The DORATHEA Methodology for ATM Security Risk Assessment

José Neves, André Rocha and Bruno Tavares
Homeland Security and Defense
GMV Skysoft
Lisbon, Portugal
jose.neves@gmv.com, andre.rocha@gmv.com,
bruno.tavares@gmv.com

Francesca Matarese, Patrizia Montefusco and Daniela Dell'Amura
SESM Scarl
Naples, Italy
fmatarese@sesm.it, pmontefusco@sesm.it,
ddellamura@sesm.it

Abstract—**This paper presents the security risk assessment methodology developed within the DORATHEA project, and tailored for the ATM (Air Traffic Management) domain. Recent airline disasters, such as the 9/11 or the Concorde Air France flight 4590, have exposed weak points of the aviation system. Risk-based implementation of safety and security improvements proves to be the most cost-efficient response to passenger and regulatory demands of increased flight safety. While the SAM (Safety Assessment Methodology) methodology, developed by Eurocontrol, is regarded by most EU ATM stakeholders as the most fitting framework to perform safety risk assessment, there is little consensus on the most appropriate security risk assessment methodology. The objective of the DORATHEA project was the development of a common methodology for carrying out risk, threat and vulnerability assessments for ATM Critical Infrastructures (ATM-CI) protection. DORATHEA follows the strength features of SAM, striving to clearly define the respective responsibilities of all relevant stakeholders at each stage of the methodology. After the detailed presentation of the DORATHEA methodology, a few improvement points for the methodology will be briefly discussed, as well as future steps regarding the harmonization of ATM safety and security aspects.**

Keywords- security; risks; ATM; risk assessment; methodology

I. INTRODUCTION

Recent aircraft accidents have unmasked the shortcomings of the whole aviation network. In particular, the 2002 mid-air collision in Uberlinger, Germany, and the 1997 disaster in Buah Nabar, Indonesia, raised awareness for the crucial role of ATM (Air Traffic Management) and underlined the need for safety improvements in the ATM environment. In a similar fashion, the latest terrorist attacks, notably the 9/11 attacks in New York, revealed that the aviation system possesses vulnerabilities likely to be exploited by malicious individuals and organizations. As a response to the concerns of their citizens, in particular of airline passengers, governments dictated new regulations on security precautions and fostered the enhancement of aviation security. The enhancements put in place required tremendous investments.

As the study in [2] demonstrates, there are several different measures that can improve the security of a system that, in the end, may achieve the same result, but differ on one fundamental aspect: their cost. Organization directives urge for the solution that is the least costly while enabling the same level of protection as the more expensive ones.

Risk management focuses on the identification of hazards involved in each aspect of the operation, whether it involves aircraft flight operations, cockpit procedures, aircraft maintenance, turn-around, ticketing, scheduling, or baggage handling [1]. The risk-based approach implements a logic-driven process to analyze the degree of risk associated with identified hazards, allowing categorizing and prioritizing risks to propose the most fitting risk-mitigating solutions. This strategy avoids useless spends of money in elements that are not at considerable risk, or that are not at risk at all.

Security risk assessment is the determination of risks related to any event that compromises the assets, operations and objectives of an organization. These events pose threats (or hazards) to the system that can be intentionally acted upon by actors with the goal of producing undesirable results on the system; these actors are called attackers. This intentionality concept is what sets apart security risks from their safety counterparts.

ATM security risk assessment is viewed as the ongoing process of understanding the vulnerabilities, threats and consequences to the ATM-CI (ATM Critical Infrastructures), to determine which actions provide the greatest total risk reduction for the least impact on limited resources. It is crucially important to identify a threat in order to make a direct relation with appropriate measures, and it is equally important for this assessment to be monitored on a continuing basis to ensure that measures do not remain in force unnecessarily.

DORATHEA was an R&D project with the objective of developing a new security risk assessment methodology tailored for ATM-CI. The project partners, GMV Skysoft and SESM Scarl, sought to bring together key ATM stakeholders, namely ANSPs (Air Navigation Service Providers) and ATM security experts, in order to foster the discussion on best practices for carrying out security risk assessment; this was accomplished through 3 international workshops with an average participation of 25 key players. The conclusions derived from these project workshops were seized as guidelines for the development of the DORATHEA security risk

DORATHEA was a project co-financed by the European Commission, in the scope of the CIPS 2010 Programme

assessment methodology presented in this paper. Section II introduces the methodology and its 3 main phases, which are described in Sections III, IV and V. Section VI discusses future work on the methodology itself as well as other relevant research trends identified during project meetings.

II. The DORATHEA Methodology

The DORATHEA security risk assessment methodology was defined taking into account the strength points of the SAM (Safety Assessment Methodology) produced by Eurocontrol [3], at the same time striving to incorporate key aspects of the SecRAM (Security Risk Assessment Methodology) developed in SESAR (Single European Sky ATM Research). Similarly to SAM, DORATHEA clearly preserves the distinction of roles and responsibilities:

- ANSPs are responsible for operations, have the first and the last word on the whole security assessment process;
- System manufacturers, who have the knowledge of equipment, have to identify Security Requirements in order to satisfy the Security Objectives identified by the ANSPs.

As suggested by ISO (International Organization for Standardization) [5] and SESAR [4], DORATHEA considers two types of assets:

- **Primary assets**: are the intangible activities, information and services that contribute to have the functionalities of the system to be protected;
- **Supporting assets**: are the physical entities which enable the primary assets. They are of various types, including for example hardware, software, operating systems, networks, storage media, communication interfaces, personnel, sites, subcontractors, authorities and organizations.

The DORATHEA methodology approaches the security risk assessment process through a clearly defined workflow comprising three main phases:

- **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, evaluating system functionalities, identifying potential Security Hazards and assessing the consequence of their occurrence on the system, produces the system's Security Objectives.
- **PSSecA (Preliminary System Security Assessment)** aims at evaluating if the proposed architecture is expected to achieve a tolerable risk. It is a process that produces system requirements related to security, i.e. Security Requirements, in order to satisfy all the Security Objectives defined in the 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 the system elements meet the Security Requirements specified in the PSSecA.

Each of these methodology stages will be detailed in the next sections.

III. SecFHA – Security Functional Hazard Assessment

SecFHA is the first phase of the DORATHEA security risk assessment methodology. It is a top-down iterative process, starting at the beginning of the development or modification of an Air Navigation System (ANS). The objective of the SecFHA step is to determine how secure the system needs to be.

This stage is under the responsibility of ANSPs, who are in charge of identifying the Security Objectives of the system under evaluation.

The process identifies Security Hazards of the system and assesses the consequences of their occurrences. In particular, the steps to be performed during the SecFHA are:

- Identifying the system's Security Hazards, which implies:
  - Identifying all system functionalities;
  - Classifying all system functionalities in terms of the Impact of loss of CIA (Confidentiality, Integrity and Availability) and the Appeal of causing the loss of CIA. For each functionality, the operational effects of the loss of CIA will be described and linked to the Impact classification;
  - Selecting the highest priority subset of system functionalities based on the previous classification;
  - Identifying all potential Security Hazards associated with the system and related to the most critical functionalities;
  - Deriving the Impact of the Security Hazards' effects;
- Deriving the system **Security Objectives**, i.e. determine the Security Hazards' maximum Likelihood of Occurrence, derived from the Impact and the maximum Appeal of the Security Hazards' effects.

A. Identification of Security Hazards

1) Identification of System Functionalities

The first step of this methodology is for the ANSPs to identify the functionalities they are expecting the system under evaluation to provide. The output is a System Functionalities Table (SFT) composed by two columns: a Functionality ID shall be assigned to each functionality to ease future reference of that functionality (e.g. FUNC_01); the Functionality Description shall consist of a short description of the functionality provided (e.g. message exchange service).

2) *Categorization of System Functionalities*

On the basis of the SFT, ANSPs shall next select the highest priority subset of system functionalities to be protected. The criterions for this selection are two, as it will take into consideration not only the Impact that the loss of either Confidentiality, Integrity or Availability of the functionality will bring about, but also the Appeal of causing the loss of either Confidentiality, Integrity or Availability.

In other words, this phase will individually tackle the loss of Confidentiality, Integrity and Availability of each system functionality to decide whether it is a critical event or not. To this end, we will consider the impact that the loss of CIA will have, discriminating this impact by each of the 7 Impact Areas as defined in SESAR (see [4]).

TABLE I. SECURITY IMPACT AREAS

Impact Areas	**5. Catastrophic**	**4. Critical**	**3. Severe**	**2. Minor**	**1. 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 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 & 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 environment	Severe pollution with long term impact on environment	Severe pollution with noticeable impact on environment	Short Term impact on environment	Insignificant

This impact is a number from 1 to 5 as reported in TABLE I. Comparison shall not be done between impact areas, as they should be evaluated independently. For each system functionality, and for each loss of CIA event, the final impact value will be the maximum impact level from this evaluation.

All the possible consequences and operational effects will be identified and the impact of these consequences will be established. These consequences are then translated into IAs categories. This Impact analysis will be translated into a table as depicted in TABLE II.

TABLE II. IMPACT ANALYSIS FOR THE LOSS OF EACH CIA ATTRIBUTE FOR EACH SYSTEM FUNCTIONALITY

Loss of CIA attribute	**Loss of CIA Operational Effect**	**Loss of CIA Impact**						
		IA1	IA2	IA3	IA4	IA5	IA6	IA7
Loss of CIA attribute of system functionalities (e.g. Loss of C of FUNC_01)	Effect on operations of the loss of CIA attribute of system functionalities	Impact of the loss of CIA attribute of system functionalities						

On the other hand, the Appeal of each system functionality will also have to be considered. The appeal is the evaluation of the desirability of an attack to the functionality. The appeal of the loss of CIA is a number from 1 (very low) to 5 (very high), with the qualitative definition depicted in TABLE IV.

In order to systematize the assignment of appeal levels, 7 Appeal Factors will be considered as specified in TABLE III. These parameters shall be used to explain the choice of the selected Appeal level. The appeal level of the loss of CIA event will be the floor of the average appeal of all the Appeal Factors.

TABLE III. APPEAL FACTORS

Appeal Factors	**Very High**	**High**	**Medium**	**Low**	**Very Low**
AF1: Elapsed Time	Minutes	Hours	Days	Weeks or Months	Years
AF2: Expertise	Script kiddie (no skill required)	Basic adult level skills	Higher education skills	Area specific skills	Expert level skills
AF3: Knowledge of the Target	No knowledge	Black box level knowledge	High level architecture knowledge	Low level architecture knowledge	Implementation / design level knowledge
AF4: Equipment	No equipment	Common utensils	Target-specific equipment	Government-controlled equipment	Military grade equipment
AF5: Feeling of Impunity	Assured impunity	Almost assured impunity	Impunity under specific circumstances	Very doubtful impunity	No impunity
AF6: Window of Opportunity	Any time during the system lifecycle	Most time frames during the system lifecycle	Few time frames during the system lifecycle	Almost no time frames during the system lifecycle	No time frames or one short and specific time frame during the system lifecycle
AF7: Attractiveness of the Target	Very high reward	High reward	Medium reward	Low or dubious reward	No reward

Thus, at this stage the system evaluators should produce a table as outlined in TABLE V. for each CIA attribute. This will allow obtaining the Impact and Appeal for the loss of each CIA attribute, which in turn will be used to determine the priority of protecting that system functionality from the loss of each CIA attribute. The values in TABLE V. are given just as an <u>example</u> to aid in understanding the priority scheme.

TABLE IV. APPEAL SCHEME

Appeal	Qualitative Interpretation
5. Very High	There is a very high desire of attacking the functionality.
4. High	There is a high desire of attacking the functionality.
3. Medium	There is some desire of attacking the functionality.
2. Low	There is little desire of attacking the functionality.
1. Very Low	There is no desire of attacking the functionality.

TABLE V. IMPACT AND APPEAL OF THE LOSS OF SYSTEM FUNCTIONALITIES' CONFIDENTIALITY

	Impact due to the loss of Confidentiality								Appeal of causing the loss of Confidentiality							
Functionality ID	IA1	IA2	IA3	IA4	IA5	IA6	IA7	max Imp	AF1	AF2	AF3	AF4	AF5	AF6	AF7	avg App
FUNC_01	2	2	3	2	4	1	3	4	3	4	1	5	2	2	2	2

The priority level is attributed in accordance to the priority scheme in ATM illustrated in TABLE VI. For all Impact classes which mean that the system is actually impacted (2. Minor to 5. Catastrophic), the Appeal of the loss of a functionality's CIA attribute will directly influence how important it is to address that potential Loss. The same cannot be said for the Impact class 1. No Impact which, regardless of the Appeal, does not need to be considered, as the system is not being impacted. Only functionalities with High priority levels will be selected as the subset of critical functionalities.

TABLE VI. PRIORITY CLASSIFICATION SCHEME IN ATM

		Appeal				
		1. Very Low	2. Low	3. Medium	4. High	5. Very High
Impact Class	5. Catastrophic	🟥	🟥	🟥	🟥	🟥
	4. Critical	🟩	🟥	🟥	🟥	🟥
	3. Severe	🟩	🟩	🟥	🟥	🟥
	2. Minor	🟩	🟩	🟩	🟥	🟥
	1. No impact / NA	🟩	🟩	🟩	🟩	🟩

🟩 Low 🟥 High

In the example of TABLE V. an Impact of 4 and an Appeal of 2 will yield a High Priority functionality in terms of loss of Confidentiality. The same process shall also be conducted for both the functionality's Integrity and Availability.

Therefore, we will ultimately identify the highest priority system functionalities, while simultaneously pinpointing which of the CIA properties contribute to make the functionality critical from a security point of view. This will be of use in the identification of potential Security Hazards.

3) *Identification of Potential Security Hazards*

A Security Hazard is defined as any condition, event, or circumstance which could lead to the loss or the corruption of the critical system functionalities.

The identification of all potential Security Hazards is performed through brainstorming sessions aiming at defining all the potential Security Hazards, on the basis of the identified critical CIA losses of functionalities. This means that for each diagnosed critical loss of a functionality's Confidentiality, Integrity or Availability, one or more Security Hazards will have to be identified.

A Security Hazards Table (SHT) will be outputted, and it shall include the Security Hazard unique identifier (e.g. SH_01) and respective description (e.g. theft of messages of the message exchange service), as well as the consequences at functionality level (e.g. loss of Confidentiality of FUNC_01) and the respective Security Hazard Impact. This Impact will be inherited from the Impact of the Security Hazard consequences on the critical system functionalities as set out in the previous point.

B. *Definition of Security Objectives*

Each Security Objective specifies for each identified Security Hazard the maximum tolerable Likelihood of its Occurrence, given its assessed Impact.

The definition of Security Objectives is performed using the Risk Classification Scheme reported in TABLE VII.

TABLE VII. RISK CLASSIFICATION SCHEME IN ATM

		Likelihood of Occurrence				
		1. Very Unlikely	2. Unlikely	3. Likely	4. Very Likely	5. Certain
Impact Class	5. Catastrophic	🟨	🟥	🟥	🟥	🟥
	4. Critical	🟩	🟨	🟥	🟥	🟥
	3. Severe	🟩	🟩	🟨	🟥	🟥
	2. Minor	🟩	🟩	🟩	🟨	🟥
	1. No impact / NA	🟩	🟩	🟩	🟩	🟨

🟩 Acceptable 🟨 Tolerable 🟥 Unacceptable

As defined in SESAR [4], the Likelihood of Occurrence of an attack is the evaluation of the chance of an event successfully occurring. The likelihood of the loss of CIA is a number from 1 (improbable) to 5 (frequent), with the qualitative definition depicted in TABLE VIII.

Thus, for each identified Security Hazard, the Security Risk associated to it will be evaluated as follows:

$$Security\ Risk = L_{sh} \times I_c \tag{1}$$

Where L_{sh} indicates the Likelihood of Occurrence of the given Security Hazard and I_c stands for the Impact of the consequences of the Security Hazard.

The Risk Classification Scheme is used in order to fix the maximum tolerable Likelihood of Occurrence of a determined Security Hazard, given its assessed Impact, in order to achieve a tolerable risk. This corresponds to the Security Objective linked to that Security Hazard.

TABLE VIII. LIKELIHOOD SCHEME

Likelihood of Occurrence	Qualitative Interpretation
5. Certain	There is a high chance that the event successfully occurs in the short term.
4. Very likely	There is a high chance that the event successfully occurs in the medium term.
3. Likely	There is a high chance that the event successfully occurs during the lifetime of the project.
2. Unlikely	There is a low chance that the event successfully occurs during the lifetime of the project.
1. Very Unlikely	There is very little or no chance that the event successfully occurs during the lifetime of the project.

The output of this phase will be the Security Objectives Table (SOT) listing the Security Objectives associated to the system. Each line of this table will specify a Security Objective (SO), attributing a unique ID, fixing the Security Hazard it concerns, and stipulating the SO Description as the maximum Likelihood of Occurrence of the SH that yields a tolerable risk, in accordance to TABLE VII.

IV. PSSecA – Preliminary System Security Assessment

PSSecA is the second phase of the DORATHEA security risk assessment methodology. The objective of the PSSecA process is to evaluate if the proposed architecture is expected to achieve a tolerable risk.

It is a top-down iterative process, conducted during the system design phase of the system lifecycle. PSSecA should be performed for a new system or each time there is a change to the design of an existing system. The essential pre-requisite for conducting PSSecA is a description of the high level functions of the system.

This phase is under the responsibility of the ATM system providers, who are in charge of deriving the Security Requirements for each individual system element under evaluation, in order to satisfy the Security Objectives of the system.

The system architecture can only achieve the Security Objectives established during the SecFHA if the architecture elements meet their Security Requirements. As such, this core stage of the methodology is in charge of assessing the supporting assets' underlying threats and vulnerabilities and, based on the incidents leading to the non-fulfilment of the Security Objectives, derive the system's Security Controls and respective Security Requirements.

The distilling of Security Objectives into Security Requirements allocated to the system elements is performed through two analyses:

- **Attack Tree Analysis (ATA)**: is a functional analysis that aims at identifying the logical combination of Security Incidents leading to the non-fulfilment of the Security Objectives.
- **Identification of Vulnerability and Effects Analysis (IVEA)**: is a physical analysis and aims at evaluating if the supporting assets linked to the Security Objectives are vulnerable to the identified threats. Every supporting asset must be linked to the primary assets that it is supporting, and only the supporting assets possess the vulnerabilities that are exploitable by threats, i.e. only the supporting assets are directly attackable. In this view, it is immediate that a Security Objective is satisfied if the primary assets that provide the functionalities associated to it are protected, and the primary assets are protected if and only if the supporting assets supporting them are not attackable.

The combination of the ATA and the IVEA analyses allows identifying how critical the supporting assets are and, consequently, to define the **Security Controls** in a cost-effective way. The Security Controls will be traced to the system requirements that will become **Security Requirements**.

A. ATA – Attack Tree Analysis

Security Incidents are one or more unwanted or unexpected security events that could very likely compromise the security of the organization and weaken or impair business operations.

The ATA graphically shows how a system's functionality (related to a Security Objective) can be attacked. The topmost node represents the attacker's goal. This overall goal is decomposed into nodes representing increasingly detailed tasks which, by themselves or in combination, will result in the attacker obtaining their objective. The focus is on the system's primary assets.

In order to build the attack trees, the following is applied:

1. The Security Objective to be analyzed is the top event of the tree;
2. All the Security Incidents that contribute to the non-fulfilment of this top event are identified;
3. The Security Incidents identified in point 2 are correlated between themselves through logic gates (AND / OR gates) until the top event is reached;
4. For each Security Incident identified in point 2 that seems to be not enough detailed, the Security Incidents that lead to it have to be identified and correlated through logic gates;
5. From the Security Objective defined as the top event of the tree, the Incident Criticality for each identified Security Incident is derived.

The symbols used for the ATA building are explained in TABLE IX. To build the attack tree of a given Security Objective, the immediate Security Incidents (SI) that lead to the non-fulfilment of that Security Objective are considered and correlated, e.g. if a given Security Incident SI_01 and another SI_02 directly conduct to the non-fulfilment of the SO, then they are correlated via an OR gate. This process is iterated through all identified Security Incidents until the circumstances that might lead to the non-fulfilment of the Security Objective are all evident.

TABLE IX. ATA SYMBOLS

Symbol	Description
OR	Or gate: the Security Incident occurs if at least one of the input Security Incidents are in place
AND	And gate: the Security Incident occurs if, and only if, all the input Security Incidents are in place
TRANSFER	Transfer gate: the gate is a reference to another sub-tree
BASIC EVENT	Basic event: it indicates a Security Incident

The Incident Criticality is a measure of how critical each Incident is in relation to the non-fulfilment of the Security Objective. In other words, the Incident Criticality reflects the chance that, in case the respective Security Incident occurs, the Security Objective is not achieved and the system is impacted. In light of this, 5 levels of Incident Criticality are defined, as shown in TABLE X.

TABLE X. INCIDENT CRITICALITY SCHEME

Incident Criticality	Qualitative Interpretation
5. Very High	There is a very high chance that the Security Incident leads to a non-tolerable impact on the system.
4. High	There is a high chance that the Security Incident leads to a non-tolerable impact on the system.
3. Medium	There is a medium chance that the Security Incident leads to a non-tolerable impact on the system.
2. Low	There is a low chance that the Security Incident leads to a non-tolerable impact on the system.
1. Very Low	There is a very low chance that the Security Incident leads to a non-tolerable impact on the system.

The Incident Criticality of a given Security Incident is deduced from the Likelihood of Occurrence of the Security Hazard as specified by the Security Objective, as well as from the combination of logic gates that lead the Security Incident to the upper event:

- In case of an OR gate above the considered Security Incident, the Incident Criticality figure of this SI is inherited from the one of the upper Security Incident;
- In case of an AND gate above the considered Security Incident, the Incident Criticality figure of this SI is inherited from the one of the upper Security Incident, decreased by one value. If the Incident Criticality of the upper SI is equal to 1 and hence cannot be decreased, the Incident Criticality figure of this SI is equal to the one of the upper SI;
- In case the upper Security Incident of a given SI is the SO, its derived Incident Criticality figure will be the reversed maximum tolerable Likelihood of Occurrence of the SH as specified by the SO. TABLE XI. presents the conversion between these schemes.

TABLE XI. CONVERSION BETWEEN LIKELIHOOD AND INCIDENT CRITICALITY

Likelihood of Occurrence	Incident Criticality
1. Very Unlikely	5. Very High
2. Unlikely	4. High
3. Likely	3. Medium
4. Very Likely	2. Low
5. Certain	1. Very Low

The attack tree paradigm is well evidenced in the example of Figure 1. It ultimately yields the Incident Criticality of each Security Incident linked to a given Security Objective.

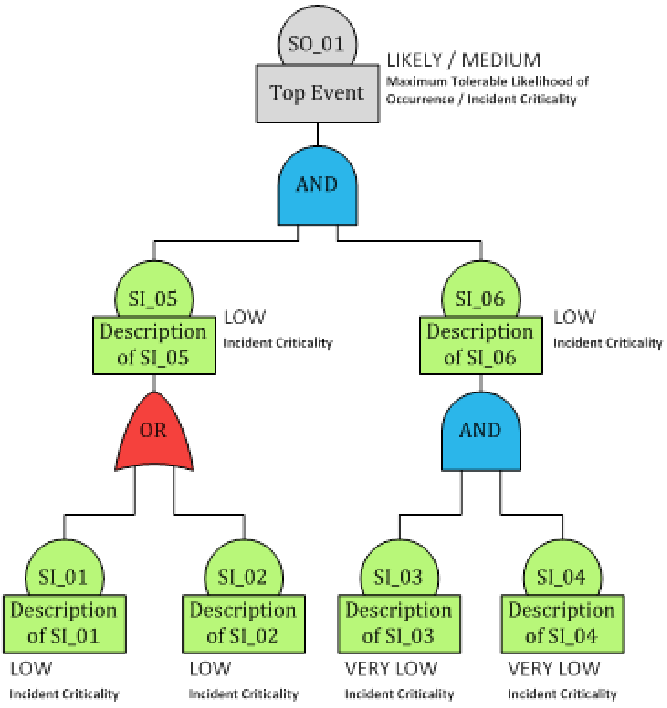

Figure 1. Example of an Attack Tree Analysis

In addition to the attack trees for the system's Security Objectives, the ATA will output the Security Incidents Table (SIT). This is a table listing all the identified Security Incidents, including each incident's maximum Incident Criticality as well as the Security Objectives it impacts. It should be noted that the same Security Incident can be linked to several Security Objectives and thus possess different criticalities depending on the Security Objective. The maximum criticality will be bound to the attack tree where the Security Incident possesses its maximum Incident Criticality.

B. IVEA – Identification of Vulnerabilities and Effects Analysis

IVEA is performed on the physical components of the system under evaluation, i.e. on the system's supporting assets. The objectives of this analysis are to identify the system vulnerabilities, evaluate how an attacker can use them (i.e. the list of threats that exploit the vulnerability), and reckon which Security Incidents are provoked by these threats.

Thus, the consequences of a threat's attack on a given supporting asset will be traced to the Security Incidents identified through the ATA and related to the system's primary assets.

The identification of threats and vulnerabilities will be accomplished through brainstorming sessions. The most common vulnerabilities and threats, as suggested by ISO 27005 [5], can be used as an auxiliary guide to produce the IVEA analysis.

TABLE XII. IVEA TABLE

Supporting Assets	**Vulnerabilities**	**Threats**	**Security Incidents**	**Maximum Incident Criticality**	**Security Controls**	**Derived Security Requirements**
Name of the physical component	Vulnerabilities of the supporting asset	Threats that are able to exploit the vulnerabilities of the supporting asset	Security Incidents, identified in the ATA, that are caused by the selected threats	It indicates the maximum Incident Criticality of all the identified incidents in the previous column	Possible Security Controls to be applied to the supporting asset to avoid, counteract or minimize the Security Risks	Security Requirements of the system linked to both Security Incidents and Security Controls

The input of this analysis will be the design information of the system that allows establishing which supporting assets enable the primary assets that provide the functionality associated to a given Security Objective. The analysis follows the next steps:

1. The list of supporting assets is considered;
2. The vulnerabilities of each supporting asset are identified;
3. The list of threats is considered. Each threat will be traced to a determined supporting asset if the latter is vulnerable to the former;
4. The Security Incidents that are caused by the threats related to the supporting asset under scope will be linked. This task implies the assessment of the threats' consequences in terms of Impact, and thus entails relating the supporting assets to their underlying primary assets. These Security Incidents were identified during the ATA analysis, and can be referred by their IDs. Only Security Incidents at the bottom of the attack trees will be considered;
5. The maximum Incident Criticality of all the pinpointed Security Incidents will be set;
6. The most appropriate Security Controls (SC) to mitigate or prevent the threat's effects will be selected;
7. The system Security Requirements will be derived.

The IVEA table is pictured in TABLE XII.

The IVEA process presupposes the selection of the most appropriate Security Controls for each identified Security Incident connected to a specific supporting asset. Security Controls will be dependent on the types of threats and vulnerabilities related to the supporting asset, and also on the latter. Various examples of typical Security Controls are given by the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce in [6] and [9], and by the SANS (SysAdmin, Audit, Networking, and Security) Institute [7]. Of course, brainstorming sessions shall also be of use for this task. The Security Controls of the system will be organized in a Security Controls Table (SCT). This table indicates which SIs are countered by each SC; as before, only SIs at the bottom of the attack trees will be considered.

Security Requirements (SR) are requirements linked to Security Controls. They act as mitigation means or as operational, procedural or functional requirements and they help to satisfy the fulfilment of the Security Objectives. The Security Requirements of the system shall be gathered in a Security Requirements Table (SRT). This table includes a column linking SCs to SRs, and another column that references the SO that originated each SR.

C. Risk Treatment

Security Controls are means of managing Security Risks, including policies, procedures, guidelines, practices or organizational structures. Security Controls may be classified by several different criteria. They can be categorized according to the time they are put in place in relation to the occurrence of a Security Incident (see [7]) as Preventive (e.g. by locking out unauthorized intruders), Detective (e.g. by sounding the intruder alarm and alerting the security guards or the police), or Corrective (e.g. by recovering the organization to normal working status as efficiently as possible).

As reported by NIST in [6], Security Controls can be further classified as Management Controls (e.g. legal and regulatory or compliance controls, such as privacy laws, policies and clauses), Operational Controls (e.g. incident response processes, management oversight, or security awareness and training), or Technical Controls (e.g. user authentication and logical access controls, antivirus software, or firewalls, as well as more physical controls such as fences, doors, locks or fire extinguishers).

As a result of the PSSecA phase, through the ATA and IVEA analyses, the system's Security Requirements shall be directly derived from the Security Controls identified for a given supporting asset. The Security Requirements must be linked to the system's Security Objectives, and consist of documented physical and functional needs that the system must be able to deliver. As such, each Security Requirement will be a statement that identifies a necessary attribute, capability, characteristic or quality of the system for it to be protected from a security point of view against intentional attackers. Security Requirements specify the potential means to avoid or mitigate Security Incidents (refer to [3]), i.e. to:

- Prevent the occurrence of incidents: Precautions for system and equipment design, development, procurement and validation; Precautions for procedures design and validation; Precautions for people training and licensing;
- Reduce the impact of incidents' consequences: Detection; Protection; Recovery (automatic or human intervention); Graceful degradation (deliver a reduced service in degraded mode).

In conclusion, Security Requirements aim at preventing or mitigating the effects of a given supporting asset's vulnerabilities on the overall system's security. It is up to the SRs to make sure that the SIs are not attainable, and consequently that the SOs are satisfied.

V. SSecA – System Security Assessment

SSecA is the last step of the methodology. This phase aims at evaluating if the implemented architecture achieves a tolerable risk. SSecA is a top-down iterative process under the responsibility of the ATM systems providers, and is led during system integration, validation and on-site acceptance. The process produces assurance that the Security Objectives are satisfied and that system elements meet their Security Requirements. The correct implementation of Security Controls will be demonstrated through:

- Verification and Validation activities;
- Security metrics: a measure of the Security Risk.

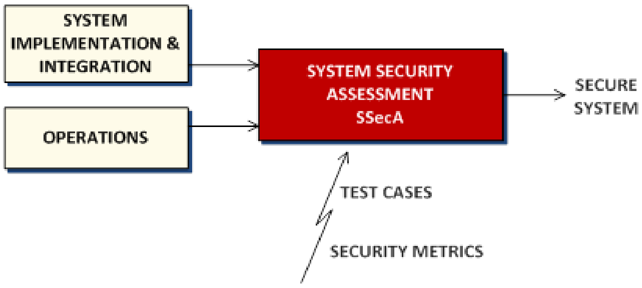
SYSTEM IMPLEMENTATION & INTEGRATION
OPERATIONS
SYSTEM SECURITY ASSESSMENT SSecA
SECURE SYSTEM
TEST CASES
SECURITY METRICS

Figure 2. Overview of the SSecA phase

A general outline of SSecA can be seen in Figure 2.

VI. Next Steps

In the final stages of the project, the methodology was used to perform the security risk assessment of a real system. This, together with the feedback obtained from security experts at the last project workshop, led to the identification of improvement points for the methodology, notably:

- There is a need to systematize the identification and categorization of system functionalities to protect;
- The assignment of the attack appeal should be postponed until system implementation details are known;
- A database of known attacks would be useful to build the attack trees in the ATA analysis;
- Threats' propagation and vulnerabilities resulting from the integration of legacy and new systems would be useful additions to the framework;
- The impact of proposed Security Controls, namely their cost, should be taken into account when selecting them.

Finally, we have also pinpointed a new topic of the upmost relevance: a framework to assure the harmonization of safety and security in ATM. This research theme responds to real industry needs and will certainly feature in future R&D proposals.

Acknowledgment

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 Home Affairs (Registration number HOME/2010/CIPS/AG/030, DORATHEA Project).

References

[1] Southern California Safety Institute (SCSI). Operational Risk Management (ORM). Retrieved February 20, 2014, from http://www.scsi-inc.com/orm.php

[2] Robert W. Poole Jr. Toward Risk-Based Aviation Security Policy. Discussion Paper No. 2008-23, Joint Report Research Centre, November 2008

[3] Eurocontrol. Safety Assessment Methodology (SAM). Retrieved February 20, 2014, from http://www.eurocontrol.int/articles/safety-assessment-methodology-sam

[4] SESAR. WP16.2 – ATM Security. Deliverable 16.02.03 D02 – SESAR ATM Security Risk Assessment Method, Ed.01.01.

[5] ISO/IEC. ISO/IEC 27005:2008 Information technology – Security techniques – Information security risk management, Ed. 1.0, June 2008.

[6] National Institute of Standards and Technology (NIST). Information Security: Recommended Security Controls for Federal Information Systems and Organizations, Revision 3, August 2009.

[7] SysAdmin, Audit, Networking, and Security (SANS) Institute. Security Controls. (September 1, 2009). Retrieved February 20, 2014, from http://www.sans.edu/research/security-laboratory/article/security-controls

[8] SysAdmin, Audit, Networking, and Security (SANS) Institute. Twenty Critical Security Controls for Effective Cyber Defense. Retrieved February 20, 2014, from http://www.sans.org/critical-security-controls/

[9] National Institute of Standards and Technology (NIST). Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, April 2013.

[10] GMVIS Skysoft and SESM Scarl. The DORATHEA methodology for ATM security risk assessment: methodology practical guide. DORATHEA, December 2013

[11] International Organization for Standardization (ISO). Archive of plain English ISO 27001 2005 definitions. (November 26, 2013). Retrieved February 20, 2014, from http://www.praxiom.com/iso-27001-definitions.htm