[Article] Risk Assessment Techniques for Civil Aviation Security

Risk Assessment Techniques for Civil Aviation Security

Galileo Tamasi[a]. Micaela Demichela[b]

[a]Ente Nazionale per l'Aviazione Civile – Direzione Progetti, Studi e Ricerche
Via di Villa Ricotti, 42
00161, Roma, Italy
g.tamasi@enac.rupa.it

[b]SAfeR – Centro Studi su Sicurezza, Affidabilità e Rischi
Dipartimento di Scienza dei Materiali e Ingegneria Chimica
Politecnico di Torino
Corso Duca degli Abruzzi, 24
10129, Torino, Italy
Tel. +390110904629
Fax +390110904665
micaela.demichela@polito.it

Abstract

Following the 9/11 terrorists attacks in New York a strong economical effort was made to improve and adapt aviation security, both in infrastructures as in airplanes. National and international guidelines were promptly developed with the objective of creating a security management system able to supervise the identification of risks and the definition and optimisation of control measures.
Risk assessment techniques are thus crucial in the above process, since an incorrect risk identification and quantification can strongly affect both the security level as the investments needed to reach it.
The paper proposes a set of methodologies to qualitatively and quantitatively assess the risk in the security of civil aviation and the risk assessment process based on the threats, criticality and vulnerabilities concepts, highlighting their correlation in determining the level of risk.
RAMS techniques are applied to the airport security system in order to analyse the protection equipment for critical facilities located in air-side, allowing also the estimation of the importance of the security improving measures vs. their effectiveness.

Keywords: Civil Aviation Security, Airport Security, Risk Assessment, RAMS, Terrorist threats

1. Introduction

The terrorist attack of September 11th 2001, observed from a socio-economic, cultural and political point of view, had a tremendous negative impact on air transport never seen before in aviation, unparalleled in history [1,2,3].
Proper measures have soon been taken following the considerations emerged after the attacks and most of they are listed in the seventh edition of Annex 17 of the Chicago Convention of the International Civil Aviation Organization (ICAO) [4,5]. Annex 17 is the key document concerning aviation security and is the primary Annex for security-related Standards and Recommended Practices.
ICAO realised immediately the urgency and the need for restoring the integrity of the aviation system and met representatives from 32 nations to discuss new security measures. The ICAO has then implemented 66 security standards and 16 Recommended Practices (SRPs) and has recommended the Universal Security Audit Programme (USAP). USAP programme promotes global aviation security through the auditing of Contracting States on a regular basis to determine the status of implementation of ICAO Annex 17 security Standards.
Since 9/11, new measures have been taken in order to protect the aircrafts from hijacking and sabotage threats and new preventive methodologies have been developed to prevent actions which could threaten the aircraft security.
Other methods and innovative procedures are being developed to improve the airport security system and to protect it from new threats, such as the Laser Beams which could blind the pilots, the use of Hand Portable Air Defence Systems (MANPADS) and explosives which could shoot down the aircraft during the landing or take-off procedures.

The heads of the aviation industry, such as ACI, IATA, IACA, Airbus and Boeing have formed the Global Aviation Security Audit Group (GASAG). They strongly affirm that the security of the aviation (AVSEC) is not only a responsibility of the civil aviation industry, but also is a security problem of the nations. They have also underlined the importance of government bodies and of the intelligence in the control of the new emerging threats.
New countermeasures was suggested, included hundred per cent baggage screening, explosives detection, biometric identification of passengers and, maybe, remote check-in, risk based threat perception analysis and identification of non-risk passengers instead of the rarer risk-passenger, as well as in-flight measures like using Sky Marshals, strengthening cockpit doors and cabin monitoring from within the cockpit [6-11].
Thus far, carrying arms has been banned, but the possibility of arming, or at least training the crew, in unarmed combat is being seriously considered. Research is also on going to improve the efficacy of some of these countermeasures.
After 9/11 greater attention has been paid to what is established in the Annex 17 in the field of the security programs. Particularly, the concepts of threat assessment and risk management have been underlined. Both concepts lead to a basic methodology able to face effectively the threats addressed to the civil aviation system.
In the restricted Doc ICAO 8973 [12], the methodologies of threat assessment and risk management are outlined. These methodologies have both an analytical and semi-quantitative approach based on numerical scores. However, other methodologies can be applied in aviation security and they will be delineated later in the present paper.

2. Risk management and risk assessment for airport security

The current security measures in world airports cannot assure total protection against every typology of threats, but an effective risk management approach can prepare better against acts of terrorism [13,14]. The security risk management is an analytical and systematic process which allows the evaluation of the probability of a threat to result in a negative action towards an infrastructure, people or critical functions of the airport system. Risk management principles acknowledge that while risk generally cannot be eliminated, enhancing protection from known or potential threats can reduce it.
The risk management allows the detection of actions which could reduce the risk and mitigate the consequences of an attack. The risk management allows to implement and to maintain efficient over time all countermeasures, gradually reducing the risk, in view of a constant improvement, within acceptable values.
A good risk management approach includes risk assessment composed by three primary elements: a threat assessment, a vulnerability assessment, and a criticality assessment.
A threat assessment identifies and evaluates threats based on various factors, including capability and intentions as well as the potential lethality of an attack.
A vulnerability assessment is a process that identifies weaknesses that may be exploited by terrorists and suggests options to eliminate or mitigate those weaknesses.
A criticality assessment is a process designed to systematically identify and evaluate an organization's assets based on their values, the importance of its mission or function, the group of people at risk, or the significance of a structure.

After the evaluation of the effectiveness of the security controls, the risk assessment allows the evaluation of the potential effects resulting from threats, with reference to each vulnerable area. The risk assessment, therefore, is performed in order to evaluate the risk associated to each critical element of the airport and the loss related to the success of threats. In most cases, the risk assessment procedure attempts to strike an economic balance between the impact of risks and the cost of security solutions intended to manage them.
The analysis of the Annual Losses Expected (ALE) determined through the risk assessment allows to take decision on the amount of economic resources necessary to implement the countermeasures. Of course, the cost of countermeasures is only a percentage of the ALE's. Besides, the countermeasures enables the ALE's to remain within acceptable risk limits.

3. Qualitative and quantitative risk assessment

Risk is a multifaceted issue and must be addressed with methods that are appropriate for the decisions to be taken. Historically, risk assessment and risk management professionals have focused on accident risks, natural hazard risks, business interruption risks, project risks, and financial risks. In these areas, organizations have used very systematic processes and tools to understand and prioritize these diverse risks, especially those with catastrophic consequences.
Security related risks are another broad category of risks with potentially catastrophic consequences, that after 9/11 has been receiving significant attention [15,16]. While security related risks require a different approach than other types of risk, the same fundamentals apply. Terrorist attacks and other unlawful acts are a different type of threat, but they pose risks in much the same way as other threats.
In a risk assessment carried on for the security in an airport, the analysis has to underline:

- the level of the current risk
- the possible consequences of attacks
- the actions to be undertaken if the residual risk is superior to the tolerable values

The quantitative risk assessment can be subdivided in the followings steps:

- Threat Assessment
  –Detection of the presence of hostile groups in the home territory
  –Evaluation of the threat level in the nation
  –Evaluation of the threat level near airports

- Vulnerability assessment
  –Analysis of the critical points and the functional importance of airport systems and infrastructures
  –Evaluation, within the system of airport security, of protection systems for every critical infrastructure and evaluation of the accessibility and vulnerability levels

- Criticality Assessment
  –Analysis of the potential accidental scenarios consequent to the success of the attacks on critical targets
  –Analysis of the costs for the re-establishment of the critical targets and evaluation of the missed indirect incomes because of their unavailability;
  –Evaluation of the economic losses related to every accidental scenario

The quantification can be done through the followings generalized relations:

$$\text{Risk} = \text{Frequency (F)} \times \text{Consequence (C)} \quad (1)$$

$$\text{Frequency (F)} = \text{Initiating Event Frequency} \times \text{Probability All Safeguards Fail} \quad (2)$$

$$\text{Risk} = [\text{Threat (T)} \times \text{Vulnerability (V)}] \times \text{Criticality (C)} \quad (3)$$

Where:
Threat (T) is a measure of the likelihood that a specific type of attack will be initiated against a specific target (that is, a scenario).
Vulnerability (V) is a measure of the likelihood that various safeguards against a scenario will fail.
Criticality (C) is the magnitude of the negative effects if the attack is successful.

Figure 1 there shows the approach for the risk assessment.

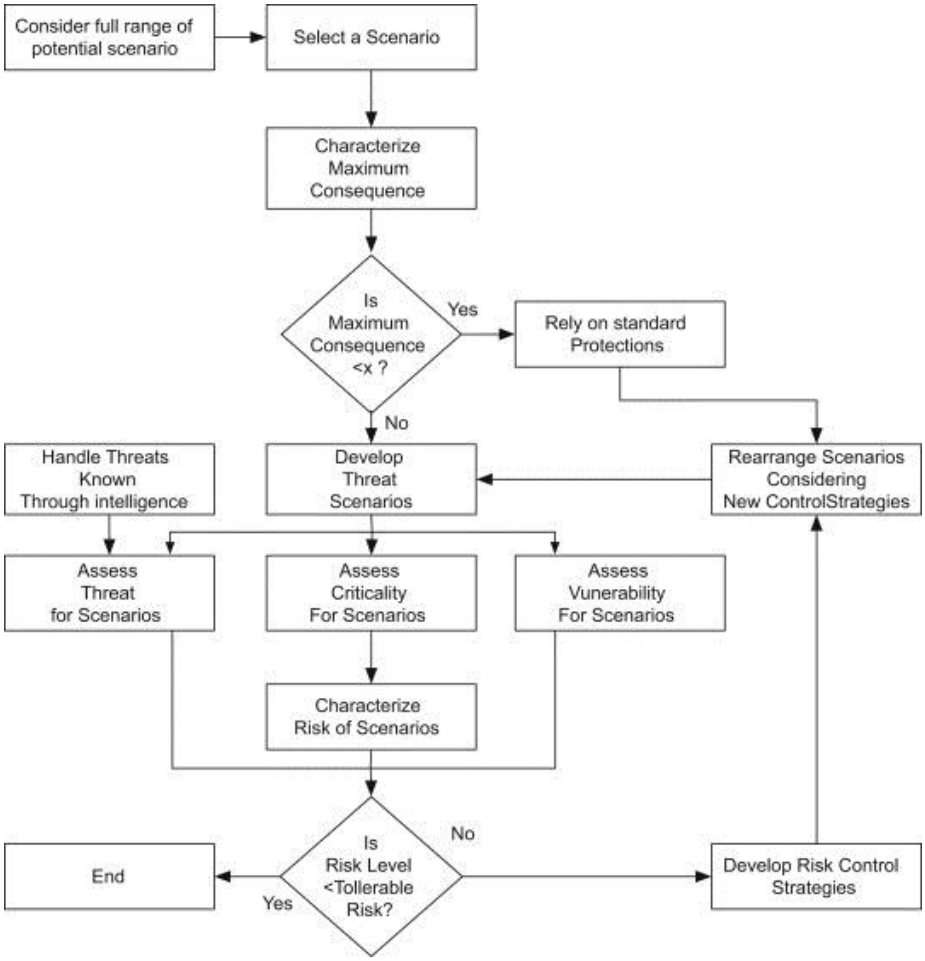

Figure 1. Risk assessment approach.

One of the key challenges in defining a framework for collecting, organizing, and reporting the risk-based information is to determine what level of precision is appropriate to support the decisions to be taken.

In particular, the goal of this study was to propose a framework for risk assessment able to support the decision making in the design and/or optimisation of protection levels for airport security.

High or even medium precision may not necessarily be achievable, particularly when the specific technology for achieving a given antiterrorism capability is not defined or is under development [17, 18].

Several approaches can help accomplishing this objective.

Matrix based semi-quantitative approach can be based on threat, vulnerability, and consequence categories that can be used to capture security related risks information. Assigning numerical scores to each category of threat and vulnerability and assigning "representative" loss estimates to the consequence categories will provide a scoring system that will express the measure of risk in terms of loss exposure, which can be directly compared to cost of implementation, thus providing a meaningful benefit/cost index for relative ranking.

A mixed quantitative and semi-quantitative experimental risk based design is e.g. currently ongoing in designing the new security systems of Lampedusa and Pantelleria airports that are managed directly by the ENAC, the Civil Aviation Authority Italy.

The qualitative analysis, instead, which is at present conducted in Italy, is based on Security Audit, primarily constituted by check lists elaborated by ENAC on the indications of the current Italian and European Community legislation.
The check lists and the inspective procedures are obviously integrated in order to take into consideration the international legislation and the technical security recommendations (ICAO, ECAC, IATA).
The Security Audit particularly refers to the following areas:

- Organization and management of the security systems at national level and cooperation with other states
- Organization and management of the security systems at airport level
- Control of the access to the airport structures
- Passengers and hand baggage
- Hold Baggages
- Aircraft and flight procedures
- Cargo and Catering
- Ability to answer to illegitimate actions and contingency planning

The results are given as predetermined levels of conformity to the actual security standards. The level of vulnerability and the necessary countermeasures to be implemented are expressed for each airport area.
The qualitative risk survey is completed with a report submitted to the airport management companies and to other subjects charged with the security services who must solve the critical points shown and ranked by the analysis within a fixed temporal term.

4. Vulnerability and Criticality analysis through modified recursive HAZOP and Fault Tree Analysis

A vulnerability assessment is a process that identifies weaknesses in physical structures, personnel protection systems, processes, or other areas that may be exploited by terrorists and may suggest options to eliminate or mitigate those weaknesses. For example, a vulnerability assessment might reveal weaknesses in an organization's security systems or unprotected key infrastructure such as power supplies, ATC control towers, and electric facilities.
A criticality assessment is a process designed to systematically identify and evaluate important assets and infrastructure in terms of various factors, such as the mission and significance of a target. For example, power generators, radio navigation aids, computer networks might be identified as "critical" in terms of their importance to airport security, airport economic activity, and airport safety. In addition, facilities might be critical at certain times, but not others. For example, a runway when in use in heavy air traffic and low visibility conditions may represent an important target. Criticality assessments are important because they provide a basis for identifying which assets and structures are relatively more important to protect from an attack.

The use of RAMS (Reliability, Availability, Maintenability and Safety) techniques in vulnerability and criticality assessment of an airport is here described applying it to a key electrical facility that is a vital part of equipments needed for the airport exercise. The equipments are usually located in air side in the physical areas.

The physical areas usually present in the airport requiring protection are shown in Figure 2.

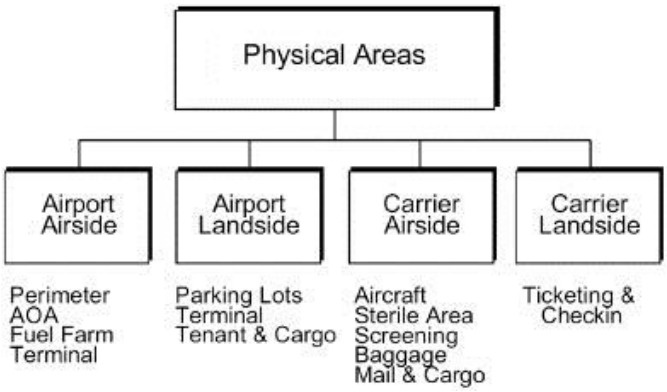

Figure 2. The physical areas usually present in an airport.

The airport perimeter fence is the first physical defence and together with technological systems is a fundamental component of the airport security system. Inside the airport perimeter there are other critical areas which are protected with further combinations of technological systems.
The technological systems are connected through a centralized architecture that manages the monitoring, the events and the states of alarm. An example of simplified architecture is illustrated in Figure 3.

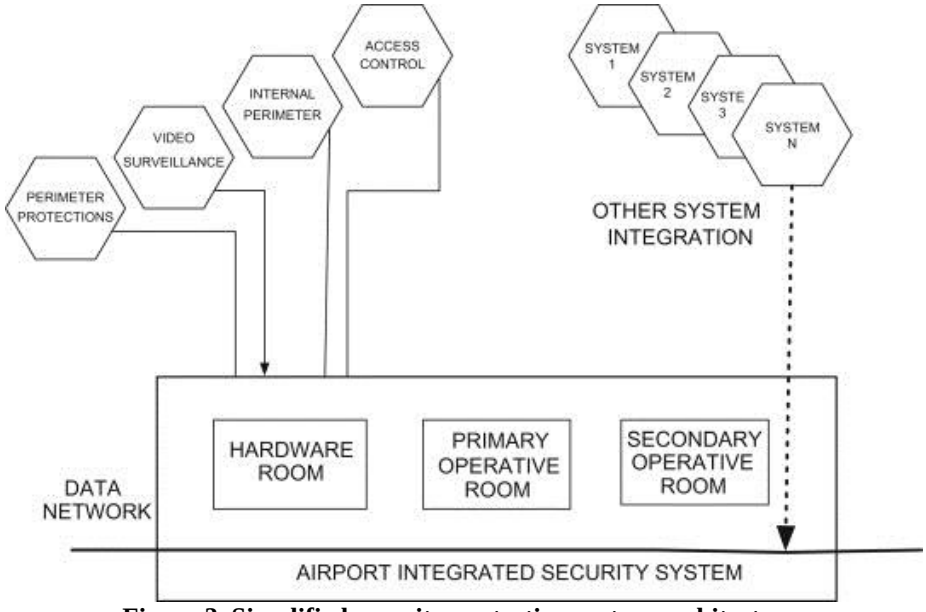

Figure 3. Simplified security protection system architecture.

The case study has been approached through the Recursive Operability Analysis [18,19,20] and the Fault Tree Analisys the vulnerability and criticality of a airport security protection system of an electric substation for power supply the airfield ground lighting and radio navigation aids. These methodologies allow the examination of both logical and probabilistic behaviour of the protection system.

An electric substation dedicated to Airfield Ground Lights (AGL) and Radio Navigation Aids (RNA) is an important part of the airport electrical systems and,

together with other electric components, it is of vital importance for exercise of every airport luminous visual aids and of the radio navigation aids. The radio navigation aids lead the aircraft to a precision instrumental approach to the runway while the luminous visual aids allow the pilots to verify the correctness of approach procedure. The unavailability of these systems for lack of power supply makes the airport runway unavailable and this, for the airports with only one runway, causes the unavailability of the whole airport.

The immediate lack of power supply of radio navigation aids and visual aids can cause severe anomalies in the air traffic system and can lead to an accidental sequence that could cause air disaster as shown in Hazop analysis depicted in Table 1. For these reason the electrical network and the electric substation could constitute the target of severe threats by external entity aiming at disabling it through illegal actions.
The simplified sketch of the monitoring and protection systems of electric substation, subjected to the vulnerability assessment, is illustrated in Figure 4.

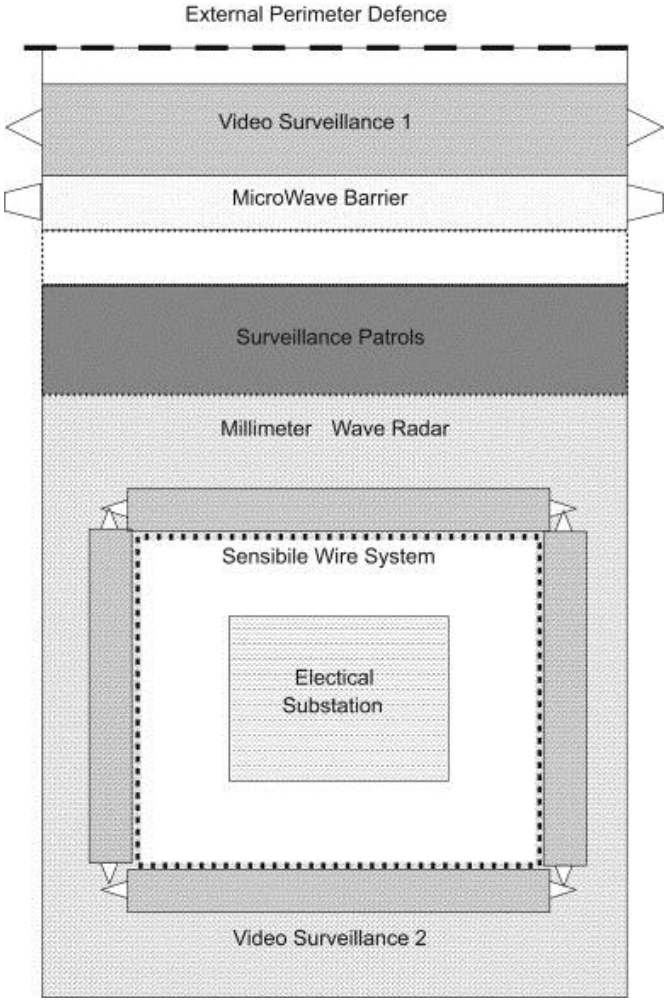

Figure 4. Simplified scheme of monitoring and protection systems.

The protection system can be considered as composed by:

- Physical perimeter fence with metallic enclosure
- System of microwaves sensors

- System of perimeter video surveillance
- Airside millimetre-wave radar
- Surveillance patrol
- Physical perimeter of electric substation and protection system with sensitive wire
- System of second internal perimeter video surveillance
- Protection system of electrical facility internal area through volumetric sensors

The security systems above illustrated are predisposed to identify the presence of external non-authorised entities in each part of the airside in order to be able to immediately activate suitable countermeasures.
A hostile entity, that wants to reach the electric substation, has to disable or to avoid all the control systems already installed outside and inside the airport. The vulnerability of the system is obviously connected with its leaning to become unavailable after an attack to some essential components of protection system is carried out.
Through a Recursive Operability Analysis (ROA) is possible, therefore, to examine in a better way the functionality of the system and its ability to protect the potential targets.
Furthermore, it is possible to evaluate the differential vulnerability, in comparison to the conditions of normal operation, if some components of the system are put out of order under attack.
The ROA allows the Fault Trees to be directly extracted by the analysis tables, for the quantification of the identified Top Events.

5.1 Recursive Operability Analysis

In Table 1, the ROA analysis related to the security protection system in Figure 5 and the consequences of the Top Event 1 are shown.

Deviation	Causes	Consequences	Alarm Systems	Automatic Protection Systems	Top Event
Bypass external enclosure	Damage airport enclosure	Entry Air Side Zone 1			
Entry Air Side Zone 1	Overcoming external perimeter	Entry Air Side Zone 2	Microwave System Video Surveillance		
Entry Air Side Zone 2	Entry Air Side Zone 1	Entry Air Side Zone 3	Millimetric Radar Patrol Surveillance		
Entry Air Side Zone 3	Entry Air Side Zone 2	Entry Area Electric Facility	Sensitive Wire Protection System Video surveillance		
Entry Area Electric Facility	Entry Air Side Zone 3	Entry Electric Facility	Volumetric Control System		TE1
Unavailability Electrical Facility	Accessibility Electrical Facility Night Flights & Sabotage group presence	Unavailability RWY for Unavailability Radioassistance and Luminous Visual	Monitoring Electric TWR Facility		TE2
Unavailability RWY	Unavailability Electrical Facility Night Flights	Anomaly Air Traffic Control	Monitoring TWR ATC		TE3
Anomaly Air Traffic Control	Unavailability RWY	Aircraft accident	Aircraft Avionics		TE4
Aircraft accident	Anomaly Air Traffic Control	Air disaster	Emergency Center Airport Monitoring Rescue & Fire Fighting		TE5

Figure 5. Recursive Operability Analysis.

This analysis is related to the technological failure of the protection systems and, at this stage, does not take into account the voluntary damaging or by-passing carried on by airport operators.

5.2 Fault Tree Analisys

The fault tree directly drawn from the ROA tables was solved using ASTRA FTA Software [21-24] and is shown in the Figures 6 and 7:

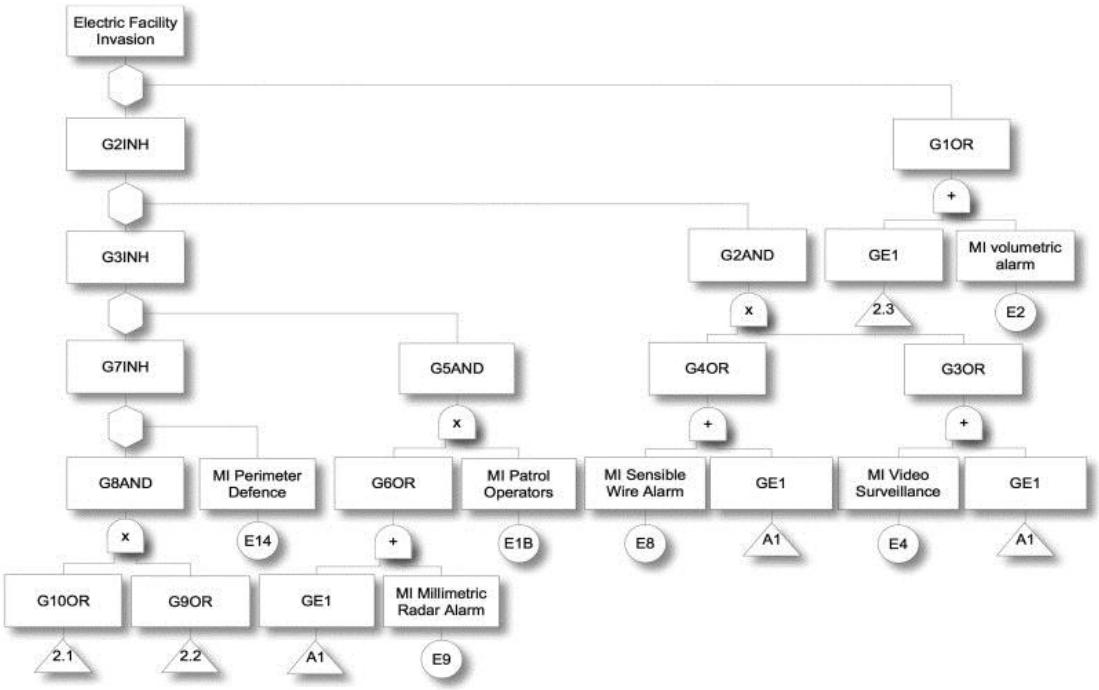

Figure 6. Astra Fault Tree—part 1.

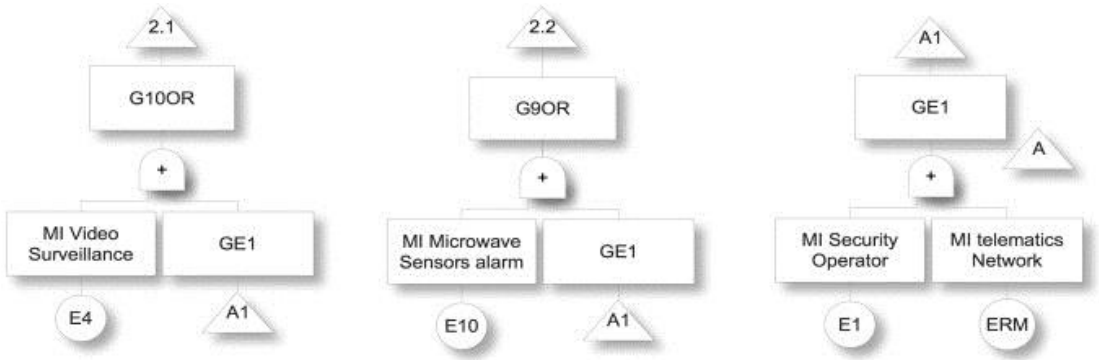

Figure 7. Astra Fault Tree—part 2.

The reliability parameters used in numerical solution of the fault tree are detailed in Table 1:

Table 1.

Event name	Unavaila-bility	Description
E1	1.5000E-03	MI Security Operator
E10	1.0000E-03	MI Microwave Sensors Alarm
E14	5.0000E-01	MI Perimeter Defence
E1B	1.0000E-02	MI Patrol Operators
E2	1.0000E-03	MI Volumetric Sensors Alarm
E4	1.0000E-03	MI Video Surveillance
E6	1.0000E-04	MI Sensitive Wire Alarm
E9	1.0000E-04	MI Millimeter-wave radar Alarm
ERM	1.0000E-05	MI Alarms Telematics Network

Some probabilistic parameters are gathered from reliability data-banks [25], the missing ones related to the airport security systems was given by the producers of the hardware apparatuses.

The cut sets are listed according to their probabilistic importance in table:

Table 2.

#	Q	W	Minimal cutsets		
1	7.5000E-06	7.5000E-06	E1	E14	E1B
2	5.0000E-08	5.0000E-08	E14	E1B	ERM

Through the simple model here described, it is possible to analyse the two cut sets, that for an external hostile entity is very difficult to contemporarily disable both the operators of the airport security centre (E1) and the surveillance patrols (E1B) and after to climb over the perimeter enclosure (E14).
It is much more simple to attack the monitoring network (ERM), to climb over the monitoring enclosure (E14) and to reach the electric substation deceiving the controls of the surveillance patrols (E1B).

The initiating events are illustrated according to their importance in table:

Table 3.

Event	Importance	Description
E1B	1.0000E+00	MI Patrol Operators
E14	1.0000E+00	MI Perimeter Defence
E1	9.9337E-01	MI Security Operators
ERM	6.6225E-03	MI Alarms Telematics Network

This classification allows, both in phase of design of a new system and in phase of analysis or change of an existing system, to understand which system needs to be improved.
With such analysis tools, the relative importance of system components can be examined, with the possibility to improve both the general architecture and the behaviour of every sub-system.

The analysis of the accessibility has shown, through the examination of cuts sets, that a hostile group to have a successful action needs to:

- know the facilities airport configuration and the position of the target
- know the airport surveillance procedures
- have knowledge of alarms network
- have equipments to climb over the perimeter enclosure
- have equipments to disable the alarm network
- have weapons and tools to shoot the patrol controls
- have weapons and tools to disable the electric substation

After carrying out the structure vulnerability analysis and the criticality analysis, we have also outlined the profile of the hostile external entity. The criticality analisys conducted also by ROA had individualized (see Figure 5) the consequences of an attack in terms of economic losses, denial of service, negative image to passengers. To complete the risk assessment procedure (see Figure 1) it is necessary to evaluate the likelihood that the profiled entity has to decide to attack the target.

By using the threat assessment, the risk assessment procedure is completed then by defining the likelihood that one specific hostile entity has, under particular conditions, to attack and overcome the protections of a vulnerable target, thus producing consequences to which an economic value is associated.

The results can be expressed as expected annual loss (ALE) and they are a good indicator in deciding the investments in the security sector. The threat assessment methodology which completes the risk assessment procedure will be shortly illustrated soon.

6. Threat Assessment

This last step is fundamental to perform a complete risk assessment related to security aspects, but it is still a critical point and characterised by large uncertainties and lack of objectivism.
A threat assessment is used to evaluate the likelihood of terrorist activity against a given asset or location. It is a decision support tool that helps to establish and prioritize security-program requirements, planning, and resource allocations. A threat assessment identifies and evaluates each threat on the basis of various factors, including capability, intention, and lethality of an attack.
The definition of a realistic or real threat set to be taken into account is delegated to the intelligence, and to the government bodies (in Italy the Ministry of Defense and the Ministry of Interior). Nevertheless, the civil aviation authority contributes to the identification of the key elements to be kept into consideration in the analysis.
In the identification of threats addressed to the civil aviation there are different sources of empirical evidence and of available statistic data. They have to be valued considering every factor which could result in a terrorist event.
The ICAO, e.g. has defined a semi-quantitative methodology which considers the presence in the nation of terrorist groups, the historical records of aviation attacks, the level of internal strike, the entity of the economic problems, the number of the airport flights and the number of high risk flights. From elaboration of these indicators which

are numerically quantified in a matrix you can have numerical scores which can be easily connected with the likelihood of an attack.
Similarly, the probability that a group with specific characteristics, ability, information and equipments is motivated to start a predetermined terrorist action can be valued, as in the case of the disabling of an electric substation underlined before.

7. Conclusions

A set of scenario attacks towards a specific target can be investigated trough examination of its vulnerability and its criticality.
Every potential scenario can be studied in order to have an estimation of the current risk level, the evaluation of possible economic losses on a annual base, and the set of the countermeasures to adopt in order to reduce the risk.
The quantitative analysis carried out with RAMS methodologies has shown the possibility to investigate vulnerabilities and criticality of the airport components. The use of the previous analysis results, melted with the result of threat assessment complete the risk assessment procedure. The procedure offer as result the likelihood that an attack is successful in the selected scenario, so, is possible to have the likelihood that the airport have an economic loss and others serious problems. The cumulative set of scenarios investigated define at the end of the process the necessary indication to select suitable countermeasures also in terms of economical investment.
The maintenance of countermeasures over time is a task of the risk management and it is fundamental to protect the airport infrastructures and to plan changes to airport security systems.
The effectiveness of the quantitative techniques borrowed from the industrial risk assessment for airport security purposes has been demonstrated through their application to a simple case study, that could be seen as a part of a complete and more detailed analysis.
The optimised design of the airport security system, its ability to innovate and to modify itself in consequence of the results of risk assessment is surely the best indicator of the ability to answer to the new incumbent threats and to assure an acceptable security risk level to the passenger and airport operators.

Acknowledgements

The authors would like to express their thankfulness to Prof. Norberto Piccinini (Politecnico di Torino) who initiated and encouraged the present work, to Paolo Mazzaracchio of Civil Aviation Authority Italy – Airports Technologies Office for the continuous and precious suggestions, to Roberto Passatore of Civil Aviation Authority Italy - Security Directorate for his unique indications and last but not least to Mladen Cala of ICAO Security International for the significant help in the research of references.

References

[1] Dillingham GL. Post-September 11th Initiatives and Long-Term Challenges. New York: United States General Accounting Office; 2004.

[2] Coughlin CC, Cohen JP, Khan SR. Aviation security and terrorism: a review of the economic issues. In: Federal Reserve Bank of St. Louis. Working Papers 2002-009A, St.Louis: 2004, p.1-16.

[3] Ito H, Lee D. Assessing the Impact of the September 11 Terrorist Attacks on U.S. Airline Demand. Brown University Economics Department. USA: 2003.

[4] Dillingham GL. Progress Since September 11, 2001, and the Challenges Ahead. New York: United States General Accounting Office; 2003.

[5] ICAO. Annex 17, Annexes to the Convention on International Civil Aviation, ICAO, Montreal: 2002.

[6] Salter MB (2007), SeMS and sensibility: Security management systems and the management of risk in the Canadian Air Transport Security Authority, Journal of Air Transport Management, pp. 389-398.

[7] Olapiriyakul S, Das S. (2007), Design and analysis of a two-stage security screening and inspection system, Journal of Air Transport Management, pp. 67-74

[8] Gkritza K, Niemeier D, Mannering F. (2006), Airport security screening and changing passenger satisfaction: An exploratory assessment Journal of Air Transport Management, pp. 213-219

[9] Lazar Babu VL, Batta R, Lin L. (2006), Passenger grouping under constant threat probability in an airport security system, European Journal of Operational Research, pp. 633-644

[10] Eiceman GA, Schmidt H, Cagan AA. (2007), Explosives detection using differential mobility spectrometry, Counterterrorist Detection Techniques of Explosives, pp. 61-90

[11] Xiaofeng Nie, Rajan Batta, Colin G. Drury, Li Lin (2009) Passenger grouping with risk levels in an airport security system, European Journal of Operational Research, 194 (2), pp. 574-584

[12] ICAO (2002) DOC 8973 Restricted - Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference, Annexes to the Convention on International Civil Aviation, ICAO, *Montreal, Canada, 2002*.

[13] Raymond J. Decker, (2003), Key Elements of a Risk Management Approach, United States General Accounting Office, *New York, USA, October 12 2001*. pp. 1-11.

[14] John Moteff, (2004), Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences, Congressional Research Service, *Washington, USA, September 2 2004*. pp. 1-27

[15] B. D. Jenkins, (1998), Security Risk Analisys and Management, Countermeasures Inc., *Hollywood, USA, 1998*. pp. 1-16

[16] R.Winther, O. Johnsen, B. Axel Gran (2001), Security Assessments of Safety Critical Systems Using HAZOPs, in the Proc. of Safecomp 2001, *Budapest, Hungary*, 26 – 28 September 2001.

[17] A.S. Barry, D.S. Mazel (2008), Airport Perimeter Security: Where we've been, Where we are, and Where we're going, in the Proc. of Technologies for

Homeland Security, 2008 IEEE Conference on Digital Object Identifier, pp. 57-62.

[18] Piccinini N, Ciarambino I. (1997), Operability analysis devoted to the development of logic trees, *Reliability Engineering and System Safety: 55* pp. 227-241:

[19] Demichela M, Marmo L, Piccinini N. (2002), Recursive operability analysis of a complex plant with multiple protection devices, *Reliability Engineering and System Safety 77*, Number 3, September 2002, pp. 301-308(8)

[20] M. Demichela, N. Piccinini, I. Ciarambino, S. Contini (2002), How to avoid the generation of logic loops in the construction of fault trees, *Reliability and Maintainability Symposium*, 2002. Proceedings, *Seattle, WA, USA*, pp. 178-185

[21] S. Scheer, S.M. Contini, M.A. Wilikens, G.G. Cojazzi, G.De Cola (1998) – ASTRA, an Integrated Tool Set for Complex Systems Dependability Studies. *Workshop on Tool Support for Systems Specification,Development and Verification* (TOOLS '98), Univ. Kiel, 2-4 June 1998, Malente (D) - ORA 41374

[22] S. Scheer, S.M. Contini, M.A. Wilikens (1999) – ASTRA FTA, a Powerful Software Tool for Fault Tree Analysis – Special Pubblications /I.99.51 – European Commission, Joint Research Centre, Ispra, VA, Italy

[23] S. Scheer, S.M. Contini, M.A. Wilikens (1999) – ASTRA PTD, Probabilistic Time Dependent Analysis Module of ASTRA – Special Pubblications /I.99.50 – European Commission, Joint Research Centre, Ispra, VA, Italy

[24] S. Scheer, S.M. Contini, M.A. Wilikens (1999) – ASTRA-SAM, a Powerful Software Tool for On-Line Sensitivity Analysis – Special Pubblications /I.99.49 – European Commission, Joint Research Centre, Ispra, VA, Italy

[25] EIREDA *European Industry Reliability Data Handbook*, C.E.C.- J.R.C./ICEI 21020 ISPRA (Varese) Italy, EDF-DER/SPT 93206 Saint Denis (Paris) France, 1991.

List of Caption