Risk Assessment for Airworthiness Security

Silvia Gil Casals[1,2,3], Philippe Owezarski[1,3], Gilles Descargues[2]

[1]CNRS, LAAS, 7 avenue du colonel Roche, F-31400 Toulouse, France
{silvia.gil.casals, philippe.owezarski}@laas.fr
[2]THALES Avionics, 105 av. du General Eisenhower, F-31100 Toulouse, France
gilles.descargues@fr.thalesgroup.com
[3]Univ de Toulouse: INSA, LAAS, F-31400 Toulouse, France

Abstract. The era of digital avionics is opening a fabulous opportunity to improve aircraft operational functions, airline dispatch and service continuity. But arising vulnerabilities could be an open door to malicious attacks. Necessity for security protection on airborne systems has been officially recognized and new standards are actually under construction. In order to provide development assurance and countermeasures effectiveness evidence to certification authorities, security objectives and specifications must be clearly identified thanks to a security risk assessment process. This paper gives main characteristics for a security risk assessment methodology to be integrated in the early design of airborne systems development and compliant with airworthiness security standards.

Keywords: airworthiness, risk assessment, security, safety, avionic networks

1 Introduction

The increasing complexity of aircraft networked systems exposes them to three adverse effects likely to erode flight safety margins: intrinsic component failures, design or development errors and misuse. Safety[1] processes have been capitalizing on experience to counter such effects and standards were issued to provide guidelines for safety assessment process and development assurance such as ARP-4754 [1], ARP-4761 [2], DO-178B [3] and DO-254 [4]. But safety-critical systems segregation from the Open World tends to become thinner due to the high integration level of airborne networks: use of Commercial Off-The-Shelf equipments (COTS), Internet access for passengers as part of the new In-Flight Entertainment (IFE) services, transition from Line Replaceable Units to field loadable software, evolution from voice-ground-based to datalink satellite-based communications, more autonomous navigation with e-Enabled aircrafts, etc. Most of the challenging innovations to offer new services, ease

[1] Please note that safety deals with intrinsic failures of a system or a component (due to ageing or design errors) whereas security deals with the external threats that could cause such failures. Security being a brand new field in aeronautics, instead of building a process from scratch, the industry is trying to approximate to the well-known safety process, which has reached a certain level of maturity through its 50 years of experience.

air traffic management, reduce development and maintenance time and costs, are not security-compatible. They add a fourth adverse effect, increasingly worrying certification authorities: vulnerability to deliberate or accidental attacks (e.g. worms or viruses propagation, loading of corrupted software, unauthorized access to aircraft system interfaces, on-board systems denial of service). De Cerchio and Riley quote in [5] a short list of registered cyber security incidents in the aviation domain. As a matter of fact, EUROCAE[2] and RTCA[3] are defining new airworthiness security standards: ED-202 [6] provides guidance to achieve security compliance objectives based on future ED-203[4] [7] methods.

EU and US[5] certification authorities are addressing requests to aircraft manufacturers so they start dealing with security issues. However, ED-203 has not been officially issued and existing risk assessment methods are not directly applicable to the aeronautical context: stakes and scales are not adapted, they are often qualitative and depend on security managers expertise. Also, an important stake in aeronautics is costs minimization. On the one hand, if security is handled after systems have been implemented, modifications to insert security countermeasures, re-development and re-certification costs are overwhelming: "fail-first patch-later" [8] IT security policies are not compatible with aeronautic constraints. It is compulsory that risk assessment is introduced at an early design step of development process. On the other hand, security over-design must be avoided to reduce unnecessary development costs: risk needs to be quantified in order to rank what has to be protected in priority.

This paper introduces a simple quantitative risk assessment framework which is: compliant with ED-202 standard, suitable to the aeronautics, adaptable to different points of view (e.g. at aircraft level for airframer, at system level for system provider) and taking into account safety issues. This methodology is in strong interaction with safety and development processes. Its main advantage is to allow the identification of risks at an early design step of development V-cycle so that countermeasures are consistently specified before systems implementation. It provides means to justify the adequacy of countermeasures to be implemented in front of certification authorities.

Next chapter gives an overview of risk assessment methods; third one, depicts our six-step risk assessment framework, illustrated by a simple study case in chapter 4; last one concludes on pros and cons of our method and enlarges to future objectives.

2 About Risk Assessment Methods

Many risk assessment methodologies aim at providing tools to comply with ISO security norms such as: ISO/IEC:27000, 31000, 17799, 13335, 15443, 7498, 73 and 15408 (Common Criteria [9]). For example, MAGERIT [10] and CRAMM [11] deal with governmental risk management of IT against for example privacy violation.

---

2 European Organization for Civil Aviation Equipment

3 Radio Technical Commission for Aeronautics

4 ED-203 is still under construction, we refer to the working draft which content may be prone to change.

5 Respectively EASA (European Aviation Safety Agency) and FAA (Federal Aviation Administration)

NIST800-30 [12] provides security management steps to fit into the system development life-cycle of IT devices. Others, such as OCTAVE [13] aim at ensuring enterprise security by evaluating risk to avoid financial losses and brand reputation damage. Previously stated methods are qualitative, i.e. no scale is given to compare identified risks between them. MEHARI [14] proposes a set of checklists and evaluation grids to estimate natural exposure levels and impact on business. Finally, EBIOS [15] shows an interesting evaluation of risks through the quantitative characterization of a wide spectrum of threat sources (from espionage to natural disasters) but scales of proposed attributes do not suit to the aeronautic domain.

Risk is commonly defined as the product of three factors: *Risk* = *Threat* × *Vulnerability* × *Consequence*. Quantitative risk estimations combine these factors with more or less sophisticated models (e.g. a probabilistic method of risk prediction based on fuzzy logic and Petri Nets [16] vs. a visual representation of threats under a pyramidal form [17]). Ortalo, Deswarte and Kaaniche [18] defined a mathematical model based on Markovian chains to define METF (Mean Effort to security Failure), a security equivalent of MTBF (Mean Time Between Failure). Contrary to the failure rate used in safety, determined by experience feedback and fatigue testing on components, security parameters are not physically measurable. To avoid subjective analysis, Mahmoud, Larrieu and Pirovano [19] developed an interesting quantitative algorithm based on computation of risk propagation through each node of a network. Some of the parameters necessary for risk level determination are computed by using network vulnerability scanning. This method is useful for an a posteriori evaluation, but it is not adapted to an early design process as the system must have been implemented or at least emulated.

3 Risk Assessment Methodology Steps

Ideally, a security assessment should guarantee that all potential scenarios have been exhaustively considered. They are useful to express needed protection means and to set security tests for final products. This part describes our six-steps risk assessment methodology summarized in Figure 1, with a dual threat scenario identification inspired on safety tools and an adaptable risk estimation method.

3.1 Step 1: Context Establishment

First of all, a precise overview of the security perimeter is required to focus the analysis, avoid over-design and define roles and responsibilities. Some of the input elements of a risk analysis should be:

- security point of view (security for safety, branding, privacy, etc.),
- depth of the analysis (aircraft level, avionics suite level, system or item level),
- operational use cases (flight phases, maintenance operations),
- functional perimeter,
- architecture perimeter (if available),
- assumptions concerning the environment and users,

- initial security countermeasures (if applicable),
- interfaces and interactions,
- external dependencies and agreements.

A graphical representation (e.g. UML) can be used to gather perimeter information, highlight functional interfaces and interactions.

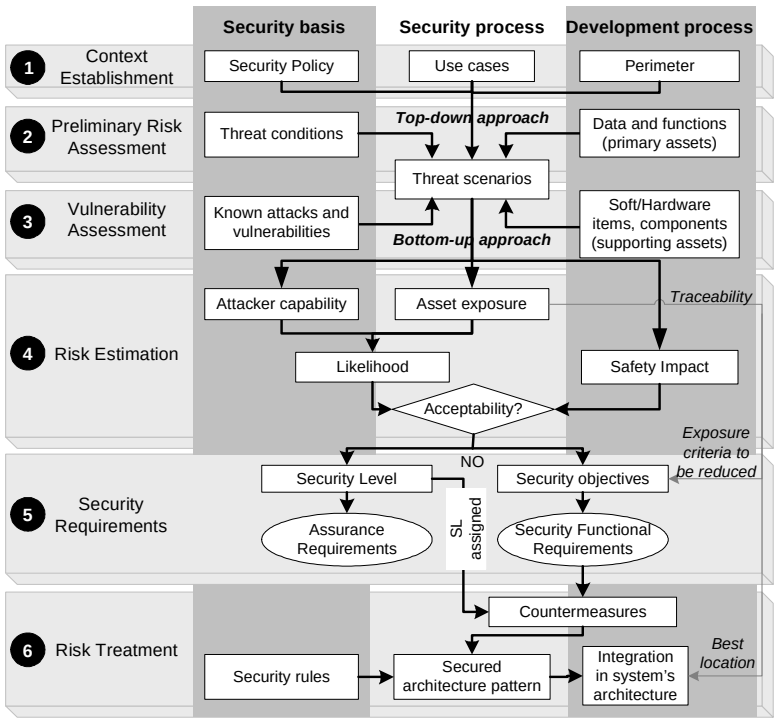

Fig. 1. Risk assessment and treatment process: the figure differentiates input data for the security process as coming either from the development process or from a security knowledge basis.

3.2 Step 2: Preliminary Risk Assessment (PRA)

PRA is an early design activity: its goal is to assess designers so they consider main security issues during the first steps of avionic suite architecture definition. Basically, it aims at identifying what has to be protected (assets) against what (threats).

Primary Assets. According to ED-202, assets are "those portions of the equipment which may be attacked with adverse effect on airworthiness". We distinguish two types of assets: primary assets (aircraft critical functions and data) that are performed or handled by supporting assets (software and hardware devices that carry and process primary assets). In PRA, system architecture is still undefined, only primary assets need to be identified.

Threats. Primary assets are confronted to a generic list of Threat Conditions (TCs) themselves leading to Failure Conditions (FCs). Examples of TCs include: misuse, confidentiality compromise, bypassing, tampering, denial, malware, redirection, subversion. FCs used in safety assessment are: erroneous, loss, delay, failure, mode change, unintended function, inability to reconfigure or disengage.

Top-down Scenarios Definition. Similarly, to safety deductive Fault Tree Analysis (FTA), the security PRA follows a top-down approach: parting from a feared event, all threat conditions leading to it are considered to deduce the potential attack or misuse causes deep into systems and sub-systems. Due to the similarities with Functional Hazard Analysis (FHA) made in safety process and as a matter of time and cost saving, this assessment could be common both to safety and security preliminary processes as they share the same FCs.

3.3 Step 3: Vulnerability Assessment

Supporting Assets. Once architecture has been defined and implementation choices are known, all supporting assets of a given primary asset can be identified. Supporting assets are the ones that will potentially receive countermeasures implementation.

Vulnerabilities. They are weaknesses exploited by attackers to get into a system. TC are associated to types of attacks and all known vulnerabilities are listed to establish a checklist. This vulnerability list is based on the public database CVE[6] (Common Vulnerabilities and Exposures), eventually completed by new vulnerabilities found by intrusion testing.

Bottom-up Scenarios Definition. Similarly to the safety inductive approach of Failure Mode and Effect Analysis (FMEA), the security vulnerability assessment is a bottom-up approach: it aims at identifying potential security vulnerabilities in supporting assets, particularly targeting human-machine and system-system interfaces. First with vulnerability checklists and then by testing, threat propagation paths must be followed to determine the consequences on sub-systems, systems and aircraft level of each item weakness exploitation.

To summarize, the top-down approach allows the identification of high-level security requirements. Whereas the bottom-up approach, allows validating and completing these requirements with technical constraints and effectiveness requirements, as well as identifying threats and vulnerabilities left unconsidered during the top-down analysis.

[6] http://cve.mitre.org/

3.4 Step 4: Risk Estimation

It would be impossible to handle all of identified scenarios. It is necessary to quantify their likelihood and safety impact, to determine whether risk is acceptable or not, and measure the effort to be provided to avoid the most likely and dangerous threats.

Likelihood. It is the qualitative estimation that an attack can be successful. ED-202 considers five likelihood levels: 'pV: frequent', 'pIV: probable', 'pIII: remote', 'pII: extremely remote', 'pI: extremely improbable'. As they are too subjective to be determined directly, we built Table 1 to determine likelihood by combining factors that characterize and quantify both attacker capability (A) and asset exposure to threats (E). Note that Table 1 is usable whatever the amount of attributes required, and whatever the number of values each attribute can take, i.e. this framework allows flexible evaluation criteria as they may vary according to the context (aircraft or system level, special environment conditions, threats evolution). However, these criteria must be defined with an accurate taxonomy so the evaluation is exhaustive, unambiguous and repeatable.

Table 1. Attack likelihood through attacker characteristics and asset exposure

		ATTACKER CAPABILITY SCORE				
		0 ≤ A ≤ 0,2	**0,2 < A ≤ 0,4**	**0,4 < A ≤ 0,6**	**0,6 < A ≤ 0,8**	**0,8 < A ≤ 1**
EXPOSURE	**0 ≤ E ≤ 0,2**	pI	pI	pII	pIII	pIV
	0,2 < E ≤ 0,4	pI	pI	pII	pIII	pIV
	0,4 < E ≤ 0,6	pII	pII	pIII	pIV	pV
	0,6 < E ≤ 0,8	pIII	pIII	pIV	pV	pV
	0,8 < E ≤ 1	pIV	pIV	pV	pV	pV

Let $X = \{X_1, \dots, X_n\}$ be a set of n qualitative attributes chosen to characterize the "attacker capability". For instance, $X = \{X_1$="elapsed time to lead the attack", X_2= "attacker expertise", X_3= "previous knowledge of the attacked system", X_4= "equipment used", X_5= "attacker location"$\}$. Each attribute X_i can take m values: $\{X_i^1, \dots, X_i^m\}$, X_i^j being more critical than X_i^{j-1}. E.g. X_1 can take the values: $\{X_1^1$=">day", X_1^2="<day", X_1^3="hours (by flight time)", X_1^4="minutes"$\}$. To each qualitative value X_i^j , we associate a quantitative value x_i^j with $x_i^j > x_i^{j-1}$. In the study case, let us set: x_1^1 =0, x_1^2=1, x_1^3=2 and x_1^4=3.

Let us call $f_j()$ the evaluation function performed by the security analyst to assign the corresponding value a_i to each X_i for a given threat scenario: $a_i = f_{j=1}^m(x_i^j)$. Attacker capability is expressed by the normalized sum of the values assigned to all attributes of set X (see equation 1). Exactly the same reasoning is made to express the "asset exposure".

$$A = \sum_{i=1}^{n} \left(\frac{a_i}{x_i^m} \right), \quad x_i^m \geq x_i^j, \forall i = 1 \dots n, \forall j = 1 \dots m \tag{1}$$

Acceptability. To determine whether a risk is acceptable or not, we use Table 2: the risk matrix provided by ED-202 that associates safety impact and likelihood. Safety impact levels are: 'N/E: no safety effect', 'MIN: minor', 'MAJ: major', 'HAZ: hazardous', 'CAT: catastrophic'.

Table 2. ED-202 acceptability risk matrix

		SAFETY IMPACT				
		No Effect	**Minor**	**Major**	**Hazardous**	**Catastrophic**
LIKELI	**pV: Frequent**	Acceptable	Unacceptable	Unacceptable	Unacceptable	Unacceptable
	pIV: Probable	Acceptable	Acceptable	Unacceptable	Unacceptable	Unacceptable
	pIII: Remote	Acceptable	Acceptable	Acceptable	Unacceptable	Unacceptable
	pII: Extremely Remote	Acceptable	Acceptable	Acceptable	Acceptable	Unacceptable
	pI: Extremely Improbable	Acceptable	Acceptable	Acceptable	Acceptable	Acceptable*

* = assurance must be provided that no single vulnerability, if attacked successfully, would result in a catastrophic condition

3.5 Step 5: Security Requirements

Security Level (SL). The SL is similar to safety Design Assurance Level [7] (DAL) defined in DO-178B. SL has a dual signification, it stands both for:

- strength of mechanism (assurance must be provided that countermeasures perform properly and safely their intended security functions)
- implementation assurance (assurance must be provided that security countermeasure has followed rigorous design and implementation process)

For each non acceptable threat scenario identified, a SL is determined based on the risk reduction required so that risk becomes acceptable in Table 2. Depending if the likelihood has to be reduced of 0, 1, 2, 3 or 4 levels to be on an acceptable level, SL will respectively take the values E, D, C, B or A. A SL is assigned to each developed countermeasure and associated assurance requirements will be given by ED-203.

Security Requirements. For each unacceptable threat scenario, a set of security objectives are established. They are translated into security requirements using the Security Functional Requirements (SFR) classes of Common Criteria part 2 in order to have an initial template to express security requirements in a formal way. Indeed, Common Criteria provide a classification of requirements patterns where interdependencies between them are already traced.

Assurance Requirements. Proving security requirements have been respected is not enough; development assurance must be consistent with a given environment and

[7] DAL stands for the accuracy dedicated to the design and development of a system according to its criticality in terms of safety impact, it sets objectives to properly provide assurance to certification authorities that developed system performs safely its intended functions. For example a DAL A system will receive the maximum care as a failure would have a catastrophic impact, whereas a DAL E system will have no design constraint as a failure would not have any consequence on safety of flight. Design and development rules are given by standards DO-178B for software and DO-254 for hardware.

procedures. To do so, we have mapped each SL with Common Criteria EALs (Evaluation Assurance Levels). Each EAL is linked to a set of assurance families themselves composed of SARs (Security Assurance Requirements). Assurance requirements aim at establishing accurate development rules so that security functions perform correctly their intended purpose and means to maintain security during development, maintenance and operational use have been taken into account.

3.6 Step 6: Risk Treatment

Countermeasure selection. Countermeasures must be selected for their compliance towards security requirements and for their effectiveness, but also taking into account development costs in order to avoid over design. Once a countermeasure has been developed on the most exposed supporting asset, verification such as intrusion tests must be performed on the basis of threat scenarios to prove its conformity with security requirements. Both countermeasures and intrusion tests should be made according to component AVA_VAN (Vulnerability assessment) of Common Criteria [9].

Security Rules. Safety process counts on a set of "safety rules" to provide for integrity or availability loss ensuring a fail-safe state of the systems. For instance, continuous monitoring, reconfiguration, redundancy (duplex, triplex, etc.), voting or comparison and dissimilarity are some of these rules. The Common Mode Analysis (CMA) is then performed to verify the correct and safe construction of the architecture.

The same way, in order to ease security architecture design, "security rules" can be set around principles such as: passive (e.g. monitoring) or active defense, perimetric defense (e.g. at Human-Machine Interface level or at any equipment receiving external data or software), middleware defense (e.g. at switch or router level), "onion skin" defense (e.g. at each system interface of a functional chain or potential attack path), central defense (e.g. central decision system), etc. Formal verification methods such as CMA could be then deployed to verify security rules for architecture patterns construction have been correctly applied (e.g. respect of segregation between critical and non-critical data in a router). These rules and verification means are to be defined.

4 Study Case

4.1 Scope

Let us consider the Weight and Balance (WBA) function that ensures 3D stability control of aircraft gravity center. It determines flight parameters (e.g.: quantity of kerosene to be loaded, takeoff run and speed, climbing angle, cruising speed, landing roll) and requires interactions with ground facilities. Figure 2 depicts the interactions required by the WBA function: check-in counters furnish number and distribution of passengers in the aircraft. Ground agent enters weight of bulk freight loaded in aft hold. Weight data is directly sent via data link to the ground WBA calculation tool to compute flight parameters. On ground, flight crew imports flight parameters to be directly loaded in the Flight Management System (FMS).

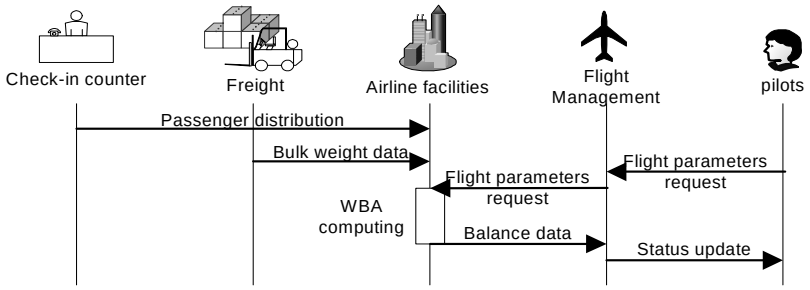

Fig. 2. WBA simplified functional chain sequence diagram

4.2 Preliminary Risk Assessment

Figure 3 depicts the top-down approach of threat scenario building, with identified primary assets, Failure and Threat Conditions. It should be shaped as a FTA but we choose this representation for a matter of space, left-right rows are causal links.

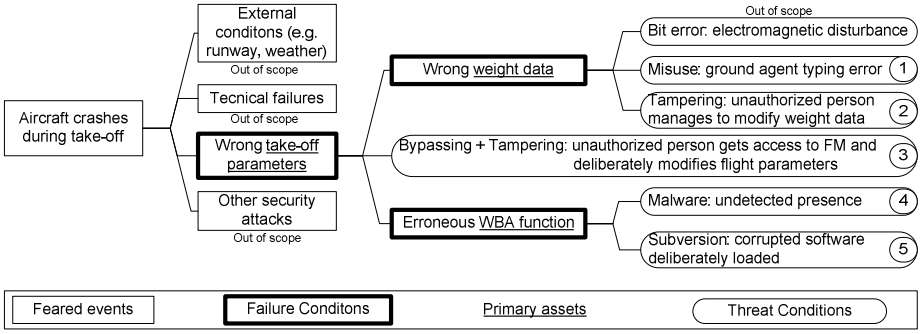

Fig. 3. Top-down approach threat scenario identification: from feared event to potential causes

4.3 Vulnerability Assessment

Most of supporting assets in this study case such as check-in counters and freight management computers are COTS. Let us suppose they present the following weaknesses: activated autorun, system bootable from peripherals, connection to Internet, no antivirus, no passwords. These vulnerabilities could be exploited by intruders or by a certain kind of boot virus. Depending on the consequences of these vulnerabilities exploitation on the aircraft, more threat scenarios would have to be added.

4.4 Risk Estimation

We estimate threat scenarios (TS) derived from TC 1 to 3 on Fig.2: “ground agent weight typing mistake on freight laptop” (TS1), “unauthorized person enters deliber-

ately wrong weight data on freight laptop" (TS2) and "intruder modifies flight parameters by accessing directly to FMS" (TS3).

To summarize, for each threat scenario, attacker capability and asset exposure are evaluated using a set of attributes and scales (respectively tables 3 and 4 for this study case). Values A and E are obtained thanks to equation 1 and used in table 1 intervals to determine likelihood. Obtained likelihood level combined with the safety impact of a successful attack attempt on table 2, allow deciding on risk acceptability. Results are gathered on table 5.

Table 3. Attacker capability score example

	Values			
Attributes	**3**	**2**	**1**	**0**
$\mathbf{X_1}$: Elapsed time for the attack	minutes	hours	<day	>day
$\mathbf{X_2}$: Attacker expertise	"misuser"	layman	proficient	expert
$\mathbf{X_3}$: Attacker system knowledge	public	restricted	sensitive	critical
$\mathbf{X_4}$: Equipment used	none	domestic	specialized	dedicated
$\mathbf{X_5}$: Attacker location	off-airport	airport	cabin	cockpit

Table 4. Asset exposure score example

	Values				
Attributes	**4**	**3**	**2**	**1**	**0**
$\mathbf{Y_1}$: Asset location	off-aircraft	cabin	maint. facility	cockpit	avionic bay
$\mathbf{Y_2}$: Class[8] of asset	class 1		class 2		class 3
$\mathbf{Y_3}$: DAL	DAL E	DAL D	DAL C	DAL B	DAL A
$\mathbf{Y_4}$: Vulnerabilities	large public	limited public	not public	unknown	none at all
$\mathbf{Y_5}$: Countermeasure	none	organizational	technical	on asset	>2 on chain

Table 5. Risk estimation: likelihood, impact, acceptability and SL determination

TS	**Attacker capability**						**Asset Exposure**						**Likelihood**	**Impact**	**Acceptable?**	**SL**
	$\mathbf{a_1}$	$\mathbf{a_2}$	$\mathbf{a_3}$	$\mathbf{a_4}$	$\mathbf{a_5}$	**A**	$\mathbf{e_1}$	$\mathbf{e_2}$	$\mathbf{e_3}$	$\mathbf{e_4}$	$\mathbf{e_5}$	**E**				
1	3	3	2	1	2	0,73	2	4	4	3	3	0,8	pV	HAZ	no (> pII)	B
2	3	1	2	3	2	0,73							pV	HAZ	no (> pII)	B
3	0	0	1	1	1	0,4	2	0	0	1	1	0,5	pII	HAZ	yes (≤ pII)	E

4.5 Security Requirements

In this example, only cases 1 and 2 will require to set security objectives that are: to provide means of user and data authentication. In Common Criteria part 2, this aspect corresponds to the SFR class FIA (Identification and Authentication) and more par-

[8] class 1: Portable Electronic Device (PED); class 2: modified PED; class 3: installed equipment under design control.

ticularly the families FIA_UAU (User Authentication) and FIA_AFL (Authentication Failure Handling). An example of SFR is "FIA_UAU.2.1: The system shall require each user to be successfully authenticated before allowing any other actions on behalf of that user" [9].

4.6 Risk Treatment

For cases 1 and 2, an organizational countermeasure is having a third party checking the weight data entered by ground agent. For case 1, a technical countermeasure is simply having the software used by ground agent asking to type twice the value to avoid typing mistakes. For case 2, a personal authentication password should be added to ground agent computer. Case 3 does not need treatment as an attacker able to break into the system must be very prepared and have a critical knowledge of the system, which is considered as unlikely to happen.

5 Conclusion

This paper justifies the need to develop an efficient risk assessment method to build secured architectures for digital aircrafts. We aim at introducing security considerations at an early design step of the development, allowing a certain degree of freedom to use attributes that best fit to the scope of analysis. Criteria taxonomy rules are to be improved by practice to make procedures as systematic and accurate as possible. However the exhaustiveness of threat scenarios identification cannot be proved nor guaranteed. Readjustments will have to be made to comply with future ED-203 modifications. This methodology has been tested on various examples and then applied on a real case of security certification. It has been agreed by the certification authority provided that intrusion test results validate the coherence of identified threat scenarios and eventually reveal new vulnerabilities.

References

1. SAE International (Society of Automotive Engineers, Inc.): Certification Considerations for Highly-Integrated Or Complex Aircraft Systems (ARP-4754). USA (1996)
2. SAE International (Society of Automotive Engineers): Guidelines and methods for constructing the safety assessment process on civil airborne systems and equipment (ARP-4761). USA (1996)
3. Radio Technical Commission for Aeronautics (RTCA SC-167) and European Organization for Civil Aviation Electronics (EUROCAE WG-12): Software considerations in airborne systems and equipment certification (DO-178B/ED-12). Washington, USA (1992)
4. European Organization for Civil Aviation Electronics (EUROCAE WG-46) and Radio Technical Commission for Aeronautics (RTCA SC-180): Design assurance guidance for airborne electronic hardware (DO-254/ED-80). Paris, France (2000)
5. R. De Cerchio, C. Riley : Aircraft systems cyber security. In: IEEE/AIAA Digital Avionics Systems Conference, pp.1C3.1-1C3.7. Seattle, USA (2011)

6. European Organization for Civil Aviation Equipment (EUROCAE WG-72) and Radio Technical Commission for Aeronautics (RTCA SC-216): Airworthiness security process specification (ED-202). (2010)
7. RTCA SC-216 and EUROCAE WG-72: Airworthiness security methods and considerations (ED-203). Working draft version rev.9.5 (2011)
8. Jacob J.M.: High assurance security and safety for digital avionics. In: 23rd IEEE/AIAA Digital Avionics Systems Conference, vol. 2, pp. 8.E.4-8.1-9. Salt Lake City, USA (2004)
9. International Organization for Standardization: Common Criteria for Information Technology Security Evaluation (CC v.3.1). <http://www.commoncriteriaportal.org>, (2009)
10. Ministerio de Administraciones Publicas (Spanish Ministry for Public Administrations), MAGERIT. Spain (2005)
11. Insight Consulting: CRAMM (CCTA Risk Analysis and Management Method). United Kingdom (2003)
12. National Institute for Standards and Technology (NIST): Risk Management Guide for Information Technology systems. United States (2002)
13. Carnegie Mellon University, SEI (Software Engineering Institute): OCTAVE v2.0. USA (2005)
14. CLUSIF (Club for the Security of Information in France): MEHARI (Method for Harmonized Analysis of Risk). France (2010)
15. Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI): EBIOS - Expression des Besoins et Identification des Objectifs de Sécurité. Paris, France (2004)
16. Liao N., Li F., Song Y.: Research on real-time network security risk assessment and forecast. In: 2010 International Conference on Intelligent Computation Technology and Automation (ICICTA), Vol.3, pp.84-87. Changsha, China (2010)
17. Alhabeeb M., Almuhaideb A., Dung L.P., Srinivasan B.: Information Security Threats Classification Pyramid. In: 24th IEEE International Conference on Advanced Information Networking and Applications Workshops, pp. 208-213. Paderborn, Germany (2010)
18. Ortalo R., Deswarte Y., Kaaniche M.: Experimenting with quantitative evaluation tools for monitoring operational security. In: 6th International Conference on Dependable Computing for Critical Application (DCCA-6). Garmish, Germany (1997)
19. Ben Mahmoud M.S., Larrieu N., Pirovano A.: A risk propagation based quantitative assessment methodology for network security. In: 2011 Conference on Network and Information Systems Security (SAR-SSI), p.1-9. La Rochelle, France (2011)