# Risk Assessment for Airworthiness Security

Silvia Gil-Casals, Philippe Owezarski, Gilles Descargues

# Risk Assessment for Airworthiness Security

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

[1]THALES Avionics, 105 av. du General Eisenhower, F-31100 Toulouse, France
{silvia.gil-casals, gilles.descargues}@fr.thalesgroup.com
[2]CNRS, LAAS, 7 avenue du colonel Roche, F-31400 Toulouse, France
philippe.owezarski@laas.fr
[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 processes have been capitalizing on experience to counter such effects and standards were issued to provide guidelines for safety assessment process and development assurance. Safety-critical systems segregation from the Open World tends to become thinner due to the high integration level of airborne networks. Most of the challenging innovations to offer new services, ease 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. As a matter of fact, EUROCAE[1] and RTCA[2] are defining new airworthiness security standards: ED-202 [1] provides guidance to achieve security compliance objectives based on future ED-203[3] [2] methods.

[1] European Organization for Civil Aviation Equipment

[2] Radio Technical Commission for Aeronautics

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

EU and US[4] 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 experimented security managers criteria. 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" [3] 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). For example, MAGERIT (Spain) and CRAMM (UK) deal with governmental risk management of IT against for example privacy violation. NIST800-30 provides security management steps to fit into the system development life-cycle of IT devices. Others, such as COBRA or OCTAVE 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 proposes a set of checklists and evaluation grids to estimate natural exposure levels and impact on business. Finally, EBIOS shows an interesting evaluation of risks through the quantitative characterization of threat sources of a wide spectrum of threats (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

[4] Respectively EASA (European Aviation Safety Agency) and FAA ( Federal Aviation Administration)

on fuzzy logic and Petri Nets [4] vs. a visual representation of threats under a pyramidal form [5]). Ortalo, Deswarte and Kaaniche [6] 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 fatigue testing or experience feedback, security parameters are not physically measurable. To avoid subjective analysis, Mahmoud, Larrieu and Pirovano [7] 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.

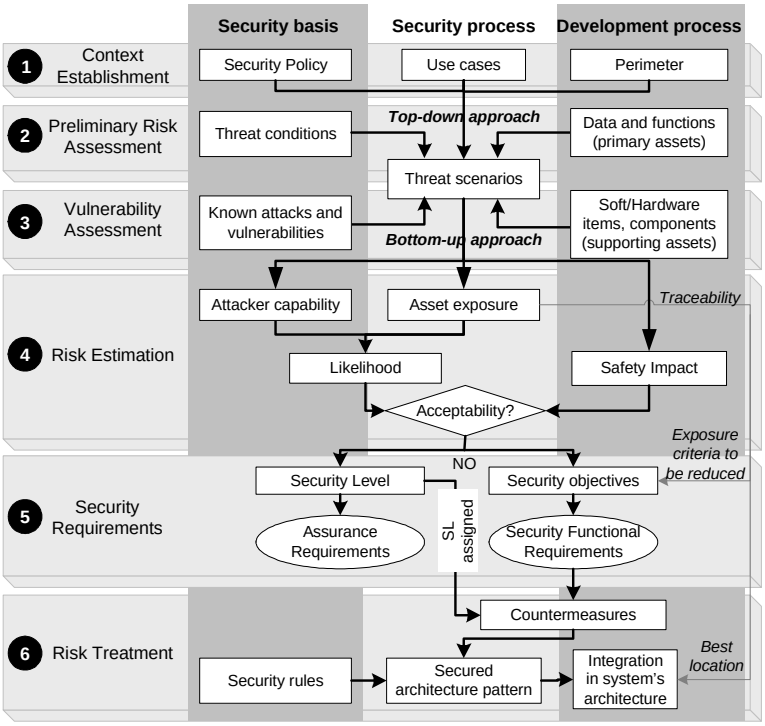


**Fig. 1.** Risk assessment and treatment process: the figure differentiates input data for the security process as coming either from the development process or from a security knowledge basis.

### 3.1 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, depth of the analysis, operational use cases, 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.

### 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 primary assets (aircraft critical functions and data) from 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 (TC) themselves leading to Failure Conditions (FC), e.g.: TC={misuse, confidentiality compromise, bypassing, tampering, denial, malware, redirection, subversion} and FC={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. 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 exploited vulnerabilities are listed to establish a vulnerability checklist.

*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 completing these requirements with technical constraints and effectiveness requirements, as well as identifying threats left unconsidered during the top-down analysis.

### 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 most probable and dangerous threats.

**Likelihood.** It is the qualitative probability that an attack is successful. ED-202 considers five likelihood levels: 'frequent', 'probable', 'remote', 'extremely remote', '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). Table 1 is usable whatever the amount of attributes used, 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). These criteria must be defined with an accurate taxonomy so the evaluation is exhaustive, unambiguous and repeatable.

Let $X = \{X_1, \dots, X_n\}$ be a set of n qualitative attributes chosen to characterize the "attacker capability". Each attribute $X_i$ can take m values: $\{X_i^1, \dots, X_i^m\}$, $X_i^j$ being more critical than $X_i^{j-1}$ and so on. To each qualitative value $X_i^j$, we associate a quantitative value $x_i^j$ with $x_i^j > x_i^{j-1}$and so on. Let us call $f_j()$ the evaluation function performed by the security analyst allowing 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). The same reasoning is made to express asset exposure E.

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

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

**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 |

**Table 2.** ED-202 acceptability risk matrix

| | | SAFETY IMPACT | | | | |
|---|---|---|---|---|---|---|
| | | **No Effect** | **Minor** | **Major** | **Hazardous** | **Catastrophic** |
| LIKELIHOOD | **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 and 6: Security Requirements and Risk Treatment

For each non acceptable threat scenario, security objectives (i.e. asset exposure criteria to be reduced) are translated into Security Functional Requirements to find the best countermeasure to be implemented on most exposed supporting asset. A Security Level (SL) is assigned based on required risk reduction so that risk becomes acceptable. 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. SL has a dual signification, it stands both for effectiveness (assurance must be provided that countermeasures perform properly and safely their intended functions) and implementation assurance (assurance must be provided that security countermeasure has followed rigorous design and implementation process). SL is assigned on developed countermeasures and associated assurance requirements will be given by ED-203.

## 4 Study Case

**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. 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).

**PRA.** Figure 2 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.

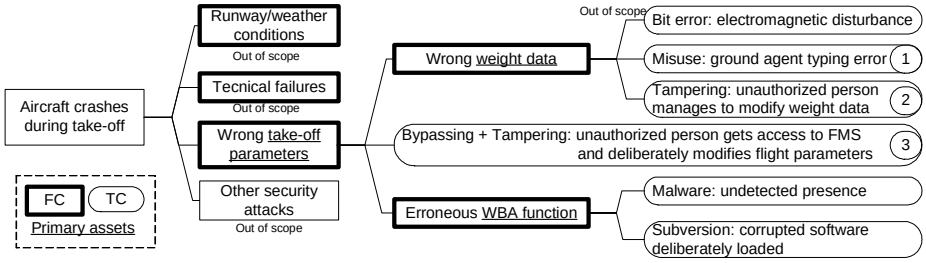


**Fig. 2.** Top-down approach threat scenario identification: from feared event to potential causes

**Vulnerability Assessment.** Most of supporting assets in this study case are COTS which are vulnerable to malware. Let us say that these COTS present the following weaknesses: activated autorun, system bootable from peripherals, connection to Internet, no antivirus, no passwords. Then, these vulnerabilities could be exploited by intruders or by a certain kind of boot virus. These case will not be further developed.

**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 deliberately wrong weight data on freight laptop"(TS2) and "intruder modifies flight parameters by accessing directly to FMS"(TS3). Scenarios are evaluated with tables 3 and 4 and $f_{j=1}^{m}(x_i^j) = j$. Results are summarized 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 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 |

* class 1: Portable Electronic Device (PED) e.g. COTS; class 2: modified PED; class 3: installed equipent under design control

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

| TS | Attacker capability | | | | | | Asset Exposure | | | | | | Likelihood | Impact | Acceptable? | SL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $a_1$ | $a_2$ | $a_3$ | $a_4$ | $a_5$ | A | $e_1$ | $e_2$ | $e_3$ | $e_4$ | $e_5$ | $E_n$ | | | | |
| 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 |

**Risk Treatment.** For case 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 should be improved by practice to make procedures as systematic and accurate as possible. Readjustments will have to be made to comply with future ED-203 modifications.

## References


1. 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)
2. RTCA SC-216 and EUROCAE WG-72: Airworthiness security methods and considerations (ED-203). Working draft version rev.9.5 (2011)
3. 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)
4. 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)
5. 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)
6. 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)
7. 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)