regulatory infractions	Major regulatory infraction	Multiple minor regulatory infractions	Minor regulatory infraction	No impact
IA7: Environment	Widespread or catastrophic impact on the environment	Severe pollution with a long-term impact on the environment	Severe pollution with a noticeable impact on the environment	Short-term impact on the environment	Insignificant

Table 1. SESAR Security Impact Areas

		LIKELIHOOD OF OCCURRENCE				
		5 Extremely Rare	4 Rare	3 Occasional	2 Frequent	1 Very Frequent
IMPACT CLASSES	5 Catastrophic					
	4 Critical					
	3 Severe					
	2 Minor					
	1 No impact					
		Acceptable		Tolerable		Unacceptable

Table 2. Risk Classification Scheme in ATM

Where:

- L_{sh} indicates the likelihood of a given security hazard;
- I_c indicates the impact of the consequence of the vulnerability on the security of the system (people, procedures, equipment).

The Risk Classification Scheme (see [6]) is used in order to fix the maximum tolerable likelihood of a given security hazard, given its assessed Impact, in order to achieve a ***tolerable risk***.

The likelihood of an attack is defined as follows:

- **Very Frequent:** likely to occur often;
- **Frequent:** likely to occur several times;
- **Occasional:** likely to occur sometimes;
- **Rare:** unlikely but which may occur exceptionally;
- **Extremely Rare:** unlikely to occur during the lifetime of the system.

2.2 Preliminary System Security Assessment (PSSecA)

The objective of the PSSecA process is to evaluate *whether the proposed architecture is expected to achieve a tolerable risk.*

PSSecA is a top-down iterative process, conducted during the system design phase of the system lifecycle. A PSSecA should be performed for a new system or else each time there is a change to the design of an existing system. In the second case, the purpose of PSSecA is to identify the impact of such a change on the architecture and to ensure the ability of the new architecture to meet either the same or new security objectives.

The essential pre-requisite for conducting a PSSecA is a description of the high level functions of the system.

This phase aims at deriving the security requirements for each individual system element under evaluation (people, procedure and equipment) in order to satisfy the security objective of the system.

The system architecture can only achieve the security objectives established during the SecFHA, provided that the architecture elements meet their security requirements.

The PSSecA starts with the identification of all the assets that provide the functionalities associated with the security objectives identified during the SecFHA.

According to [6], the assets will be classified as:

- Primary assets: these are the intangible activities, information and services that contribute to having the functionalities of the system to be protected (i.e., those specified in the security objectives).
- Supporting assets: these are the physical entities that enable the primary assets.

They can consist of various types, including, for example, hardware, software, operating systems, business applications, networks, storage media, relays, communication interfaces, personnel, sites, premises, utilities, subcontractors, authorities and organizations.

A security objective is satisfied if the primary assets that provide the functionalities associated with it are protected.

The primary assets are protected if, and only if, the supporting assets supporting them are not attackable.

Next, the apportionment of security objectives into security requirements allocated to the system elements is performed through two analyses:

- **Attack Tree Analysis (ATA):** this is a functional analysis that that identifies the logical combination of consequences arising from attacks, leading to the non-fulfilment of the security objectives. The focus is on the consequences for primary assets. The output of this analysis will be the list of attacks that can impact a given security objective (linked

to one or more primary asset) with an assigned likelihood.

- **Identification of Vulnerability and Effects Analysis (IVEA):** this is a physical analysis and aims at evaluating whether the supporting assets linked to a given security objective are vulnerable to the identified threats.

The combination of ATA and IVEA analyses allows the identification of how critical the supporting assets are and, consequently, enables the definition of the security controls in a cost-effective way. The security controls will be traced to those system requirements that will become security requirements.

Figure 2 gives an overview of the PSSecA process.

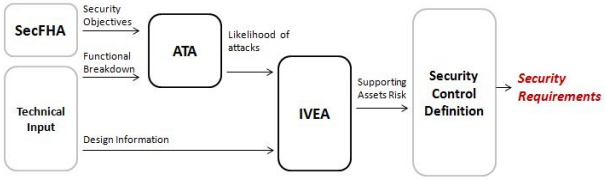

Figure 2. PSSecA Overview

2.2.1 Attack Tree Analysis (ATA)

The ATA is a functional analysis that identifies the logical combination of consequences arising from attacks and leading to the non-fulfilment of the security objectives.

The focus is on the consequences for primary assets. Starting from the likelihood of the security objective (the top event), the attack tree analysis allows for the identification of the likelihood that an attack will successfully lead to the non-fulfilment of the security objective. If an attack is associated with two different values of likelihood, the most stringent value is considered.

2.2.2 Identification of Vulnerability and Effects Analysis (IVEA)

IVEA is performed on the physical components. The objective of this analysis is to identify the system vulnerabilities, evaluate how an attacker can use them (i.e., a threat that exploits the vulnerability), and what the consequences of such an attack are.

The input of this analysis will be the design information of the system that allows for the establishment of which supporting assets support the primary assets that provide for the functionality associated with a given security objective. The analysis follows the following steps:

1. The list of supporting assets is considered;
2. The vulnerabilities of these supporting assets are identified;
3. The list of potential threats is considered;
4. Each threat in (3) will be traced to the supporting assets in (2) if they are vulnerable to it (i.e., if the threat can exploit the vulnerability of the supporting asset);
5. The effect of the threat will be evaluated (in order to identify the primary asset affected by it).

The IVEA will be in table format:

2.3 System Security Assessment (SSecA)

System security assessment is the last phase of the methodology.

This phase aims at evaluating *whether the implemented architecture achieves a tolerable risk.*

SSecA is a top-down iterative process led during system integration, validation and on-site acceptance.

The process produces assurance that the security objectives are satisfied and that the system elements meet their security requirements.

Supporting Asset	Vulnerability	Threat	Effect(s)	Likelihood	Security Controls	Likelihood after mitigation
Name of the physical component	Vulnerability of the supporting asset	Threat that exploits the vulnerability of the supporting asset	The consequences are related to the impact on the primary asset(s), supported by the associated physical component, as identified through ATA	Likelihood associated to the effect on the primary asset, as identified through ATA	Possible measures to be applied to the supporting asset in order to mitigate the risk	The resulting likelihood after the application of the security controls

Table 3. IVEA

The objective of the SSecA is to collect evidence and to provide assurance that:

- Each system (people, procedure, equipment) element as implemented meets its security requirements;
- The system as implemented satisfies its security objectives throughout its operational lifetime (until decommissioning);
- The system satisfies users' expectations with respect to security;
- The system achieves a tolerable risk.

The correct implementation of the security controls will be demonstrated through:

- Verification and validation activities.

3. Case Study Application: Controller-Pilot Data Link Communications

The Air Ground Datalink (AGDL) communication system has been selected to validate the proposed methodology. In particular, the controller-pilot data link communications (CPDLC) application provides a means of communication between the controller and the pilot, using a data link for ATC communication. As such, CPDLC is a means of digital communication between aircraft and ATCO, allowing for data exchange in a digital text format.

There are two types of CPDLC messages:

- Downlink messages, which are CPDLC messages sent from the aircraft;
- Uplink messages, which are CPDLC messages sent from a ground system.

The CPDLC application is used by the following services [10]:

- **ATC Communication Management (ACM)** service provides automated assistance to the aircrew and current and successive controllers in conducting the transfer of ATC communications. The ACM service encompasses the transfer of all controller/aircrew communications, - both the voice channel and the data communications channel used to accomplish the ACM service. The ACM service is completed prior to using any other CPDLC service.
- **ATC Clearance (ACL)** for exchanging clearances and requests between the current data authority ATSU and flight crew. An aircraft under the control of an ATSU transmits reports, makes requests and receives clearances, instructions and notifications. The ACL service describes the dialogue procedures to be followed to perform these exchanges via air/ground data communications. The service description states the exchanges that can be conducted via data communications, the rules for the combination of voice and data link communications, and any abnormal mode requirements and procedures.
- **ATC Microphone Check (AMC)** for instructing pilots to check that the aircraft is not blocking a given voice channel. The AMC service allows a controller to send an instruction to all CPDLC-equipped aircraft in a given sector at the same time in order to instruct flight crews to verify that their voice communication equipment is not blocking the sector's voice channel. This instruction will be issued only to those aircraft for which the controller currently has responsibility.
- **Departure Clearances (DCL)** for exchanging departure clearance, request and start-up messages between the current ATSU and grounded aircraft to prepare for its departure. Where local procedures or a flight category require, flights intending to depart from an airport must first obtain a departure clearance from the C-ATSU. The process can only be accomplished if the flight operator has filed a flight plan with the appropriate ATM authority. The DCL service provides automated assistance for requesting and delivering departure information and clearance, with the objective of reducing aircrew and controller workloads and diminishing clearance delivery delays.

3.1 SecFHA

An analysis of CPDLC functionalities is performed in order to identify security hazards. According to the classification of effects, security objectives are identified:

Security Objectives	Description
SO-1	The likelihood of an out-of-sequence CPDLC message shall be less than occasional
SO-2	The likelihood of the denial of CPDLC services shall be less than extremely rare
SO-3	The likelihood of a loss of integrity of CPDLC messages' exchange shall be less than rare
SO-4	The likelihood of the theft of a CPDLC message shall be less than rare
SO-5	The likelihood of the reception of a fake CPDLC message shall be less than rare

Table 4. CPDLC Safety and Security Objectives

Supporting Assets	Vulnerability		s)	ood	ty Controls	Likelihood after mitigation
Controller Working Position (CWP)	Unsecured protection of integrity of data	Corruption of data	If the message is related to a clearance, the flight crew and ground are out of sync	Rare	Requirements for ensuring authenticity and protecting message integrity	Occasional
CWP	Lack of data validity checks	Corruption of data	If the message is related to a clearance, the flight crew and ground are out of sync	Rare	Automatic checks shall be incorporated to detect any corruption of information through processing errors due to deliberate acts	Occasional
Dual Data Link Server (DLS)	Unsecured protection of integrity of data	Corruption of data	uation will develop slowly: not all aircraft will receive corrupted messages and take action at the same time. ntroller will have time to deal with all impacted aircraft.	Rare	Requirements for ensuring authenticity and protecting message integrity	Occasional
DLS	Services running with unnecessary privileges	Corruption of data	The situation will develop slowly: not all aircraft will receive corrupted messages and take action at the same time. The controller will have time to deal with all impacted aircraft.	Rare	The allocation and use of privileges shall be restricted and controlled	Occasional

Table 5. IVEA example

3.2 PSSecA

ATA is performed in order to analyse those primary assets potentially affected by the identified safety and security objectives.

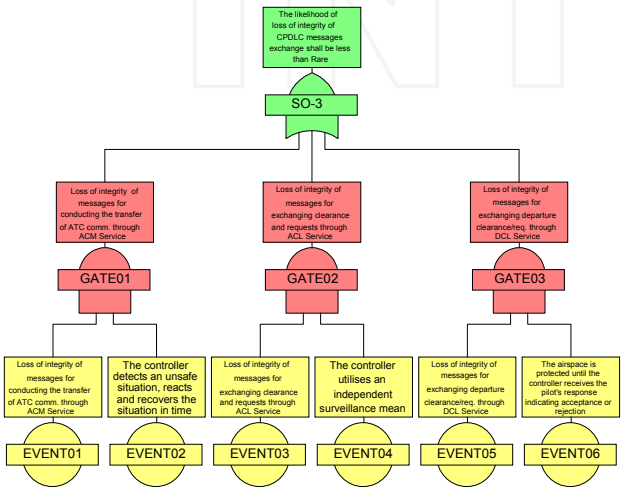

Figure 3. ATA example

IVEA is performed in order to analyse any supporting assets potentially affected by the identified safety and security objectives and to identify safety and security requirements.

4. Conclusions

The objective of this paper is the definition of a new methodology for carrying out security risk assessment in the ATM domain.

Countermeasures must be considered at the design phase, identifying areas of synergy and potential conflicts between safety and security approaches, and highlighting cost-effectiveness opportunities within certain security and safety strategies.

The proposed methodology allows for the identification of countermeasures in a systematic way. Countermeasures can be adopted as security system requirements at the design level.

For demonstrative purposes, the methodology has been applied to the real case study of an approach and landing flight phase scenario, with a special focus on controller-pilot data link communications systems.

5. Acknowledgments

The research leading to these results was carried out with the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-Related Risks Programme of the European Commission – Directorate-General of Home Affairs (Registration number HOME/2010/CIPS/AG/030, DORATHEA Project).

6. References

[1] Brian Slack, Jean-Paul Rodrigue, "Transport Security," 2012.
[2] UK Centre for the Protection of National Infrastructure (CPNI), "Cyber Security in Civil Aviation," 2012.
[3] Richard Paradis, Bambi Tran, "Balancing Security/Safety and Sustainability Objectives," National Institute of Building Sciences, 2010.
[4] Federal Aviation Administration, "Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems," U.S. Department of Transportation, 2009.
[5] SESAR Definition Phase Project, "D1 Air Transport Framework – The Current Situation," v3, SESAR Consortium, 2006.
[6] EUROCONTROL, Deliverable 16.02.03 – SESAR ATM Security Risk Assessment Method, Ed.01.01, SESAR WP16.2 ATM Security, 2013.
[7] ICAO, Security Manual for Safeguarding Civil Aviation against Acts of Unlawful Interference, Seventh Edition, 2010.
[8] IEC 15408, Information Technology – Security Technique – Evaluation Criteria for IT Security, 2005.
[9] IEC 27005, Information Technology — Security Techniques — Information Security Risk Management, Second Edition, 2011.
[10] ICAO, Manual of Air Traffic Services Data Link Applications, First Edition, 1999.

INTECH