Agent-based security risk assessment of the airport security system

B.M. Meijer

Agent-based security risk assessment of the airport security system

By

B.M. Meijer

in partial fulfilment of the requirements for the degree of

Master of Science
in Aerospace Engineering

at the Delft University of Technology,
to be defended publicly on Thursday September 7, 2017 at 10:00

Thesis committee:	Dr. A. Sharpanskykh,	TU Delft, supervisor
	Prof. dr. R. Curran,	TU Delft
	Ir. M. Schuurman	TU Delft

Background: *https://architizer.com/projects/john-f-kennedy-international-airport-international-arrivals-building-terminal-4/*

Abstract

The thought of being secure has been on the minds of people throughout history. First and foremost security is used in a physical meaning as the protection against a harmful action against a person. Furthermore, security can consider objects, resources, information and economical assets. However, security is not something self-evident [1]. A threat can be exposed in various forms upon this notion of security. A characteristic of a threat in the security domain is that the threat is performed with a certain intend from the attacker [2].

In recent years especially security in aviation is getting more and more important. Threats were revealed which were before unthinkable for everybody. Especially the 9/11 attacks and several other attacks on airports before and after this horrendous act showed the vulnerability of the airport environment [3]. The airport environment is an interesting target. It is a major way port to destinations all over the world, the growing demand of air travel makes that there is a huge amount of people present within the airport environment and there are many valuable assets which can fall victim to considerable damage [4]. Therefore an airport security system is present in the airport environment in order to timely identify the threat sources and objects such that an attack is prevented from happening. It is the utmost importance that the airport security system performs in the most efficient way. Although, the need for universal and rapid deployment of individual security systems to tackle prominent threats have led to a stand-alone way of working of these systems.

The airport security system is a complex socio-technical system. It consist of many different actors, both human operators and technical systems. Although all these different actors are present, the current airport security system appears to perform in a more stand-alone way of the individual security systems. The stand-alone way of working inhibits the communication of security data between individual security systems. Which means that a more conservative operational configuration must be used. The hypothesis reads that this stand-alone way of working does not exploit the full efficiency of performance of the airport security system. In other words, a different approach could lead to an increased performance. Therefore the research questions of this research are: How can the current airport security system be integrated and how does the systemic integration of this airport security system react on specific airport threats?, What is the difference in performance between the current stand-alone airport security system and the newly designed integrated airport security system? and How does an adaptive mechanism in the integrated airport security system influence the performance?. The current airport security system is modeled as a baseline, where after a new integrated airport security system is designed. This airport security system uses decision data fusion. By integrating the data from individual security systems it is believed that the performance can be increased [5]. Data fusion is a technique that is executed by an additional system that transforms the incoming individual data into a general reference frame, then links data that can be associated to achieve a higher efficiency, builds a risk profile for every passenger based on this linked data, estimates the perceived threat level based on the risk profile and communicates this threat level to the security systems such that the most appropriate action can be undertaken.

The performance of the airport security system is investigated by means of a security risk assessment. The main steps during the security risk assessment are the investigation of the boundaries of the research, the construction of a security risk scenario [6], the construction of the conceptual model and finally the implementation of the conceptual model [7].

The airport environment is a very broad area that can be considered, with all the possible threats, the boundaries of the airport premises, the airport security system and its vulnerabilities, the attackers and the way in which the attacker executes the planned attack. The propagation of a threat through the airport terminal into an aircraft is seen as one of the most dangerous threats and is an interesting

research domain. The boundaries of the security risk scenario are therefore set by the airport terminal. The airport security system is then considered from the arrival into the airport terminal all the way to the entrance of the aircraft [8]. A wide variety of individual security systems are present in this environment. Attackers can be categorized based on their level of expertise and characteristics. These personal characteristics can be exploited by the airport security system to identify these passengers as attackers. Different types of attackers with different ways of executing the attack are therefore present in the security risk scenario in order check the agility of the airport security system.

An agent-based modeling and analysis framework, [9], is used to build a conceptual model of both the current airport security system and the newly designed integrated airport security system. The conceptual model is based on four views, respectively the organizational view, the agent view, the process view and the performance view. All views show an unique part of the conceptual model, but are related. The agent-based approach models the behaviors of all agents in the system individually, while also the relationships between agents can be defined.

The main goals of the airport security system are the detection of all attackers present in the airport environment, minimization of detection of false positives and to present a high level of service to the passengers undergoing the airport security processes. A trade-off needs to be made between the security performance and service performance however. The research shows the difference between the stand-alone and integrated airport security system.
Four different case studies are performed. One with the current stand-alone airport security system and three different configurations for an integrated airport security system, respectively a simple decision data fusion configuration requiring three different alarms for a positive identification, a complex decision data fusion configuration with weighed security systems still requiring three alarms for a positive identification and an adaptive approach of an integrated airport security system.

It is found that integration of the airport security system only works when a wide variety of sensors is present in the airport environment. If so, the adaptive integrated airport security system acts as the most trustworthy of all integrated configurations. Moreover, when comparing the performance with the current airport security system, the adaptive configuration shows much better results with respect to the detection of false positives and thus the service performance while maintaining the same performance of detection of attackers. A decrease from 60% to 21% of detection of false alarms is found, while remaining the detection of attackers close to 100%. The delay passengers encounter at a checkpoint such as the passenger security check decreases with just over 10% in case of the adaptive integrated approach with respect to the current airport security system. These results look promising, but are only represent the security risk scenario considered in this research. These results require further study and validation.

Preface

The basis for this research arose from the current perception of security, especially in large public areas such as the airport environment. On the one hand people ask for stricter security measures, but on the other hand the level of service and throughput should be as high as possible. These are contradicting goals. However, with the ever growing demand for air travel the situations at airports need to change in order to guarantee an effective level of security and level of service. By using an innovative way of modeling the airport environment regarding a security risk scenario this contradiction is examined. This research is one of the first in this domain, for sure at the technical university of Delft, and can be categorized as an exploratory research.

The period in which I performed the research was a very interesting and fruitful time, however not by any means straightforward. I have learned a lot about the security domain, the airport environment, performing security risk assessments and the innovative way of modeling with LEADSTO. The fact that the topic is really relative nowadays and that some aspects of this research were unknown to me before, increased the curiosity to gain knowledge. Moreover, I have learned a lot about myself simultaneously. In truth, I could not have achieved my current level of success without the support around me. I would like to thank all the people around me for their enduring and strong support throughout this period. First of all my parents, who supported me with love, understanding, inspiration, patience and encouragements, not only during this research period but my entire study program. Secondly my close friends and girlfriend, who supported me with love, understanding and company in this period of my life. Thirdly my fellow university colleagues, who supported me with the enjoyable work environment and knowledge. And last of all my supervisors, especially dr. Alexei Sharpanskykh, who has provided patient advice and guidance for this research and shared his expertise in this domain.

Contents

1 Introduction

Security is one of the most important goals for society. First and foremost security is used in a physical meaning as the protection against a harmful action against a person. Furthermore, security can consider objects, resources, information and economical assets. However, security is not something self-evident. A threat can be exposed in various forms upon this notion of security. A characteristic of a threat in the security domain is that the threat is performed with a certain intend from the attacker. Therefore, security systems are built in order to set up security precautions which have as main goal the protection of all assets present within the environment under supervision.

In recent years especially security in aviation is getting more and more important. Threats were revealed which were before unthinkable for everybody. Especially the 9/11 attacks and several other attacks on airports before and after this horrendous act showed the vulnerability of the airport environment. The airport environment can be an interesting target. It is a major way port to destinations all over the world, the growing demand of air travel makes that there is a huge amount of people present within the airport environment and there are many other valuable assets. Therefore an airport security system is present in the airport environment in order to timely identify the threat sources.

Due to the existence of security threats within the airport environment and the extensive use by society of this airport environment it is the utmost importance that the airport security system performs in the most efficient way. Travelers may not see the complex socio-technical infrastructure that is built to protect them against the ever evolving broad diversity of threats. The airport security system consists of multiple individual security systems, both human operators and technical systems. However, the need for universal and rapid deployment of individual security systems prevented the set-up of communication and integration among these systems. This means that the individual security systems currently work in a more stand-alone configuration. Additionally, a trade-off needs to be addressed by the airport security system as well. A high level of security needs to be maintained, while also a high level of service needs to be provided. Although the security at current airports is of course of a good level, the airport security system in this stand-alone way may not operate at its most efficient configuration.

A security risk assessment is one of the main activities in security research. This assessment forms the basis for the steps to be executed. The airport environment should regularly be subjected to an analysis of the performance of the airport security system in order to account for the evolving threats. After the 9/11 attacks airports all over the world implemented specially assigned individual security systems in their overall airport security system. The organizational structure has not changed since then, while the technique is becoming more modern. Two interesting aspects can be highlighted from the current airport security system. First of all the characteristic that the airport security system is a complex socio-technical system. Which means that both humans and technical system work together. In order to utilize the socio-technical nature of the airport security system an agent-based modeling method is used instead of the general computational models. Agent-based modeling is one of the few modeling frameworks that allows representing and analyzing socio-technical systems. Agent-based methods can define individual actors in a system and set up rules for their individual behavior as well as the relationships with other individual actors. Secondly, the characteristic that the current airport security system has a more stand-alone way of working of the individual security systems. The stand-alone gives the impression that the airport security system can operate in an even more efficient configuration. The modern technology will be used to make a design of a new type of the airport security system, based on the current structure. Integration is the key word. Integration of systems is more and more implemented in complex systems with the prospect of increasing the performance. A more integrated and adaptive way of working of the airport security system could lead to an even more desirable performance concerning both level of security and level of service. This research aims to provide an answer on how to integrate the current stand-alone airport security system and to show the difference between the stand-alone and integrated airport security systems.

The remainder of the report is structured as follows. Chapter 2 presents all domains in literature reviewed in order to gain the knowledge to perform this research. The literature consist of parts related to the aviation domain of the research problem, but as well to the security domain, security assessment domain and modeling domain. A project plan presenting the problem statement and research objective and questions is discussed in Chapter 3. The research methodology, comprising all steps to execute a thorough security risk assessment, for the airport security problem is described in Chapter 4. The Implementation of the model, as well as the language of the modeling software used is presented in Chapter 5. Chapter 6 discusses the analysis performed after the implementation of the model in all four case studies and the results that can be drawn from that. The conclusions drawn based on the research objectives are presented in Chapter 7. The report ends with recommendations for future work in Chapter 8.

2 Literature Review

Airport security is currently a hot topic. Passengers are aware of the environment and threats in the current world, but still want to enjoy the opportunity to be transported around the world as convenient and quick as possible. After the 9/11 attacks rapid deployment of individual security systems was organized in order to meet the security requirements. The aim of the proposed research is to investigate the opportunity to improve the performance of the airport security system by means of integrating the individual security systems. Several different domains will be investigated in order to set up a usable research. The literature study starts with a description of the airport environment in Section 2.1. After that in Section 2.2 the term security is described. The security risk methodology framework established to be followed during this research is presented in Section 2.3. One of the main steps of the security risk methodology is the analysis of threats, vulnerabilities and risks. The general framework for analyzing the aforementioned elements is shown in Section 2.4. The chapter finishes with Section 2.5 with an investigation of the modeling approaches which can be adopted in order to implement the airport security problem.

2.1 The airport environment

Security has always been an important subject and is nowadays a growing concern in the aviation domain as well. Safety research in the aviation domain is well established, while security research is rather new. An airport is a major way port to destinations all over the world. The growing demand in air travel makes that the society present at airports keep increasing. This means as well that more materialistic assets are present as well. This asks for the presence of a sound security system to ensure security at all times for everybody and everything against any possible type of threat. In order to see what impact threats have on the airport environment, the current situation of the airport environment and its processes must be understood.

The majority of the processes performed by the airport environment are present in the airport terminal. Several authors already made use of a typical representation in their studies to model and simulate the airport terminal layout and its processes [10] [11] [12] [13] [14] [15] [16]. A typical schematic overview of the processes at airports a traveler encounters on the day of the travel can be seen in Figure 2.1. The representation in these studies is used to build a general airport terminal layout suitable for this research.

The difficulty of airport security lies in the aspect that there are a lot of stakeholders within the entire security system. Those stakeholders are all interrelated and have different kind of information about the security which need to be exchanged [17]. Above all, there are not only relations between stakeholders, but also between technical systems and persons. This makes the airport security system a highly dynamic system with socio-technical aspects [18].

The airport environment is divided into landside and airside areas. The landside area is defined as the area of the airport environment which is accessible for the entire public. While the airside area is only accessible for passengers or staff. Public parking areas, access roads, rental car facilities, transportation stations, hotels and a part of the airport terminal are the most common assets of an airport in the landside area. The airside area of the airport environment consist among other things of another part of the airport terminal, runways, taxi ways, aviation equipment, aircraft hangars and maintenance facilities. Not only the assets of the airport environment are divided by these two definitions, also airport processes are categorized by means of landside and airside positions. Again, landside operations are all the processes in the area of the airport terminal that is accessible for the entire public. The security checkpoint generally forms the boundary between the landside and airside areas. After clearing the security check all consecutive processes belong to the airside operations. For the entire airport terminal however, may it be landside or airside, hold strict security regulations [18].

Nowadays the security doesn't only start at the premises of the airport itself. This only holds for the physical security. It actually starts at home, where travelers can book their tickets on the internet without any control. They only have to fill in some of their personal information, choose the type of flight, the amount of baggage they want to take with them and pay. After paying they can even already check-in for the flight. This means that a lot of processes at the airport itself speed up, due to the fact that everything is already arranged at home, but it also means that there can be less physical contact between airport staff and travelers on the airport [19]. Especially if the passenger can book as a registered traveler with the help of an airline's frequent flyer program [20].

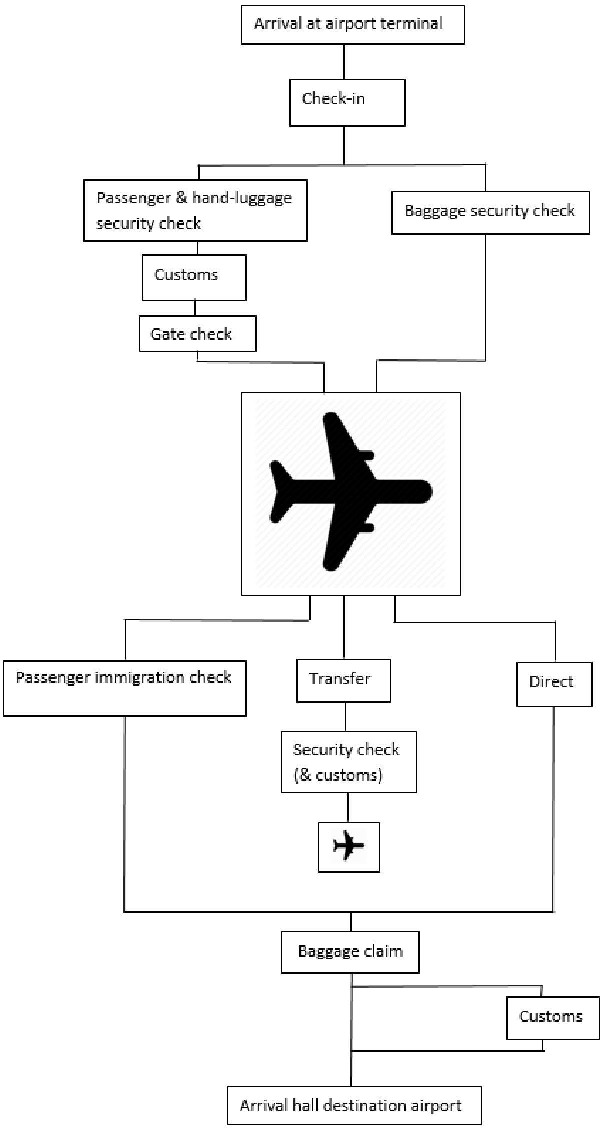
Arrival at airport terminal
Check-in
Passenger & hand-luggage security check
Baggage security check
Customs
Gate check
Passenger immigration check
Transfer
Direct
Security check (& customs)
Baggage claim
Customs
Arrival hall destination airport

Figure 2.1: Schematic overview of the infrastructure of the main airport processes from a passenger point of view

At the day of the flight, passengers move towards the airport. Physical security activities apply in order to provide all passengers with a safe environment. The landside part of the airport terminal, from which departing passengers can enter the airport terminal is also accessible for the public, as people want to drop off relatives and due to the presence of hotels, shops and public transport possibilities. This means that there can be a lot of people present at this area of the airport who may or may not have anything to do with boarding an airplane. The crowd can create a blur to the supervision of security at the airport. To get control over the situation, monitoring equipment like video surveillance is installed outside and inside the airport terminal in the landside area. Life safety measures are also taken in the form of duress alarms, emergency phones and medical equipment. Passengers need to run through all the processes within the airport terminal before they can board the airplane. As mentioned before, the airport terminal consist of a public area and a secured area. The processes executed within the terminal cannot be seen individually, as it is a chain of operations. Therefore the processes and thus security as well is generally analyzed as an infrastructure problem. The processes have a complex operational make up and take place over a certain period of time. This means that the dynamics of the airport processes also need to be considered. So, passengers arrive at the airport either by public transport or car which may include the help of others. Upon arrival in the airport terminal the first process which passengers encounter is the check-in process located in the public area of the terminal. This can either be a physical confrontation with an employee of the related airline or via a computer in a self-service area. The goal of the check-in desk is to check the identity of the passenger and whether the passenger has bought a valid ticket for the specific flight and the staff or computer will generate a boarding pass. However, in this modern era passengers can already check-in and receive the boarding pass at home and skip the check-in desk at the airport terminal. This is due to the fact that industrial deployment has changed, more automation is involved in the processes in order to make the passenger more independent for a higher passenger satisfaction and less queuing time. To finish checking in passengers will have to drop off their baggage which cannot fit into the cabin. This can either be done at the check-in counter with the help of staff or at a special self-service area. Passengers will receive a boarding pass which can be equipped with a magnetic strip or a barcode. The boarding pass will help the passengers with their identification at security checks and gate to ensure boarding the aircraft. The baggage will also be given a barcode or radio-frequency identification tag. This tag will guide the baggage towards the right airplane without the help of the passenger or any airport staff [8].

After check-in the ways of the passenger, with or without carry-on luggage, and the baggage will separate. Passengers can enjoy the time with relatives and friends in the public area of the terminal before proceeding to the most extensive check on an airport, the security and border control check. In the public area it is important to identify illegitimate or threatening movements of people. The airport is a space of flows, it’s a highly mobile environment, especially this public area which everybody can enter. Airports use video surveillance systems to gather information about people’s movement and to keep control of the situation within the terminal. Special security observers watch the video footages either to detect an object or person or to categorize an object or person relative to their threatening behavior [21]. Not only video surveillance is used, physical attendance of security guards and customs officers gives a clear signal towards the public that the security is guarded on the airport premises. Those guards are in contact with the video surveillance staff to immediately control a threatening situation.

The passengers proceed to the security check or passport control, the order depends on the airport and the destination. Passengers flying between Schengen destinations do not have to go through passport control. Behind these checks the sterile area of the airport terminal is present. This area is used for boarding or deboarding the aircraft and includes shops, restaurants and lounges. The airport has to make sure that only valid passengers or airport staff can enter this sterile environment and that no threatening objects are smuggled through.

Upon display and verification of their boarding pass, passengers and their carry-on luggage will be subjected to a brief security check and identification control with the use of high-tech equipment. The well-known examination procedures performed by security personnel which contain a visual check of the documents and the categorization of people based on their behavior is still widely adopted in the focusing of attention and decision making of security officers. Categorizing passengers is especially done during the queuing time before the checks. However, nowadays modern technology influences the controls more and more. Innovative security systems shift the focus towards the biometrics of passengers. The uniqueness of the body of a passenger is an interesting tool to assure security. Different parts of the body may be used to identify the identity of a passenger or the movement of a passenger through the airport terminal. The use of the body of a passenger is a discrete form of security, in contrast to the categorization based on behavior of passengers for instance. Datasurveillance is used to obtain data from persons. This technique has been introduced after the development of aviation terrorism. Paper documents cannot give full disclosure of passengers anymore and thus guarantee security when used as only means of security measures [22].

The use of the body as a means of identification is at the moment mostly used to identify frequent flyers. In order to maximize the comfort of frequent flyers they can skip queues for the security check if they are registered in this biometric system. A security guard will indicate when it's the turn of a passenger to proceed through the security check. The carry-on luggage of this passenger will run through a special scanner. This scanner uses x-ray waves to make an image of the luggage. A security officer can identify different areas and items within the luggage. With the use of this image the security officer can make a decision whether there is any threat or not. Passengers themselves need to pass through a similar device as well. All their personal belongings need to be removed and need to go through the scanner for the carry-on luggage, such as coins, watches, belts, mobile phones, etc. It depends the airport which kind of device is used. The most common device is the walk-through metal detector. However, devices with increasing accuracy are developed. A good example is Amsterdam Schiphol airport [23], where they use an imaging device on the bases of millimeter waves. In case of the metal detector only specific type of threatening object can be found, while with the newer body scans can identify every abnormality on the body. However, in both cases the machine will indicate if a possible threatening object is found and an extensive search by a security officer is needed. In case an additional search is needed due to objects on the body or in the carry-on luggage of the passenger, this passenger is taken separately. Most of the times the additional search is done by hand, but the security officers can choose to use a more extensive scanning device. In case there is nothing suspicious found the passenger can immediately continue into the sterile area of the airport terminal. Passengers can move freely through this area of the terminal. They can enjoy the lounges or shops and restaurants. Video surveillance and active physical control by security guards is present. The last process for passengers before boarding can be found at the gate. In some cases the carry-on luggage is checked once more, but normally only the identification documents and the boarding pass of a passenger is checked in order to see if the passenger will be boarding the right flight.

However it is not just our own movements that are tracked and checked, our baggage as well. The baggage the passenger arrives with at the airport environment which cannot join the passenger in the cabin will be guided another route to the aircraft [10]. At the check in process this baggage is labeled and separated from the passenger is belongs to. Passengers, as mentioned before, will continue their way to other areas within the airport terminal, but the baggage is transported elsewhere via a huge conveyer belt system. While the passengers undergo the security check in the airport terminal, at the same time their baggage pass through a similar process. The baggage passes through x-ray machines and explosives trace detection portal machines. If any suspicious item is found the baggage is taken out of the system, if not the baggage can continue towards the aircraft.

At the arrival airport the passengers may walk unworried with their baggage to the exit of the airport and enjoy their stay. However, this depends the destination. Sometimes the passengers must undergo another passport control before they can pick up their baggage. Security officers will check their identification documents to check whether they may enter the country without causing any harm for the local population. While passengers pick up their baggage, security officers perform a physical control, which may use dogs, to find contraband that cannot enter the destination. Any suspicious passengers or baggage identified in these two checks can be chosen for a more extensive search at the arrival airport.

2.2 What is security

Security is one of the most important needs for a person to have, to feel secure. Throughout history society has been busy with assuring security. More recently security has become a major point of importance in aviation as well. Security is often confused with safety. Although these statements are closely related, they are not similar [24]. The definition of security followed in this research is presented below [1]:

"security is protection against intended incidents. Intended incidents happen due to a result of a deliberate and planned act."

As can be obtained from this definition, security is related to a certain intend from the attacker that executes the attack. Intend means that the attack is performed on purpose with a certain motivation. A lot of the principles in modelling security may be based on or related to the models used for safety due to the fact that these definitions are closely related and the lack of academic experience in the security domain thus far. Defining safety and security has proven to be difficult. It is avoided in the academic world and there is no harmony at operational level. The most appropriate definition of safety used is presented below [1]:

"safety is protection against random incidents. Random incidents are unwanted incidents that happen as result of one or more coincidences."

The difference between the two when defining them can be immediately noticed. Where security threats are related to a certain intend and executed on purpose, safety threats emerge from random activities which are not intended by the threat source to harm the victim. Dealing with both types of threats shows less differences however. The objective for both security and safety is to have an environment to be well protected and without risks. The assets within the environment must be protected against hazards and threats. If security or safety cannot be guaranteed within an environment this can in both cases cause dangerous situations for assets and the lives of people. In this modern world it will be more important to understand security and the threats, hazards and vulnerabilities within a security system to be sure that the environment does not feel any harm of these intended actions. People deliberately attack the process or organization in order to achieve a wanted outcome, to gain profit or to create harm, this in contrast to safety where accidents are unplanned. The intended actions can always be tracked down to humans, also if certain equipment is the part of the system that does not work how it should. Threats, which lead to the intended actions, can be divided into internal and external threats [1]. Internal threats are based on items which are part of the original environment. External threats are items which are not part of the original environment, but harm that environment. A lot of targets be found for the intended actions in security attacks. The main objectives in security attacks are to induce losses to physical assets, informational assets or economical assets. More as for safety, security is interrelated to the society. Security problems reflect the society in every layer, such as its social structure, economic structure, impression of law and crime and morality [1].

Threats are difficult to predict as it is not sure whether a certain scenario would unfold. This means that there is always some kind of uncertainty that needs to be added to the prediction. Thus, there must be a reasonable amount of security precautions to protect the environment beforehand. However, the usefulness of these precautions are uncertain as well [7]. The way to research a security problem is via a security risk assessment. Such an assessment uses the notion of risk to address security related issues. Risk is the potential of losing something of value [25]. Although security is the protection of something of value, via the analysis of risks or threats the performance of the security system can be determined. The importance of a security risk assessment is to know what the impact of certain threats is on the security system. This can either be done from a secure point of view or from a risk based point of view. The latter is most used in a security risk assessment, it shows which threats can break through the security system and which impact they have on the performance [26]. On the basis of these outcomes the other side of the coin can be discussed as well, such as which parts in the security system are the most reliable. Security can be defined as a notion of people, this isn't a hard value but a scale based on opinions or can be determined by definite values such as the number of attackers caught and not caught, inspection rates and queuing times and the probability, frequency and impact of scenarios to happen [27].

2.3 Security risk methodology

A security risk assessment forms an essential part of any research in the security domain. It is an ideal approach to check that security expenses are proportional with the threats exposed on the environment under consideration. However, the process to determine which security controls are the most appropriate and efficient is quite often a complex matter. Guidelines are set up for organizations to make their systems, processes, products and environment secure, although organizations are free in the way this security is achieved [28].

A security risk assessment is basically performed to check the security structure of an organization for threat situations. Based on the outcome resources can be removed or assigned to the security structure to set up the most fitting configuration to tackle threats [29]. The outcome of a security risk assessment is a prediction of either risk entirely or only a component of risk which is called vulnerability. Sources of risk or vulnerabilities are identified where after their probability of occurring is determined. When analyzing risks or vulnerabilities multiple questions can be answered [30]:

(1) What is a possible situation that can happen that endangers security?
(2) What is the likelihood for the situation to happen?
(3) What are the consequences the situation incurs?

A security risk assessment follows a certain methodology. Three main types for performing a security risk assessment can be distinguished, respectively rule based, risk based and judgment based [31]. Rule based assessments only check the regulations and standards a system needs to adhere to when providing security. Risk based and judgment based assessments dig deeper in the organization and the environment. These assessments evaluate all possible threats, known and unknown to the system already. For each threat likelihood and impact is determined. The difference between risk based and judgment based assessments can be found in the definition of the probability used. Risk based assessments use empirical data known from similar situations to determine the probability. Judgment based assessments use data based on experience of experts rather than factual data to determine probability [31]. There is also another way in which risk assessment methodologies can be defined. There are two specials approaches, respectively a quantitative based assessment or a qualitative based assessment. The difference lays in the determination of the probability of the threats addressed and which threats are addressed specifically [32]. When executing a single security risk assessment separate approaches of the above mentioned types can be implemented for different risks, this is called semi-quantitative [33].

As described a security risk assessment follows a methodology. This methodology prescribes general steps that are generally performed in any research that uses a security risk assessment [7]:

1. Set up the context, scope and goals of the research in all applicable domains and for all stakeholders present.

2. Risk Identification
Mostly seen as the most important step of a security risk assessment. This step actually defines all possible threats and vulnerabilities with their likelihood and impact on the organization.

3. Risk Analysis
This steps performs the actual analysis of the threats and vulnerabilities set up in the precedent step. The actual impact and probability of a certain threat is determined such that vulnerabilities of the organization can be highlighted.

4. Risk Evaluation
The evaluation of the outcomes from the precedent step considers the understanding and prioritizing of these outcomes. This makes it easier to react on the most important vulnerabilities in the organization.

5. Select countermeasures
After the most important vulnerabilities can be highlighted, action needs to be taken such that these vulnerabilities strengthen and the impact of the threats is mitigated.

There are many different risk assessment methodologies used in practice nowadays in all kinds of research domains, as well in the security domain in which the airport security problem belongs. Actually risk assessment methodologies from all kinds of industries can be used as guideline for the research. The main framework looks quite similar among all the different methodologies and the steps in the methodologies are quite easy to adapt to the unique needs of the performed research. All of the methodologies have common goals and incorporate the same core activities, but can slightly differ at their perspectives. Commonly used methodologies are the NIST, DHS, AS/NZS 4360, CORAS and EBOIS 2010 [34] [35] [36] [37] [38]. However there are many more methodologies available which could be applicable for the research as well.

These methodologies are not discussed in a more thorough way because of the fact that they are quite similar. Although the NIST methodology looks very applicable for this research because of the clear and elaborate steps and the ordered way the steps are structured. This makes it accessible to make adaptions for a research in the airport security domain. Furthermore is this methodology assembled by using the international ISO guidelines [39], which makes it a reliable source. The adapted NIST methodology is discussed in more detail below in order to illustrate the structure of actions performed for this research.

NIST methodology for the airport security problem research
Several general steps are laid out by the methodology. Unique tasks are defined within each of the separate steps. The basic steps consists out of a preparation, the actual performance of the risk assessment, the communication of the results and to maintain the assessment [34]. The general overview of this methodology is very similar as the ISO guidelines [39].

- Preparation of the security risk assessment

A security risk assessment starts with a preparation phase. Although this step is called preparation phase it is an important step of the security risk assessment and should not be missed. The main outcome of this step is that the context of the research is explained. Different questions need to be asked by the researcher. About the purpose of the security risk assessment, the purpose of the research, the scope of the research, the assumptions and constraints when executing the research, the origin of input data and the analytic and programming approaches used to implement the research.

- Implementation of the security risk assessment

After the context of the research is determined and the need for the security risk assessment is defined, the implementation of the security risk assessment can be executed. The main outcome of the implementation phase is an estimation of either risk or vulnerability of the organization for a certain specified threat in a certain specified situation. The implementation phase can be very extensive. Therefore, multiple separate but smaller tasks are considered. In general these tasks can be executed consecutive, although in some cases tasks need to be repeated in order to formulate the best security risk assessment.

All tasks in the implementation phase are related to the research environment and organization under consideration, the possible threats present, the likelihood and impact of all identified threats and the vulnerabilities and risks for the organization. The first step during the implementation phase is setting up the environment under consideration during the research and the aspects of the organization which are present in this environment. Secondly, the organization or security system is defined. Thirdly, the threats, vulnerabilities and perceived risk are established. This task consist of identifying all possible threats and vulnerabilities and address them based on the likelihood and impact. Consecutively, a security risk scenario is built. This security risk scenario is based on one or more threats defined in the task before. The security risk scenario shows more detail of the threat that can be imposed on the environment and the security system. Additionally to the threat, also the attacker and the way of operation of the performed attack are identified. Finally, a conceptual model is described such that simulation can be performed for the environment and security system under investigation based on the security risk scenario. The simulation is used to understand the nature and degree to which the security system is vulnerable to threats described in the security risk scenario.

- Monitor and correspond the obtained information

The last step in a security risk assessment consists of the consequent monitoring and exchanging of information. This step actually continues indefinitely as security risk information is dynamic. Long time situation specific risk mitigating actions can be performed based on the obtained information.

2.4 Assessment of the perceived risk of threats on airport assets

During the security risk assessment set-up by the aforementioned methodology the perceived risk and the reaction of the airport security system is analyzed. A general framework for the execution of the analysis can be followed. Risk can be seen as an attribute of a threat on a certain environment due to the presence of a vulnerability.

There are a lot of definitions to introduce the term threat. A threat explained in the most general way is ‘the expressed potential for the occurrence of a harmful event’ [40]. This means that a threat can either be intended or not intended by the threat source, which relate to the safety and security discussion. This research only focuses on security threats, thus threats with are induced due to a certain intend from a threat source. The threat is directed to a certain asset. Assets can be present in different forms, respectively physical human beings, materialistic goods and information. Threats are the subject in the execution of a risk assessment, as a threat can be seen as an element of risk. The eventual perceived risk for a certain environment comes from the analysis of a certain threat.

Vulnerabilities and threats are closely related. The term vulnerability refers to the weaker areas in a security system through which a threat can propagate and thus cause an attack to be successful [41]. A security system, whether it to be for an airport or not, should be tested on an ongoing basis for resolving vulnerabilities. Analyzing the vulnerabilities on an ongoing basis keeps people responsible for the security system and the resources used in the security system up to date to the ever changing threats. Vulnerabilities are not particular to technology, they can also apply to social aspects. This is also true for the airport security system as this is a so called socio-technical system [42]. In some cases it can be true that only one vulnerability can already cause the threat to succeed, but most of the times there are multiple vulnerabilities which cause that the threat can propagate through the security system [43]. This propagation is called the Swiss Cheese model [44].

Individual security systems can be seen as individual layers, where some can have holes which represent their vulnerability to threats. Due to the individual layers, and thus the unique characteristics of each layer, a threat should be caught before it can propagate through the entire system [44]. In the case that a threat can propagate through the entire system it means that the holes or vulnerabilities of the individual layers aligned such that none of the security measures identifies the threat in time. More of these individual layers means more opportunity to catch the threat before it can create a harmful outcome on the system and the environment. Additionally, the more efficiently established the security layers are the less likely is it for a threat to propagate through that specific security layer as well. Some vulnerabilities can be present due to the way the security system is designed, others arise due to the way the system is operated.

Risk can be defined as the probability that a certain threat attack will occur multiplied by the severity of the consequence of this occurrence [33]. There are many types of risks, but three main types can be distinguished: initial risk, current risk and residual risk [45].
Initial risk is the severity and likelihood of a threat when it is first identified and assessed. This type of risk is mostly calculated in the very early or preliminary stages when designing a new system. Initial risk is calculated by taking into account both verified requirements and assumptions made about the state of the newly designed system. After the initial risk is determined it is not changed. Normally, initial risk is an investigation to raise awareness for system safety.
Current risk is the predicted severity and likelihood of a certain threat category as it is present in the system at that time. Validated and verified requirements form the bases for the calculation of current risk. Current risk is subjected to change over time as it is the risk at a certain time point and threats are very dynamic, certainly in the security environment where threats have a certain degree of intend.
Residual risk is a type of risk that remains after all requirements of a system have been executed and verified. Verified requirements are the only type of requirements that are used in the determination of this type of risk.

Risk can be described by one of the following formulas [46]:

$Risk = Likelihood\ (L)\ x\ Impact\ (I)$
$Risk = Threat\ (T)\ x\ Vulnerability\ (V)\ x\ Criticality\ (C)$

With;
$Likelihood\ (L) = \ Frequency\ threat\ x\ Probability\ all\ security\ measures\ fail$

Where,
Likelihood (L) is the probability a threat action or scenario is successful.
Threat (T) is a definition of the likelihood that a specific type of attack will be executed in a specific environment.
Vulnerability (V) is a definition of the likelihood that security measures against a certain threat will fail.
Criticality (C) is the consequence of the negative effects if a threat is successfully executed.

When data is available about the elements in the formulas these could be implemented and risk can be calculated. If this data is not available a more physical representation of risk can be obtained by translating the first of the above mentioned formulas. Two schemes with categorizations which represent degrees of likelihood and impact of a certain threat can be used in order to establish a degree of perceived risk for the environment under consideration. Table 2.1 shows the categorization of the degree of likelihood a threat can have, while Table 2.2 shows the categorization of the degree of impact that threat can have.

Likelihood Rating	**Definition**
Definite	Is expected to occur in the environment
Likely	Will probably occur in within the environment
Occasional	Might occur at some time in the environment
Seldom	Could occur at some time in the environment
Rare	May occur only in exceptional circumstances in the environment

Table 2.1: Categorization by likelihood of threats [47]

Impact Rating	**Definition**
Insignificant	The amount of damage the threat impose on the assets in the environment is only very small
Minor	The threat will incur a small amount of damage, but the extent of the damage is not too significant for the assets in the environment
Moderate	The threat would result in some damage and/or consequences for the assets in the environment
Major	The threat would result in serious damage and/or consequences for the assets in the environment, which can lead to an amount of loss of assets as well
Catastrophic	The threat would result in disastrous consequences for the entire environment and its assets, it can be seen as the worst case outcome

Table 2.2: Categorization by impact of threats [47]

The approach used by following this scheme is called the security risk matrix approach [45]. Due to the fact that risk is determined by schemes for two parameters, likelihood and impact, the parameter risk will be defined on the basis of a two-dimensional scheme and uses four different degrees to categorize the severity of risk of the threat category, as can be seen in Table 2.3. The likelihood parameters can be found on the vertical axis and the impact parameters are shown on the horizontal axis. The degrees of risk are built in such way that the assets within the airport environment and the airport environment itself are represented not only in the impact parameter but as well in the risk parameter, as some assets in the airport environment are highly valuable but not in a way you would describe with money, like the lives of passengers. Using the risk matrix, threats can be analyzed and categorized on importance such that an order can be made in the handling of the threats.

	Insignificant	Minor	Moderate	Major	Catastrophic
Definite	Moderate	High	High	Extreme	Extreme
Likely	Moderate	Moderate	High	High	Extreme
Occasional	Moderate	Moderate	High	High	High
Seldom	Low	Moderate	Moderate	High	High
Rare	Low	Low	Moderate	Moderate	High

Table 2.3: General security risk matrix

2.5 Modeling approaches

One of the steps in each of the security risk methodologies is to create a model for security risk analysis. This means that all the risks, vulnerabilities, assets, scenarios and relationships between them are used to come up with results which say something meaningful about the risks that threaten the organization or the level of security of this organization. After the results are obtained they can be analyzed in order to use these meaningful results to improve the security of the organization. This security risk assessment is realized with the help of modelling.

Models are used to clarify and build systems in a mathematical and programming language in order to gain knowledge and understanding about this system. An airport environment can best be represented by a complex system. A complex system consists of large networks of connected and interacting components with an emergent global dynamics resulting from the interaction of different parts within the system [48]. Properties of complex systems are that there are nonlinear interactions, it is decentralized and there is a collective behavior. When analyzing complex systems, difficulties can arise [49]. Structural complexity is the fact that the system consists of many interconnected parts. Behavioral complexity means that the output of the system or its emergent behavior is difficult to predict [50]. The system which has to be modelled in order to perform a security risk assessment for airports has another difficulty as well. This system is a so called socio-technical system. It means that there are interactions between people and technical systems in workplaces and it also refers to interactions between infrastructures and human behavior. Socio-technical systems bring their own challenges. Changes in a certain part of the system may have unforeseen effects on other parts. There are just a few points through which the behavior of the system can be changed to a desired state and there is no theory where to find these points exactly. Finally, the sociological part within these systems is still not well captured by the widely established systems engineering approach [51].
Security risk analysis is part of every decision to be taken. When the security risk assessment is performed the outcomes need to be transformed to useful results. Sometimes this can be done already within the security risk assessment model used, however sometimes it can be more efficient to use another tool as well.

There are a lot of different types of modelling approaches which can be used to analyze a certain organization during a security risk assessment. These models can be categorized between two main types, traditional computational modeling methods and agent-based modeling approaches. Traditional modeling methods can be found in the domain of system dynamics and operations research. Model defined by systems dynamics use equations that illustrate the stochastic nature of the variables. Models constructed using an operations research approach describe the problem by using mathematical methods to determine best possible solutions to a certain scenario within the problem in order to increase performance of the investigated output. Both system dynamics methods and operation research approaches do not put much effort in single events or agents of an organization within a model, but describe the organizational dynamics in a more aggregate view. This would be useful when analyzing the performance on a macro level, especially because these type of methods are computationally particularly effective. However, on the other hand lack these type of models the ability to express behavioral characteristics of agents present in the organization and the relationships between all these agents [52]. Agent-based models on the other hand use predicate logic in order to define the model rules and are thus a more powerful tool to define individual components and relationships between these individual components of complex socio-technical systems. Below a few of the most common methods from these two categories are described in order to seek the best modeling approach for the airport security problem.

System Dynamics Models

In the system dynamics approach a model is built that represents the temporal cause-and-effect relationships between variables in a general way. Systems are modelled as interacting variables by means of differential equations. Therefore, the model is able to handle direct causal links and feedback loops between variables. A diagram shows the nodes an arrows which represent the variables and causal links between those variables respectively. The diagram is beneficial in order to change the system easily into a programming language. The system consists out of the main agents and their data, the flows into and out of these agents and the variables that control the rate of the flows. The flows clearly show the relationships between different variables within an agent and between variables of other agents. As described differential equations form the basis of a system dynamics model. Those differential equations calculate the outcome of a variable at a next time point given available data at the current time point. The aspect of time shows the dynamic behavior of such a system very well [52]. This type of model uses the behaviors of the entire group of a specific type of agents rather than individual agents. This implies a macroscopic type of modelling as the total population is used, while each individual item is not represented. The downside of this is that this makes it hard to model variety among the agents within the same model [53].

Fault Tree or Event Tree Models

Event tree analysis is a logic based modelling approach. The approach consists of multiple options after a certain situation emerged. A specific path is followed by the model as an action is chosen to be performed after a certain situation. This action triggers another situation to emerge. Eventually outputs based on success or failure of handling a certain situation can be collected. Those results are searched through a single initiating event after which a path is drawn. Depending on the type of result wanted, from each step in the event tree probabilities of success and failure rates can be determined. In the end the outcomes can be combined in order to have a meaningful result about the resilience of the overall system. All consequences within a system or subsystem that have a probability of occurring can be identified and implemented in the event tree. The event tree process consists out of branches with sub-events from an initiating situation [54]. One sub-event that follows the antecedent situation is determined on the basis of logics. There are different types of logics which can describe the probability of a next event occurring. Logics is a formalism for describing logical relations in the same way that ordinary formulas describe numeric relation [55].

An event tree model can be used within a risk assessment which focuses on the probability of failures. Performing such a risk assessment on the basis of this model starts with a set of initiating events that change the state of the overall system. The initiating event starts the slipping slope reaction and sub-events follow. Each initiating event results in another event and this can continue for a long time, therefore the lay-out of this model looks like a tree. In order to limit the size of the model, for sub-events the successive events will only be dealt with if they are mutually exclusive, meaning that they cannot occur at the same time. The end states of the overall system are categorized into groups by success or severity of consequences. The overall goal is to determine the probability of possible negative outcomes that can cause harm to the overall system [54]. A wide variety of possible threat situations can be addressed, which makes this model very versatile. Also a very practical and easy to understand way of modelling can be followed. The downside of this model is the time consuming nature. One single situation that initiates a security breach can be addressed per simulation. Also, all initiating actions and the entire pathways must be identified before the system can be modelled [56]. Moreover, the actual operators of a system do not have to be modeled, only possible events are needed, which leaves a big gap in the meaningfulness of the outputs for the airport security problem.

Network models

This type of modelling represents the system as a network. A wide variety of focal points together can be seen as a network. The main variable under investigation is active in these focal points and propagates through the focal points. The focal points are represented by nodes, while the relationships between them are represented by links between the nodes. All nodes can be directly linked or there can be a special pattern of links, this depends on the flow or relationships in the system. Populations or information will travel via these links towards the specific nodes where they either converge, diverge or may enter or leave the system. These nodes can either be modelled without any notion of time or with a specific time stamp. Boundary conditions which guide the flow through the arcs towards the nodes are determined with the use of mathematical formulas. The addition of constraints can make the model as realistic as needed [57]. Problems which have a macroscopic nature are very suitable to be represented by a network model. The nodes represent parts of the system without containing much behaviors themselves, the behaviors come from the population flowing through the network [58] [59]. There exist numerous types of network models to represent all different aspects of systems.

The Critical-Path Method is a modeling technique especially used when analyzing projects, however it has a clear structure of focal points and their relationships. The network model is preferable due to the fact that it is a conceptually simple model and it can handle many to many relationships, however it is incorporates linear modelling only while the system can become very complex. The difficulty of this type of models is as well that it is mostly used to calculate cost or profit and not for an indicator like security [60].

The Bayesian network model is another special type of network model analyzing the problem from a probabilistic nature. The nodes are the random variables or parameters and the links are their conditional dependencies. In this model not all nodes have to be connected. Independent variables are shown by isolated nodes. Probability density functions are related to certain nodes. These probability density functions determine the probability that a certain situation happens for a specific node. This model can be dynamic if a sequence of variables is obtained. Then with the use of so called influence diagrams this model can be used to represent and solve decision problems under uncertainty [61].

Agent-based Modelling for the airport security system

Agent-based modelling is an interesting technique, more and more known nowadays. Especially the characteristic that it is a powerful approach to model complex socio-technical systems makes this type of modeling technique appealing [62]. Different studies, [52] [63] [64], are used to draw a clear image about the fundamentals of agent-based modeling. With the use of such model it is an effective way to partition the problem space and to capture interactions or dependencies between agents in the environment [62]. An agent-based model represents the system under investigation by means of different agents. The single agents have individual rules which define their goals and behavior. Although the rules are defined for agents individually, they can define interaction or communication among different agents or with the environment. Agents are autonomous, which means that there isn´t an overall controller who states what an agent does, the agent does whatever it is modelled to do in a certain situation. They are able to socially interact with other agents. They can be reactive, which means that the agent is able to react appropriately to stimuli coming from the environment. Finally they can be proactive, which means that he agent has one or multiple goals that it pursues on its own initiative [52]. The overall goal of the entire system emerges from the individual rules of agents. The use of separate agents and individual rules enhances local model refinements instead of changing the entire system immediately.

These properties can be a bit vague, a more direct way of describing the characteristics of an agent is by saying they have perception of the environment and other agents, they can perform actions or communicate, they have memory such that their perceptions of previous states can be stored and they have a policy which is a set of rules that determines what behaviors they will carry out at that specific moment. All agents within the entire model have relationships with one or more other agents who are built with the same characteristics to perceive, perform and memorize and with their specific policy [52]. This means that the model can analyze very complex situations and still obtain suitable information about the system present in the real world. Due to the interactions between the different agents the agent-based model can capture emergent behaviors on a dynamic time-based scale. Systems with macroscopic or microscopic nature can all be represented.

Game Theory

Conflicts are well defined by game theory models. Therefore, these models are often applied in security-related problems. Much of the work done has been designed to provide policy insights, however it can be very useful for operational level decisions as well [65].

Similar as an agent-based model, a game theoretic model defines the system in terms of different operators within the environment. In the simplest game theory model, which is mostly used, only two different categories of parties are modelled, the defender and the attacker. However, there is no limit on the number of parties represented within the model. Using this approach, the model describes a multi-party decision scenario. The nature of the model is to represent each party and their own goals first. The parties act on the basis of anticipation on the actions from the other parties [65]. A party, the defender or attacker, is thus the most important item of the model. Just like agent-based modeling the parties are individual agents with individual rules which define their possible decisions and actions. The game between parties is a description of the strategic interaction between those parties. The constraints and payoffs are stated in the strategy of a party. All parties want to set up their best possible strategies to obtain their goal [66].

There are different ways the game can be played. Attackers want to attack the assets of a defender and the defenders want to defend those assets against the attacks. How to defend the assets is based on the value of the asset lost after an attack, the value of the precautions and the awareness an asset has in the eyes of the attackers. The attackers on the other hand take into account the value of a successful attack, the awareness of the asset in the world and the difficulty of security [66]. In simultaneous play both the attacker and defender perform their actions at the same time and thus they cannot see beforehand what the other party has come up with. This means that the attacker cannot readily observe the security investments the defender made. In the case of sequential play, the attacker and defender notice the action of the other party and act because of the new situation [66]. At the end of the game there can either be a winner, the one who reaches his goal or there can be an equilibrium. The downside of the solution is that the model will not show how the result is reached. The game is built to obtain the best solution between attackers and defenders for the same goal [67]. However, within the airport environment there are many parties but they can have another goal which may harm the overall security. This will hamper the representation of the dynamics of the system in this type of model.

3 Project Plan

This chapter describes the problem statement and research objective, respectively in Section 3.1 and 3.2. The project plan starts with a discussion of the current gaps in the analysis of the airport security system. Where after the research objective is illustrated by presenting the research questions. The research questions form the basis of the direction of the research. The problem statement and research objective are set up using the literature discussed in Chapter 2.

3.1 Problem statement

The notion of being secure has been on the minds of people for a long time in the modern world. Being secure can be based in a physical way, which means that a person is protected against harmful situations for that person or in a materialistic way, which means that objects, resources, information or economical assets are protected. All these subjects can be seen as assets for a possible threat.

In recent years security in aviation is getting more and more important. Even so in aviation and the airport environment. The airport environment is namely a crucial point in the modern world. It connects destinations all over the world with each other by a means of transportation that does not take that long. Therefore it is widely used by society. To protect the airport environment with all its resources and passengers present in it, an airport security system is constructed. An airport security system consists of individual security systems. These individual security systems are mainly located in the checkpoints of the airport terminal. These checkpoints are the locations where the airport processes are performed, such as check-in, security scan, customs and gate access. Additionally some of the security systems are present in the open environment of the airport terminal, such as the public area or the secured area after the security check and before the gates.

In the past decades aviation and the airport environment had to cope with serious threats. The individual security systems of the airport security system are set up in place in order to tackle these threat. However, due to the need of universal and rapid deployment of the individual security systems a stand-alone way of working is induced. This has only little changed nowadays in some small environments for major airports. For many airports still this stand-alone way of working is adopted. Using such stand-alone way of working the performance of an individual security system is leading in the identification of a threat source and threat objects. This does not mean that the current airport security system does not achieve a good quality of performance. However, it is a long-winded approach with the modern technology available. When only relying on one individual security system for every checkpoint in the airport environment, the hypothesis arises that not the most efficient way of working is implemented. Thus it leaves room for performance optimization of the performance measures of the airport security system. Performance measures may contradict to each other. First of all and the most important in the end, is the probability of detection of true positives, false positives and missed detections a type of performance. On the other hand, the level of service and the delay passengers receive due to the processes of the airport security system are a level of performance as well.

Integration plays more and more a prominent role within complex systems. The integration of the current airport security system could lead to an innovative way of working with an increased performance level in order to solve the gap in the operation of the airport security system. Integration means that the individual security systems will be connected to each other. The data provided will be available for every individual security system and therefore a better overall decision can be made by the airport security system. Although integration is growing when constructing complex system, it is not yet deployed in real life for the airport security system. This means that a new integrated security system needs to be designed.

In order to analyze performance results for both the current airport security system and the new designed integrated security system a conceptual model of these systems needs to be made and later implemented in programming software. The airport security system is a complex socio-technical system. Agent-based methods, rather than the general computational methods, e.g. operation research, are very convenient for this type of modeling. As in an agent-based method all actors are represented as separate agents with their own set of rules which define their behavior, goals and relationships to other agents.

Research in the security domain is not completely new. However, the use of this upcoming modeling technique and the implementation of innovative technology in order to integrate the current airport security system is a new area in the aviation security domain. This research can therefore be seen as an exploratory research which can form the basis for future research.

3.2 Research objective

Following the problem statement in which the current research gap is introduced, the research objective is established. The research objective forms the basis for the direction of the performed research. The research objective can be divided into three individual, although related, research questions.

1) How can the diverse components of the current airport security system be integrated to tackle threats in the airport environment? And how does the integrated airport security system react on specific airport threats?

2) What is the difference in performance between the current airport security system working in a more stand-alone way and a new designed integrated airport security system?

3) How does an adaptive mechanism of the integrated airport security system influence the performance measures?

The first research question approaches the thesis problem on a more systemic level. It answers how the parts of the airport security system used separately could be integrated to make the airport security system more efficient regarding the performance. Integration of the security system will make use of a novel type of security technology called data fusion. A conceptual model of the newly designed integrated airport security system will be constructed to show the difference with the current airport security system. The second research question addresses a more practical side of the thesis problem. The current stand-alone airport security system and the newly designed integrated security system will be modelled by means of an agent-based model. Case studies using these two configuration of the airport security systems based on certain security risk scenario will be simulated. The research question answers how the airport security systems differ in performance and efficiency based on valuable KPI's for the airport environment and the airport security system itself. The third research question analyses the dynamics of the integrated system. For certain threats and types of passengers the security system will adapt to the most optimal setting regarding the means which will be used. The adaptation of the security system is a crucial feature in order to be as optimal as possible and to keep the randomness in the process. Simulations of the same security risk scenario as used for the second research question are used to analyze the performance of the adaptive mechanism of the integrated airport security system.

To address and answers all the research questions a solid foundation is needed. Research in this domain is performed by following a security risk assessment. The security risk assessment provides a methodology with certain steps that need to be performed in order to prepare and execute the analysis of the research problem. The methodology followed in this research is the NIST methodology adapted to the needs of the airport security problem.

4 Research Methodology

Methodologies are indispensable as a supporting tool for research. It provides a structured way of assessing the problem and in the end more valuable results are obtained with respect to research done without a methodology. Especially in all domains concerning security it is crucial to obtain valuable results as leaks in a security system can have catastrophic consequences. So, this holds as well for the research on the airport security system. The airport environment can be seen as one of the most important public areas where security should be protected in the most thorough way. Every day massive amounts of people are present in the airport environment and above all airports are gateways to places all over the world. The general outline of the adapted NIST security risk assessment methodology for this research explained in Section 2.3 will be used throughout the thesis work. This chapter will show the implementation of the different steps of this security risk methodology in order to assess the airport security system. First the environment under consideration will be established where after the airport security system present in this environment will be set-up. Secondly, the threats and vulnerabilities for this airport security system are defined. Thirdly, the perceived risk of the defined threats upon the vulnerabilities of the airport security system are determined. Consequently, a security risk scenario is built based on a striking threat. Lastly, the airport security system will be analyzed in more detail and a conceptual model of the current airport security system and newly proposed airport security system are constructed.

When needed a difference is made between the current state of the airport security system and the newly proposed integrated airport security system analyzed in this thesis. Section 4.1 will start with the identification of the environment that will be considered during the actual research. Subsequently, the threat, vulnerabilities and perceived risks for this environment will be discussed in Section 4.2. A security risk scenario is established in Section 4.3. This security risk scenario will form the basis as input for the implementation of the problem analyzed in this research. The airport security systems in the defined environment that face the security risk scenario are further defined in Section 4.4 where a conceptual model of both the current and newly proposed airport security system will be presented based on different types of views of the systems.

4.1 Set-up the research environment

The first step of the security risk assessment methodology followed is related to the preparation of the research. Although preparation may not sound that paramount, it is actually a vital procedure. The preparation step identifies the assumptions and constraints associated with the environment of the assessment. To establish the boarders of the environment under investigation is essential for the remaining activities during the research. The boundaries of the environment can be best presented using flow charts on the basis of different types of views.

The environment of airport security can be seen very broadly. To create a good overview of the environment itself and of all the possible actions which affect the airport system a physical view in the broadest way is presented in Figure 4.1. This way the boundaries of the environment under analysis can be defined more clearly. The view can be best described as seen from a passenger's perspective.

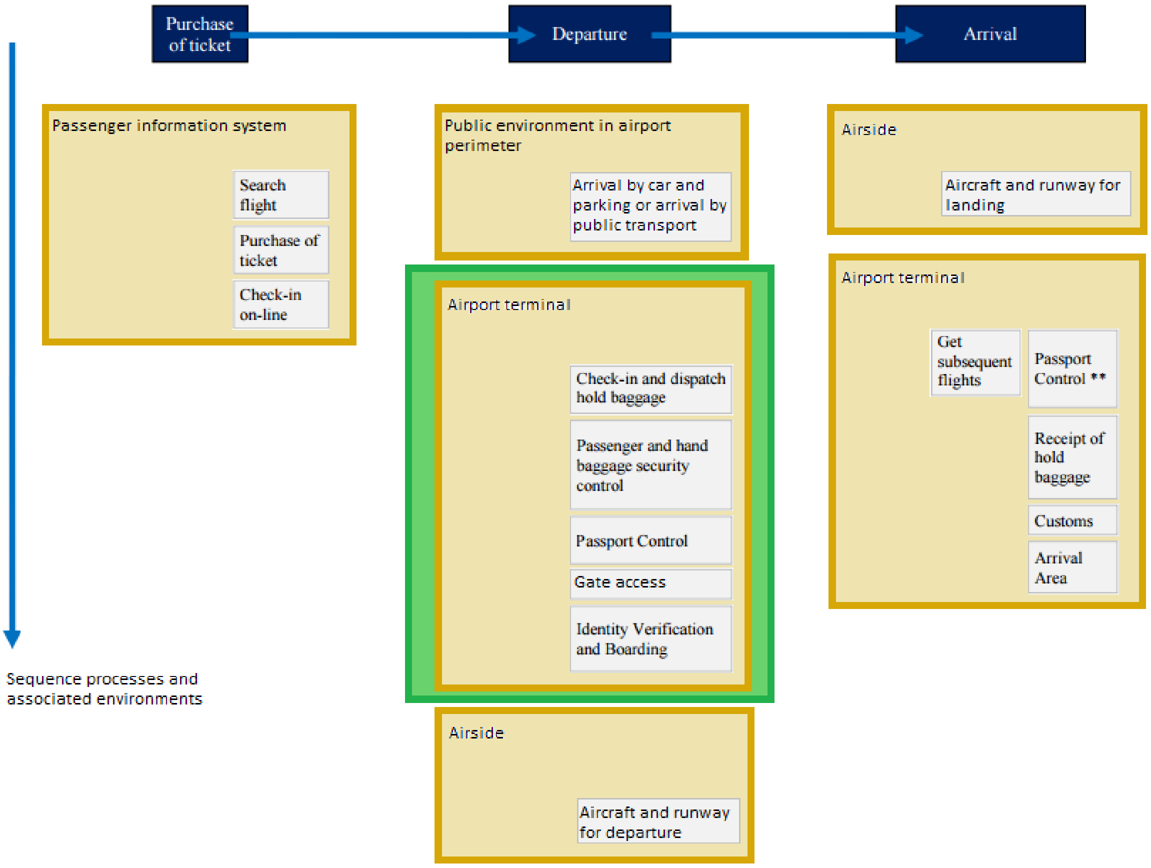
Purchase of ticket
Departure
Arrival
Passenger information system
Search flight
Purchase of ticket
Check-in on-line
Public environment in airport perimeter
Arrival by car and parking or arrival by public transport
Airport terminal
Check-in and dispatch hold baggage
Passenger and hand baggage security control
Passport Control
Gate access
Identity Verification and Boarding
Airside
Aircraft and runway for departure
Airside
Aircraft and runway for landing
Airport terminal
Get subsequent flights
Passport Control **
Receipt of hold baggage
Customs
Arrival Area
Sequence processes and associated environments

Figure 4.1: Airport environment

When passengers, with their luggage, arrive and go through all the necessary airport procedures at the airport premises and will eventually board their aircraft towards their destination. Then, when passengers aboard an aircraft their contact with the airport security system does not end. However it shifts from the airport security system from the airport of departure to the arrival airport's security system [12]. Thus passengers enter the airport security system there as well, either with a clean sheet or using data from the airport security system from the airport of departure in the most idealistic situation.

In this research the airport security system of only one airport is addressed. Which means that information about departing passengers is removed after their departure from this airport and no communication of the data of the airport security system takes place. The environment of only one airport is chosen over an airport network environment. The combining of airport's security systems is far from being executed nowadays. Of course, a similar type of security information about people is present and shared, but then via national security services. However, it could be useful if behavioral and security process data are interchanged by airports too, this would lead to a more rapid adaptation of the airport security system to find abnormalities in the behavior or actions of passengers. For this security risk assessment not only the scope of a worldwide airport network is too broad, but also the way of operating of the airport security systems drives this decision. Namely, in order for a worldwide airport network to be in place, all the airports should have a similar operating airport security system. There is no need to perform a security risk assessment for all airports separately. By only analyzing one airport's security system interesting results could be obtained, while results from communication with and operation of other airports do not add more value to these results.

The environment of a single airport security system is still very broad by itself though. Depending the size of an airport, millions of passengers set foot physically at the airport premises. These passengers can be divided into different types of travelers [11], for example business or leisure passengers, but more importantly these passengers can be categorized as departing, arriving or transferring passengers. These different types of passengers all need to undergo different processes at an airport specific for their category as explained in Section 2.1 and Figure 2.1. In security research on airports mainly departing passengers are used as a subject. This is because departing passengers physically spend the most time on the airport premises and they have to undergo the most airport processes and in the case of arrival or transfer passenger, they all were once departing passengers who had to go through the airport security system [6]. These facts form the most interesting basis for the security risk assessment which is being performed in this thesis.

When considering only one airport configuration and only departing passengers the airport environment which can be analyzed doing a security risk assessment is still fairly broad when considering all security risk scenarios possible.
Passengers send information from their houses while they buy a ticket, databases of historical data of passengers are available, criminal records and at the airport of course all the processes in order to board the aircraft. These different areas all contribute to the overall security of the airport environment and can thus be taken into account. After 9/11 and other serious terrorist attacks around that time the focus of security research laid in optimizing single security devices, such as passenger or baggage scanners, and passenger profiling by security guards [3]. Recently, the focus shifted more towards tracking of behaviors and movements of passengers in the public area of the airport terminal or in through the entire airport [68]. The research in these domains have come up with useful results and changed the equipment used at airport for the better concerning the security in the airport environment. However, security is a very dynamic domain. Threats always change and adapt such that they fulfill their purpose the best. This means that security research should be investigating new solutions all the time as well. That can be seen in the recent change of focus in this field. Nowadays security research, as well as products of airport security equipment companies, focuses on the integration of the airport security system. Integration of the airport security system is defined as the use of data of all sensors in the airport environment to make a more detailed picture of the current situation in the airport environment in order to assure the security for all people present in this environment [69] [70] [71]. As the integration of the airport security system is still a very new development, there is not a single approach which is used and different approaches may lead to other outcomes. Most security research and products of airport security companies take into account the entire single airport environment. Which means the data from passengers they can obtain already before the day of arrival, the airport environment outside the secured airport premises such as entry roads, public transport stations, car parks, the airport security access sensors which track the possibility of unauthorized access of people at places other than the airport terminal, and all airport sensors and processes within the airport terminal.

Although this integration gives the entire picture of the airport security system, it is a rather grand operation [70]. Therefore, for this thesis it is chosen that the airport terminal environment, by using known passenger information too, is the most interesting area to analyze. This decision is made because the most and a wide variety of individual security systems are present in the airport terminal environment. Propagation of a threat through this environment, from arrival to the aircraft, is highly unwanted and would mean a failure of all individual security systems. The airport terminal

environment is therefore the ideal environment to implement and analyze an integrated configuration of an airport security system.
The environment used for the research is shown within the green line as can be seen from Figure 4.1. Doing this the environment stays manageable but still gives a good overview of the integration and process of the entire airport. By using this airport terminal environment all present sensors can be used for integration and to check their working abilities when a threat propagates from entrance to aircraft. While of course there can exist certain scenarios in which the threat does not come via the airport terminal, the use of integration would suit much less in these cases.

To summarize, the environment under investigation during the security risk assessment for the airport security system will only be the airport terminal including all its equipment and attributes. Although only this airport terminal environment will be used, it gives a good opportunity to include all sensors in this area in order to investigate the performance of this security system and to analyze the possibilities to integrate the security system to increase this performance while passengers propagate through this airport terminal from entrance to aircraft encountering all airport processes needed to board the aircraft.

4.2 Identify and analyze the threats and vulnerabilities of the airport security system and determine the perceived risks for the airport environment

The basis on which security research is focusses is threats and vulnerabilities of the environment under investigation, which both cause security risks for this same environment. The step of the identification of threats is possibly the most well-known step of a security risk assessment, but it is a very useful tool to categorize threats and vulnerabilities in order to see the most dangerous potential hazards for the environment under investigation and therefore the areas of improvements or further analysis are obtained. As the domain of security is very dynamic and attacks are present every day but can have different forms every time the amount of threats, vulnerabilities and risk are very broad and diverse. Every group of a specific threat or vulnerability would need a more unique approach when further analyzed. This would be very time consuming, therefore in this thesis the threats, vulnerabilities and risk assessment will be used to obtain an interesting category which is nowadays hot topic in order to continue the airport security risk assessment with. Although the approach used later on when modelling the threats could be similar for certain categories of threats.

4.2.1 Identify the threats and vulnerabilities present for the airport security system

An airport is a really valuable asset and has many valuable assets in its environment [4]. It has a lot of people, as employees, customers, passengers, visitors. An airport is a materialistic asset too as it is most of the times a very modern property with a lot of expensive equipment. Informational assets in the form of passenger data and security data are present as well. And above all, an airport is in a way as well a freedom asset, from one airport people nowadays can move towards any other place in the world. People strongly rely on their ability to move and to perceive the feeling of freedom.

When analyzing the possible threats for the airport environment under investigation in this research only threats which have a certain degree of intend with them are dealt with. So, for instance natural disasters are not taken into account when making the list of all possible threats. The horrible attacks of 9/11 and all other similar attacks later on are a prominent example of security related threats for the airport environment, however these attacks are just one of the possible threats the airport security system should be able to cope with. After analyzing the airport environment nowadays, below a list, defined for this research, d possible intended threats which are important the airport security system can notice and take action against [4] [72] [6]:

- Panic creation technologies, i.e. noise/smoke/fireworks
- Bombs and explosives
- Ballistic attacks
- Armed assault
- Hijacking, hostage or barricade situation
- Cyber attacks
- Chemical materials attacks
- Passenger properties theft
- Equipment and/or infrastructure sabotage
- Movement of illegal immigrants
- Use of false personal ID or biometric data
- Use of false tickets
- Trafficking of unauthorized materials, i.e. drugs/guns/ammunitions/biological material/food
- Money laundering

These threats can be seen as separate categories, although some might sounds very similar and therefore will, most likely, have a similar way of representing and modeling. Still, this is a wide range of different types of threats. Although an airport should cope with them all, for this thesis that kind of analysis will be too broad. Only one group or a small number of similar groups can be addressed during this research. Therefore the threats are assessed based on their perceived risk for the assets in the airport environment. The threat category that has a perceived risk with the most striking character is addressed to be implemented in the security risk scenario for this research.

Vulnerabilities in the security system make that aforementioned threats can propagate through the secured environment and succeed in their intended goal. Vulnerabilities can be found in all aspects of the system. Although the actual cause of the propagation of a threat in this research will not be analyzed, it is still useful to know what kind of vulnerabilities there can be present in the airport security system. The type of vulnerabilities that can be defined for a system influence the likelihood of a threat in the environment.
Below a list of vulnerabilities for the airport security system is presented which could lead to a successful action of a threat:

- Understaffing
- Staff not mentally in excellent condition, i.e. poor motivation, lack of skills, tiredness
- Staff cooperating with threat
- Inadequate or unreliable equipment
- Equipment failure or not working
- Too much focus on only one piece of equipment or a part of the security system
- Technical system or software not up to date or overburdened

The degree of each vulnerability and the actual presence will determine the perceived risk of each possible threat category. The degree of vulnerability is the probability that all security measures fail. This research covers all vulnerabilities instead of addressing one at a time to describe why all security measures failed. The KPIs of the airport security system can therefore also be seen as a measure of the vulnerability of the airport security system to a certain threat.
All threats can be present and can be incorporated in a model later on when the airport security system is analyzed for a certain threat category. The only vulnerability which is not included in the research is the possibility that a certain staff member cooperates with the threat. Although it is a crucial situation

to investigate and mostly very alarming for a company to encounter, it is as well an entirely separate situation. Actually it can be seen as a threat by itself.

4.2.2 Determine the perceived risks of the analyzed threats

With the use of the identified threats and vulnerabilities the perceived risk a threat poses on the assets in the airport environment can be identified. The perceived risk can be used in order to see what impact certain threats have when the vulnerabilities of the security system can be exploited. The security system operates such that the perceived risk by a certain threat is as minimal as possible. Therefore it is important to analyze the security system and implement risk reduction where possible. Risk reduction is one of the key objectives pursued by organizations working with security related services. Before risk reduction can be executed it must be known what kind of risk should be dealt with and the severity of risk the different threat categories apply to the airport security system.

Risk can be defined as the probability that a certain threat attack will occur multiplied by the severity of the consequence of this occurrence. Therefore, a risk can be called an attribute of a threat [33]. The security risk assessment performed in this thesis is an analysis based on an existing airport security system, and although a new airport security system is designed with integration it can be assumed that the basis of the newly designed airport security system is adopted from the already existing security system. Also, the threats under consideration are threats that are assessed at only a certain time point, these can change over time for the airport environment. Therefore the most convenient type of risk analyzed is the current risk.

Due to the availability of data and the security risk assessment approach followed in this research, the risk matrix approach is adopted in order to analyze the perceived risk of the identified threats. Two parameters need to be evaluated for each threat, respectively the likelihood and the impact. The schemes defining the categorization of these parameters shown in Section 2.4 will be followed to determine the perceived risk for each threat.

The parameter likelihood in the determination of the degree of risk of a certain threat category is normally used as the probability of successful occurrence of this threat. However in the determination degree of risk put upon the airport security system the likelihood parameter will be used as just the probability of occurring of this certain threat. This approach is taken as there is not a lot of data present of actually successful threats with respect to performed threats. This means that it does not matter for the threat action to be successful or not. Eventually, the vulnerabilities of the airport security system determine whether or not the threat will actually be successful. This will be analyzed later on when the airport security system is modeled in order to analyze how it reacts on a specific threat category.

The parameter impact in the determination of the degree of risk of a certain threat category is defined as a measurement of the consequences of this threat. A successful threat can have different degrees of impact on the assets in the airport environment. Therefore it is useful to know which kind of assets are present in the environment under investigation and what type of consequences the threat can have on these assets [73]. For the airport environment impact can be seen as a harmful event for the assets. The assets have many domains which can be impacted by a successful threat [43]. The different domains are defined in Table 4.1.

Impact	Description
Health people	Refers to the state of a human being. Either physically or mentally.
Efficiency	Time needed to check-in, security controls or boarding.
Human rights	Human rights, e.g. the way a person perceives privacy, autonomy, non-discrimination, dignity.
Social values	Social inclusion, e-inclusion, trusted human relationships, etc.
Legal and regulatory	Existing legal regulatory framework needs to be respected. It foresees consequences for violations and for failure to fulfil the obligations foreseen in it. It delineates the passenger rights. PNR is also based on bilateral/international agreements on the transfer of information of the passengers.
Mobility of travelers	The freedom of a person to travel, small distance and across countries
Financial	Cost considerations for airlines, airports, companies and individuals.
Comfort	Smooth processes, services on demand, usability. The provision of services for people with amenities.
Interoperability	The possibility of communication between individual systems, operators and organizations.
Trust	Trust in the means of transportation, in the organizations providing the means of transportation and the environment in which the means of transportation is executed.
Business activities	The ability of businesses in and around the airport environment to perform their activities.
Infrastructure and equipment	Refers to the equipment and its infrastructure used in the airport environment.

Table 4.1: Possible impact domains of threats and their description

The threats within the airport environment which were identified in Section 4.2.1 are weighted with respect to the schemes of the likelihood and impact parameters in order to find the risk they impose to the airport environment and the assets present in this environment. The weights are assigned based on analysis of past attacks with the specific type of threat. The risk matrix results for all threat categories is used in order to find an intriguing threat for which the airport security system will be analyzed for. Only one threat category, or a group of threats if the way of modeling is similar, will be used to analyze the airport security system as the modeling of a security risk assessment is a time consuming performance. Table 4.2 shows the results of the performed threat risk assessment.

The degrees of the likelihood and impact parameters are assigned on the basis of historical data and the current state of the world. The likelihood shows the probability of occurrence of the threat category. This probability of occurrence is determined by the probability an attempt is made by this threat category and not by the probability that the action is successful, as it is the task of the airport security system to stop the threat from propagating through the airport environment under investigation. Historical data is used to see how often a threat category is active in the airport environment. Not only historical scenarios are used in the determination of the likelihood of a threat category. The current state in the world and scenarios used by attackers nowadays, which may happen in other domains than the airport environment, are taken into account as well.

Threat	Likelihood	Impact	Risk
Bombs/explosive attacks	Likely	Catastrophic	Extreme
Armed assults	Likely	Catastrophic	Extreme
Cybar attacks	Likely	Major	High
Chemical material attack	Seldom	Catastrophic	High
Hijacking, hostages or barricade situation	Likely	Moderate	High
Equipment and/or infrastructure sabotage	Occasional	Moderate	High
Passenger property theft	Likely	Minor	Moderate
Panic creation technologies	Likely	Minor	Moderate
Movement of illegal immigrants	Occasional	Insignificant	Moderate
Use of false personal ID or biometric data	Likely	Insignificant	Moderate
Use of false tickets	Occasional	Insignificant	Moderate
Trafficking of unauthorized materials	Definite	Insignificant	Moderate
Money laundering	Likely	Insignificant	Moderate

Table 4.2: Identified main threats and their security risk matrix categorization

With these data in mind it can be seen that chemical attacks on airports or attacks with chemical substances did not often occur and the trend nowadays of attacks is not pointing in that direction too, although there are a lot of chemical substances available. This type of attack is the least probable and rated with the degree seldom. Use of false tickets, movement of illegal immigrants, equipment and/or infrastructure sabotage are all threat categories which do not happen that often. The reason for that is that there are easier targets with less security levels present. Although all of these threats happen the vulnerabilities of the airport environment do not occur in this area that strongly. Threat categories money laundering, use of false personal ID or biometric data, passenger property theft, cyber attacks, hijacking, armed assaults, explosive attacks and panic creation technologies are all likely to happen in the airport environment. Some of these threat categories happen more than others or are more extensively discussed in the news and others have a higher probability of occurring due to the recent world state and terror attacks. For instance explosive attacks or hijacking are known to happen, with respect to the number of flights in a year it is not a large percentage. However nowadays more and more attacks with explosives are undertaken, which means that the airport security system should be prepared to tackle this threat. While a threat category as passenger property theft is always present in the airport environment, just like it is present in any public environment, regardless the change of the world state. The only threat category that is definite to happen is the trafficking of unauthorized materials, i.e. drugs, food, other objects. Every day all airports around the world have to be cautious for passengers and their luggage as there is the probability that a passenger wants to smuggle unauthorized materials as airports are an easy gateway to any place in the world.

The impact shows the consequences of the threat category on the assets in the airport environment. There should be a direct impact on these assets exerted by the threat source. The most common types of impact in the airport environment are casualties or injuries of passengers or other people in the airport environment or damage or loss of properties, equipment and infrastructure. From Table 4.2 can be seen that money laundering, trafficking of unauthorized materials, movement of illegal immigrants, use of false tickets and use of false personal ID or biometric data are rated with the degree insignificant for the parameter impact. These threat categories, although illegal and punishable, cause no harm to assets in the airport environment. The airport environment only is a means for the attacker and the goods to change places quickly. The degree minor is assigned to the threat categories panic creation technologies and passenger property theft. Both threat categories will create some damage to the infrastructure, goods or people, though not much with respect to the amount of people, goods and the size of the infrastructure. More damage is done by threats like equipment sabotage and hijacking, although not always easy to determine. Especially in the case of a hijacking the impact can be more psychological than physical. The two threat categories which got the major impact degree assigned are cyber-attacks and chemical attacks. This is due to the fact that a lot of people can get affected and even the infrastructure of the airport environment too, but it depends the type of cyber attack or chemicals used how big the disaster is. The two catastrophic threat categories are explosive attacks and armed assaults. These attacks are most likely to cause havoc in the airport environment by making many casualties and injured people and damaged property, equipment and infrastructure. It does not matter if the attack is executed at the entrance of the airport environment or at the end in an aircraft, the outcome is always catastrophic and highly unwanted.

The likelihood and impact parameters result in a degree of risk. After the explanation of the likelihood and impact parameters it can be seen that the threat categories with the catastrophic impact degree have the highest level of risk for the airport environment. This means that the airport security system should be able to avoid this threat from happening at any time. Of course the airport security system should be able to tackle all threats in the security domain identified and rated in Table 4.2, as these threats are executed with a certain degree of intend and are illegal to perform.
To continue the security risk assessment one threat category is chosen to be modelled in the airport security system in order to analyze the performance of the airport security system. The threat category chosen is explosive attacks as this is nowadays a hot topic in the domain of terrorism and attacks, it already happened before in the airport environment and it causes a catastrophic impact which should be avoided. Other threat categories as cyber attacks are nowadays getting more and more relevant for the airport environment as it can shut-down an entire airport with its operations, however these attacks do not fall in the scope of analyzing the propagation of threats through the airport security system.

4.3 Construct the security risk scenario

The identification of the airport environment and threat category under investigation are important steps for the scope of the security risk assessment. There are many different ways a threat can be executed within the airport environment and for a threat category to be modeled a clear scenario should be build [6]. A scenario can be seen as role-playing of all the actors in the airport environment such that a realistic overview of the situation and thus imposed threat can be made. Other than the threat type, the threat scenario consists of three parts which need to be identified. These three parts are:

- Where is the threat executed?
- Who executes the threat, who is the threat source? And how is the threat performed?
- How does the airport security system look like to stop the threat action from happening?

These questions should be answered for the explosive attacks threat category which is taken into account in order to analyze the performance of the airport security system. Without a good scenario the threat cannot be judged correctly, which would lead to senseless results of the security risk assessment.

Where is the threat executed?

In Section 4.1 the boundaries of the airport environment under investigation for this security risk assessment were already narrowed down. Only the airport terminal and the personal information known from outside the airport terminal environment are taken into account. This means that the area around the airport terminal, parking places, hangars, runways, fuel storage areas, business area, etc. [4], which all could have a high attractiveness for attackers are not taken into account in a threat scenario, shown in Figure 4.2 by the red circle. Nevertheless there remains a broad range of possibilities for an explosive attack to take place as the airport terminal is mainly a large property and there are many assets present at different locations. The main locations at which an explosive attack can occur in the airport terminal environment are defined in the list below:

- Near the entrance of the terminal
- In the public areas of the terminal
- In the secure areas of the terminal after security processes
- In the secure areas of the terminal only accessible by staff and not by passengers
- In the cargo areas of the terminal
- At the airport terminal security checkpoints
- In an aircraft

All areas will bring up their own problems and their own ways of avoiding the threat action from happening induced by the airport security system. In the thesis the main goal is to analyze the performance of the airport security system how it operates currently at many airports and to compare the performance with a more integrated airport security system. The best way to analyze this performance would be to investigate how a threat action would propagate through the airport environment. Therefore it would not be efficient to investigate a threat action performed early on in the airport terminal environment, although nowadays this is a commonly used approach of attackers with explosives as less airport security system layers have to be tackled. Another approach used by attackers is to smuggle the explosive on board of an aircraft in order to both make damage to a highly valuable product and make many casualties. The outcome if this would happen more times than it already did in history would be catastrophic. As smuggling an explosive on board of an aircraft requires the propagation through the entire airport security system, the scenario of an attacker wanting to bring an explosive into the aircraft is used. This will show which vulnerabilities of the airport security system are actually present and which have the most influence on the propagation of the threat.

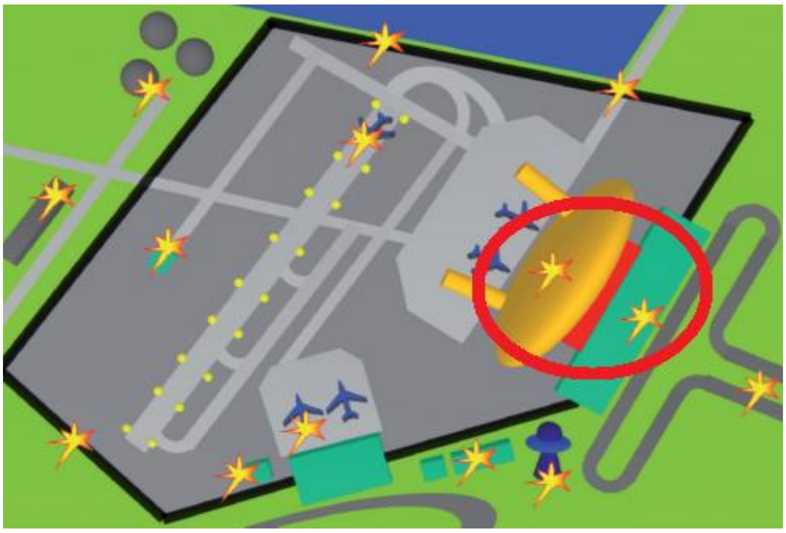

Figure 4.2: Airport assets with possible potential interest for threats, red circle indicates area under investigation in this research [4]

Who executes the threat? Who is the threat source? And how is the threat performed?

For a security system it is always important to know, not only where a threat action can take place in the environment, but also who your attackers can be. Historical actions at an airport or any other domain and experience in the change of attacks nowadays should be analyzed in order to answer the question how the composition of a threat source working on an explosive attack looks like [6]. Below a list is provided with the most likely options how an attack with explosives would be performed:

- Single attacker
- Group of attackers, all with their own threat object
- Group of attackers, all with a piece of one threat object
- Passenger used by an attacker, but not aware of being used
- Insider at the airport
- Attacker(s) with help of insider(s) at the airport

Just like the area in the airport environment where the threat will be performed in the scenario, the actual threat source should contribute to the analysis of the performance of the airport security system to stop a threat from propagating through the entire system. After an attack is performed and thorough analysis is done to find the offenders, it is mostly seen that the attack was executed by an insider at the airport or an insider at the airport provided the attackers with help. Although this is a very interesting case to analyze as no company wants to find out that their own employees performed an attack, it is a hard scenario to model the propagation of the threat through the airport security system as the insider can avoid a lot of layers of the airport security system. Furthermore there is no real difference between the single attacker, a group or an used passenger approach with respect to propagating threats through the airport environment. The only real difference may be the behavior which actually plays a significant role in categorizing passengers at an airport nowadays. A single attacker approach is chosen to show the difference between an attacker and a normal passenger in the airport environment and to check whether the airport security system is able to find the difference between an attacker and a normal passenger.

The behavior plays an important role to categorize the type of attacker and to differentiate an attacker from a normal passenger. Different types of attackers can be distinguished. These different types of attackers will have different ways of operating, different ways of behaving and thus may have different degrees of successfulness of the attack action and different probabilities of getting caught by the airport security system [74]. The airport security system should be able to recognize and detect all types of attackers when they are present in the airport environment. However, effective layers of defense of the airport security system can only be set when the airport security system understands the behavior and strategic logic that drives the different types of attackers. Although a typical profile of an attacker cannot be made, still attackers may have some signs in their behavior which are striking for the airport security system [75]. In recent days the security system only looked out for one type of characteristic of an attacker. Security officers became to rely mostly on behavioral profiling to catch attackers or suspicious acting people whom could be identified as attackers [76]. However, this may not form the entire picture of a passenger. Experts say that when you know the attackers you know their plans, which would make it easier for the security system to catch the attackers [75]. If there is a good description of a specific attacker available, then the prepared attack can be better predicted. The difficulty is that there are many types of attackers.

To form the entire picture about a possible attacker more information can be useful. Figure 4.3 shows the subdivision of the properties of an attacker which are useful to make an identification of a suspicious person. The individual security systems measure at least one of these properties, such that the picture can be formed as efficiently as possible and a suitable identification can be made.

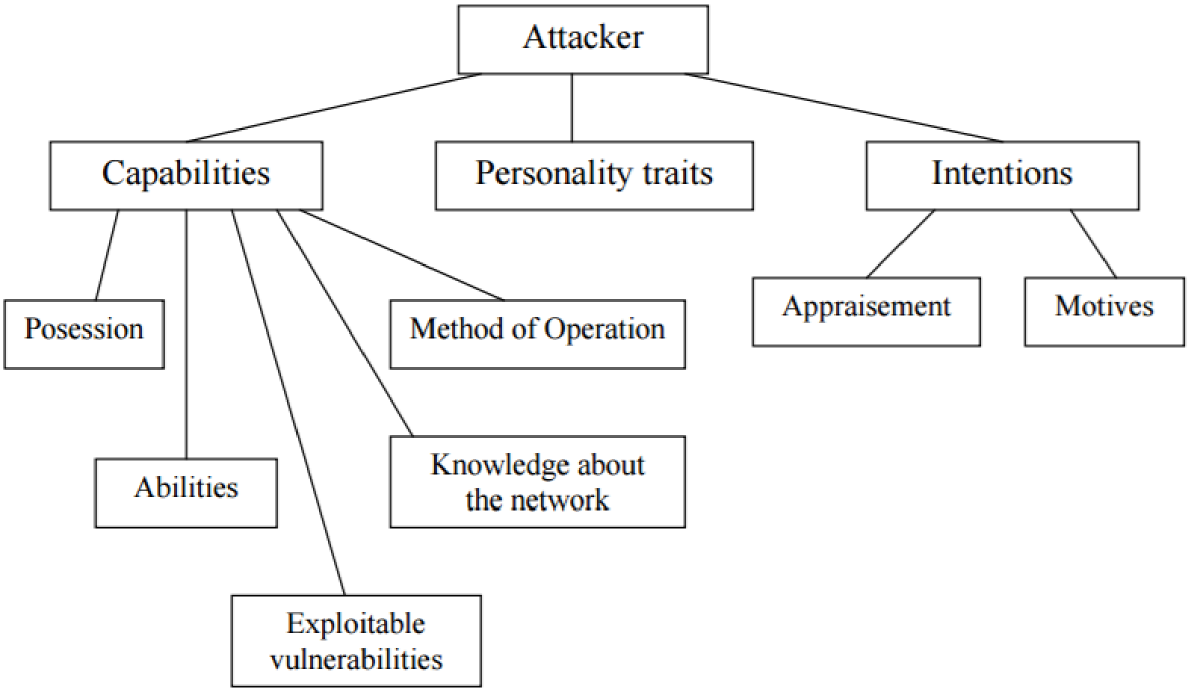

Figure 4.3: Attacker characteristics [74]

As can be seen from the Figure 4.3 three main properties of an attacker can be identified. These are the capabilities of the attacker, the personal traits or behavior of the attacker and the intentions of the attacker. These properties are used in order to make a categorization of the attackers performing the type of threat analyzed in the security risk scenario.

The capabilities of the attacker can be explained in more detail by the five groups; possession, abilities, exploitable vulnerabilities, method of operation and knowledge about the network. The capabilities category consists out of a few other groups which describe what the attacker can do and how well the attacker can do this. The abilities group describes for instance the skills the attacker has in executing a certain attack. While the method of operation, exploitable vulnerabilities and knowledge about the network describe a more general picture on what the attacker exactly does while executing the attack and how well the attacker the environment under investigation knows and can benefit from. Capabilities are thus a way to describe the level of experience and skillfulness of an attacker.

Within the environment of the security system the personal traits or behavior of a certain person are very important to identify this person as an attacker or not. Interesting behaviors to check an attacker for are judgment, morality, patience and cautiousness. Morality shows the degree to which the attacker is willing to achieve the goal of the attack. This trait can be good to take into account when composing risk scenarios, however it is difficult to tag a certain behavior as being a sign of low or high morality when the attacker is already within the environment under investigation and executing the risk scenario under investigation. The other personality traits or behavioral aspects of an attacker which were mentioned earlier are of course not the only ones, there is a wide variety of different traits, movements and behaviors an attacker or normal passenger can possess which can be identified by the security system and thus lead to a decision about the type of person the security system is dealing with. However, it can be assumed that almost all personality traits or behaviors can be explained by one of these terms. It is just the way how to explain a certain movement or exerted behavior of the attacker during the execution of the attack. Behaviors can be linked to capabilities as well. A more professional attacker has the capability to control his behavior better than a less experienced attacker or the professional attacker can even adapt his behavior in such way to try to mislead the security system.

The last category in order to draw a picture of a possible attacker is based on the intentions of an attacker. This category consists again of two different groups; appraisement and motives. Appraisement defines how the attacker rates the assets within the environment the attack needs to hit. While the group motives literally explains the motives of the attacker, why the attacker performs the attack on these specific assets. The intentions category is a very important category for a security system to take into account when building security risk scenarios, when evaluating which types of assets the environment has and when to build profiles of types of attacker who can enter the environment. However, when an attacker has entered the environment under control by the security system, like is the case in this thesis, the intentions of the attacker are less important. The main issue is to identify this person as an attacker, based on results the sensors within the environment obtain from this person.

Four different classes of attackers who are known for performing the attack under consideration in the security risk scenario are set up. The basis is to identify the difference in skillfulness of attackers and thus the different aspects security officers and the security system should look out for. The need to know the attack's skills is the principal thing in stopping them. The type of threat object an attacker uses determines the severity of the risk imposed on the target and the type of operation the security system should perform to stop the attacker. But when not considering the possibility of a different type of threat object, as for this research it was chosen that the attacker would make use of an explosive, the skills level can be used to determine different behavioral traits and tactics. Below the five different attacker classes are described:

Class I: Professionally trained attackers

Class I attackers are the attackers whom possess the highest level of skills and experience. These people can be described as really extensively professionally trained persons. Although this is the class with the most skills, it is also the rarest class of attackers. These people come from countries with a well-funded and trained secret service organization or a regime that sponsors attacks. These people operate their attacks with maximum secrecy. To obtain their goal they could even use official or nonofficial covers instead of their own being. These attackers are well aware of the threat for themselves and can adapt their behavior and tactics quickly in order to stay under the radar of any security systems. Professional attackers prepare their attack thoroughly, taking all the risks of the attack in consideration. The profile of a class I attacker can be seen in Table 4.3.

Age	22 - 50
Gender	Male or female
Schooling	University; professional intelligence agency educated
Social environment	Middle to upper class; party or political loyalist
Criminal history	No criminal history before recruitment
Military history	Military special operations soldiers, political party civilians, national intelligence community members
Most common activities	Assassination, sophisticated explosive bombings, supply equipment or give training
Level of experience / skillfulness	High level of experience, in the field and due training

Behavioral traits	Blends in environment, aware of security measures and can adapt his behavioral properties as needed

Table 4.3: Profile of a class I attacker [2] [75]

Class II: Extensively skilled attacker / religious extremist

Class II attackers are highly skilled and focused attackers. They can be defined by a combination of a good level of skillfulness of operating an attack and knowledge about the goal of the attack and its assets. This class thus consists of civilian people, but choose to live a live to execute one or more attacks but not as a profession or in a former job. The attackers in this class receive advanced combat skills and ideological training from their attack cell or group or they train themselves for the purpose of the attack. Although this training is not as professional and extensive as it would be from an official organization, which means that the skillfulness is not as professional as class I attackers. Specific character traits become therefore more visible for sensor of a security system as well, although the attacker is aware of this possibility. The profile of a class II attacker can be seen in Table 4.4.

Age	18 – 45
Gender	Male or female
Schooling	Diverse
Social environment	All classes; generally a devout follower of a certain believe (nationalism or religion)
Criminal history	Diverse
Military history	Some have military training and are often trained at local or overseas attack schools
Most common activities	Sophisticated and advanced improvised explosive bombings, firearms assassination, skyjackings or kidnappings, infrastructure attacks, cyber-attacks
Level of experience / skillfulness	High level of experience due to training
Behavioral traits	Knows the environment and security measures, shows little deviant behavior

Table 4.4: Profile of a class II attacker [2] [75]

Class III: Moderately skilled attacker

A class III attacker could possess either some skillfulness in executing an attack, some knowledge about the target and the assets of the target or a bit of both. The experience of this category of attacker cannot reach the same level as the previous two categories of attackers though. The lack of experience, especially in executing attacks, relative to class I and II attackers makes this category more vulnerable to display suspicious behaviors that attract the attention of a security system and thus to being identified as attacker by this security system. On the other hand, their lack of experience and thus history in these attacks could make them less visible for some sensors within the security system related to the history of passengers at the airport. The profile of a class III attacker can be seen in Table 4.5.

Age	20 – 50
Gender	Male or female
Schooling	Diverse; no education to university degree
Social environment	Average to upper middle-class family background
Criminal history	None to minor criminal history
Military history	None to some possible former military history

Most common activities	Improvised bombs, pistol assassination, small raids and robberies, kidnappings
Level of experience / skillfulness	Medium level of skills, commonly no high experience with attacks
Behavioral traits	Shows typical deviant behavior; strange movements, nervousness, communication, etc.

Table 4.5: Profile of a class III attacker [2] [75]

Class IV: Amateur or untrained civilian attacker

The last category is a very broad class of attackers and therefore as well one of the most time consuming in the sense of detecting an attacker from this class. Although class IV attackers are the least skillful relative to all other classes already discussed. Attackers in this category did not follow the extensive training of class I and II attackers and trained themselves in less degree than class III attackers. This means that they do not have the experience and skillfulness more professional attackers have and this can be noticed in the planning and execution of the attack. The other hand deviant behavior from attackers in this class are much more noticeable because they do not have much experience with attacks. The profile of a class IV attacker can be seen in Table 4.6.

Age	10 – 65
Gender	Male or female
Schooling	Diverse, none to university degree
Social environment	Urban or rural poverty, raised in criminal or combat culture, middle class or upper class leadership
Criminal history	Diverse, none to criminal history
Military history	Criminal or combat cultural history possible, mostly no training or self-learning
Most common activities	Improvised explosives bombings, kidnappings, pistol assassinations, small raids and robberies, physical violence
Level of experience / skillfulness	Medium level of skills and no experience
Behavioral traits	Not good aware of the environment, has striking deviant behavior

Table 4.6: Profile of a class IV attacker [2] [75]

The categories of attackers is used to further build the security risk scenario under investigation in the thesis. It was already known what the threat action and source would be, namely an attack possibly with explosives carried onto the aircraft. Which means that the threat source and object need to go through all stages of the airport environment. In order for the security system to fully understand the nature of the attack, the type of attacker executing the attack needs to be analyzed as well. That is what was done by means of the categories above. There are many different ways of categorizing attackers and many different classes can be formed within a certain categorization type. Although for the attack under investigation these four classes discussed above are the main classes within the categorization. Although all classes of attackers can be present in real life, which means that the security system always needs to be prepared to identify these attackers, two of the classes will not be used in the security risk scenario further on, respectively class I and class IV attackers. These two classes are not used to further build the security risk scenario as they would not have the depth to use of all the sensors of the security system in the airport environment. Also, if all attacker classes would need to be investigated the number of samples in the group of passengers would get really large. The group of class I attackers is just too small to include them in the security risk scenario. There are only little people who belong in this group and thus the change of actually an attack being performed by them on an airport is relatively null, even so because the airport environment is a public space with public assets. Class I attackers usually only have military missions. In the case that such an attacker would perform an attack on an airport, the attacker could easily propagate through the airport environment as the person would be unknown due to his cover and behavioral traits could be rather difficult to spot due to the extensive professional training. For class IV attackers it is the other way around. This type of attackers has no experience in executing this big attacks. The change that amateurs actually will perform an opportunistic attack from this size at such large public environment is rather small, as it takes a lot of preparation and resources. When looking at behavioral traits class III and IV attackers can be quite similar, which in that sense makes it more realistic to drop class IV attackers in the security risk scenario.

This leaves class II and class III attackers to be used in the security risk scenario. These two classes are the best to implement as they use all aspects of the airport security system. These attackers can be closest identified with real attacks nowadays at airports and force the airport security system to use every sensor present in order to identify them. The difference between the two classes is the degree of skillfulness and experience. Class II attackers are more professional relative to class III. They could benefit from more professional training. This training will address experience in combat, use of resources to prepare an attack, planning of an attack and how to behave while executing an attack. This leads to the possibility of more powerful threat objects, more professionally hidden threat objects, a better planned attack and the skills of adapting behaviors in the advantage of the attack. While class III attackers cannot benefit from this extensive training facilities or even no training at all. Nevertheless, their attack is more targeted than opportunistic. So, relative to class II attackers their attack has less professional threat objects and is less thoroughly planned and they do not have the experience or skills to adapt their deviant behavior such that they are not identified as suspicious by the airport security system. The advantage of class III attackers is the lack of history in criminal activity, which can give them a little advantage over class II attackers and leave them under the radar of a security system.

In order to investigate the possibilities of the airport security system three different attackers will be modelled. A clearly class II attacker who's history is known but has more difficult behavioral traits to identify, a clearly class III attacker from whom there is no history known but has clear behavioral traits to identify suspicion and an attacker who can be categorized in between class II and class III or as a new class II attacker, as this attacker can have some history and has less suspicious behavior as a class III attacker but more suspicious than a class II attacker. In order to see the efficiency of the airport security system not only attackers will be analyzed, but also normal passengers who can have some history and all the suspicious behavioral traits present as well, however the normal passengers should not be identified as suspicious as they are not a threat source. More explanation about the attackers and passengers is given in Section 4.4.5 when the agents of the agent-based model are described.

The attacker can use different ways to smuggle the threat object into the aircraft. The most conventional ways are by wearing the threat object on the body or hiding the explosive in either the carry-on luggage or the baggage. However nowadays attackers are getting more clever and use more modern technologies or they send the threat objects via cargo such that they cannot get linked to it personally. Only the conventional ways of smuggling the explosive into the aircraft are taken into account in this security risk assessment as this is still the most commonly used method when executing an attack used in the security risk scenario and via this route all defensive layers of the airport security system will be encountered and thus the vulnerabilities of this airport security system should be exploited in order to get to a successful attack. Three attacker profiles are used already and therefore three ways of getting the threat object onto the aircraft are considered as well. The first way is by concealing the threat object in the cargo baggage, the second way is by carrying the threat object only on the body or only in the cabin luggage and the third way is to divide the parts of the threat object between the cabin luggage and on the body. The latter would induce a more intelligent approach of the security system as maybe only one part would not be a threat object, but together it will be.

How does the airport security system look like in order to identify and stop the threat action from happening?

A security risk assessment is performed from the defenders perspective to investigate which threats are present on the assets of the defender. The previous questions answered to build such a security risk assessment have therefore dealt with the attacker's side, namely the threat objects, threat sources and threat scenarios to which the defenders environment is objected. Questions about the attacker and its ways of operating are mostly the initial questions analyzed as the attacker is commonly the first things that comes in mind when thinking about security and risk. Undoubtedly, it is very important to know as much as possible about all possible threats, attackers and ways of working. Else ways, it will be very difficult to identify such an attacker for the security system when a threat actually tries to propagate through the environment. However, as important as questions about the attacker are questions about the defender themself as well. The attacker could have an advantage if the defender does not know critical information about its own systems and ways of operating. This certainly holds for experienced attackers who would first investigate the environment in which they would like to execute the attack, as they could observe the weaknesses in the defender's security system. Therefore studying the defender's own side of the scenario is as important as analyzing the attacker's side. The investigation of the defender's side is actually already roughly done when establishing the environment for the security risk scenario. Here the borders of the defender's environment and assets were established. However, the study should go deeper into the security system, because with only the environment attackers are not identified and the threat won't be stopped. Therefore the question presented above should be always addressed when performing the security risk assessment. This question will establish a thorough representation of all the systems present within the environment which are used to identify and stop a threat action. The operational efficiency and weaknesses of the entire system can be found after this thorough representation is built and used in the threat scenarios under consideration.

Two different representations of the defender's security system will be addressed. The difference of the two systems can be found in the operation rather than the composition. As discussed before the operational efficiency of these two systems will be compared to each other as new technologies are available for building a security system. The first security system dealt with, called current security system, is a security system which is used nowadays at most of the airports in the world. It is a highly protective security system with all processes and subsystems needed within an airport environment. The operation of all these processes and subsystems however can be seen as isolated, stand-alone lay out. No direct communication is present between subsystems. The second security system is a new conceptual security system and will be built by means of a new technology called data fusion. Using this new technology the subsystems of the security system will be integrated. This means the subsystems can communicate about passenger profiles, observations, results and decisions.

The study of the defender's own security system can be labelled as an activity of workflow management [77]. Workflow management reflects on business structures, which is done by studying how the security system looks like and operates. Different views of the security system may be created, depending on the information what is needed. These views, mostly presented in a type of block diagrams, can be used as conceptual model for the implementation of the airport security systems in the programming software. Two main views are always used next to the other possible views in workflow management. Normally a separate organizational model and a process model are built, and can thus be seen as the main views. Although Sharpaskykh [9] introduced a new more thorough modeling approach of the views. Four interrelated views to accompany the formal model of the organization are used. The performance oriented view, which describes the goal structures, performance indicator structures and the relations between the goal and performance indicator structures of the organization. Organizational modeling involves the identification of all actors in an organization and the organizational relationships. The agent-oriented view, which describes all operators in the system with their capabilities and behavior. The organization view, which shows the organizational roles, the authority and relations between these roles. The agent view and the organizational view are closely related as the agents fill in the organizational roles. Lastly the process view, which shows the organizational functions and processes and the relationships and order between the processes. Although all views are related to each other, normally the views are constructed separately but there is the ability to link and merge views.

The airport security system can be approached in a similar way as this method to describe its structure. For the airport security system it is really important that the different views are used, because the socio-technical aspect of the airport security system makes this a very complex organization. To analyze its performance the structure should be thoroughly identified.

4.4 Conceptual modelling of an airport security system

In traditional organizational modeling the organizational structure is described by means of role, position, authority and organizational units. Depending on these organizational characteristics that one wants to highlight the model can be built in order to be able to express these specifics. The rapid scientific, societal and technological development in recent years combined with the changing environmental conditions in which an organization is present gave rise to the possibility of a lot of different organizational compositions and interactions within them [78]. The degree of complexity of the environment in which the organization is present, determines the capabilities in terms of organizational structure and agent behavior needed. This complexity and the changing dynamics of the environment often creates challenges for the achievement of the goals of the organization. A balance with the environment should be found in order to satisfy the organizational goals.

4.4.1 A framework for conceptual modelling

The environmental characteristic are therefore taken into account in order to efficiently construct the organizational structure with all its relationships. The environmental characteristics in this case mean external factors not related to the structure or relationships within the structure of the organization. The main environmental characteristic are later also modeled, although not being part of the airport security system itself. The attacker, the threat object and the way of working of the attacker to try to propagate through the system or organization play the most important role, which means that the organizational structure should be constructed depending on this security risk scenario. Here environmental characteristics mean all the external influences on the organization, while in the model it means all the external influences on the security risk scenario. Constructing the organization depending on external characteristics is called the contingency theory [79]. Although this theory is very useful to show the principles that form the basis for the organizational structure and the dynamics, though these principles are formulated in a very abstract way. In order to get a good performance within the organizational structure these principles should be translated to specific organizational settings. Furthermore, a lot of techniques for the analysis of the performance of the organizational structure are informal, which raises questions about the feasibility of the results [9]. For more useful results about the performance of the organization, and thus the identification of weaknesses and prediction of consequences of external characteristics, the analysis should be performed using a formal model of the organizational structure. Such a formal model forms a basis for the processes within the organizational structure and could be used to lay the framework for inter-organization cooperation.

Constructing a formal model is actually the model formulation phase within the modeling process and forms the basis of the implementation. This does not only hold for the construction of a model by means of the organizational view, but for all views needed to program the entire model and use this model in the implementation phase. The conclusion drawn in Section 2.5, that the use of an agent-based method is an interesting and good way to tackle the thesis problem, thus induces the use of an agent-based approach also in the formulation phase of the model.

Interactions among the agents present in a certain environment happen in a framework that is similar as an organizational structure. Such an organizational structure may be formed on purpose with the intention to implement behavioral rules for certain or all agents. For instance these rules are based on norms, policies or organizational culture. Overall, the organizational structure coordinates the execution of actions in an agent-based model or system. When working with agent-based models the organizational paradigm helps to improve computational properties of algorithms [80] [81].

A lot of agent-based models only consider the model from the agent point of view. This agent paradigm has three levels of representation to describe, investigate and predict the processes within the organization [9]. The first level is the macro level, which focuses on the organization as one and the interactions with the environment. The second level is the meso level, which takes into account relationships between individual agents and certain groups within the organization itself. The third level is the micro level, which focuses on just one individual within the organization. The agent paradigm does not incorporate organizational aspects or only the ones that are related to the research problem. Although the security risk scenario already imposes certain organizational aspects and rules out others which could be useful in other situation it is the case to try to establish the relationships through the three representation levels as thorough as possible. This enables a more thorough evaluation of the performance of the organization.

Roles are used to define an organizational structure. All activities that need to be performed or all capabilities that need to be possessed by an operator are defined in this role. There is no limit to the amount of operators that perform a single role or vice versa [78]. The approach to construct the organizational structure can differ on the basis of the presence and involvement of these agents. One approach is that the organizational structure can be constructed without having specific agents in mind already, the defined roles are filled later with the required agents. The other approach already has specific agents in mind who will execute the defined roles. In some occasions the known agents can even influence the construction of the organizational structure.

The operation of all the processes and activities runs against the background of the organizational structure. This organizational structure is defined in the organizational view. Although processes can be identified from the organizational view when analyzing more thoroughly as roles are linked to actions and processes, it is more efficient when it is shown in a separate view. The process view shows not only all the actions and processes it also shows the relationships between them and the order in which they need to be performed [77]. The actions and processes need to be from a similar nature, at the same type level. The advantage of modeling the airport security system over the entire airport organization is the fact that the actions and processes can be categorized to the same type level. All actions and processes are related on the basis of security tasks and have a similar hierarchy although may be performed throughout the airport environment in different departments at different times [82].

The process view is a graphical model of what the actual system looks like. Three main goals can be identified of making this process model, respectively descriptive, prescriptive and explanatory [83]. From a descriptive point of view the model shows what actually happens during a certain timeline in the airport security system. After analyzing the performance of the system one can look at the process model to identify improvements and their locations in the processes of the system. Closely related to the descriptive point of view is the prescriptive point of view, which defines the desired processes and how they should be performed. There can be a difference between the actual execution and the desired execution of tasks and processes. In order to minimize this difference organizations establish rules, guidelines, norms, behavioral protocols, etc. The improvements found after analyzing the performance of the system commonly influence these boundaries for roles in the organizational structure, however it can be the case that certain actions or processes should be adapted entirely. The explanatory point of view is used to provide interpretation about the rationale of the actions and processes and to set up the relationships between the actions, processes and requirements for the system to achieve. Furthermore, points in the system are identified from which data can be extracted in order to analyze the performance of the system.

There are many different ways to construct the process model for an organization [83] [84]. The right way depends on how the organizational structure is defined and what exactly is expected from the process model. The process model for the airport security system should consist all the activities and processes executed by the agents within the organization in order to mimic a real dynamic operation of a security system. The main part of the process model thus is to show the related set of actions performed such that the organization meets its goals. This type of process model is called an activity-oriented process model. The process view can be shown in various degrees of abstraction.

Following the terminology of organization theory this research focuses mainly on the micro and meso specifications of the airport security system. Although interaction on a macro level, which is between the airport security system and the environment in which it performs its tasks, is modeled in this research as well, still an analysis of these macro level processes is out of scope of this thesis as it would mean the analysis of the performance of the entire organization relative to the environment and the connection with other similar organizations. While the performance indicators used to analyze the performance of the airport security system are based on individual parts of the airport security system and the relations between this part and the rest of the airport security system.

Regarding the framework, different paths through the four views can be adopted, however some general relationships are formulated [9]. This way the interdependencies between all the views is really highlighted and the positive aspects of their interdependencies are used. When an informally defined goal of the organization is transformed into a formal representation or a new main goal is identified this is reflected on the performance indicator structure as well as new performance indicators should be set or old ones should be improved [85]. Improving the goals of the organization not only influences the performance view itself but also affects the process oriented view by identifying new tasks or change existing tasks to meet the improves goal hierarchy. When a task description is changed, the workflow is different, which means that a new process oriented model needs to be defined. When processes are changed this can lead to a different way of collecting data such that new performance indicators need to be set. A new performance indicator can induce a new goal for the system as well. The organizational structure and its roles is defined by means of the currently identified tasks and processes. So a change in tasks may need a change in organizational structure which may lead again to a different type of agent needed to fulfill the role as new skills are required. Figure 4.4 shows the main interdependencies between the four views during the design process. When constructing the views for the airport security system it is useful to understand the interdependencies of the four views. Even though for the analysis of the two different airport security systems no substantial changes will be made to one of the views that will trigger changes along the interdependencies described.

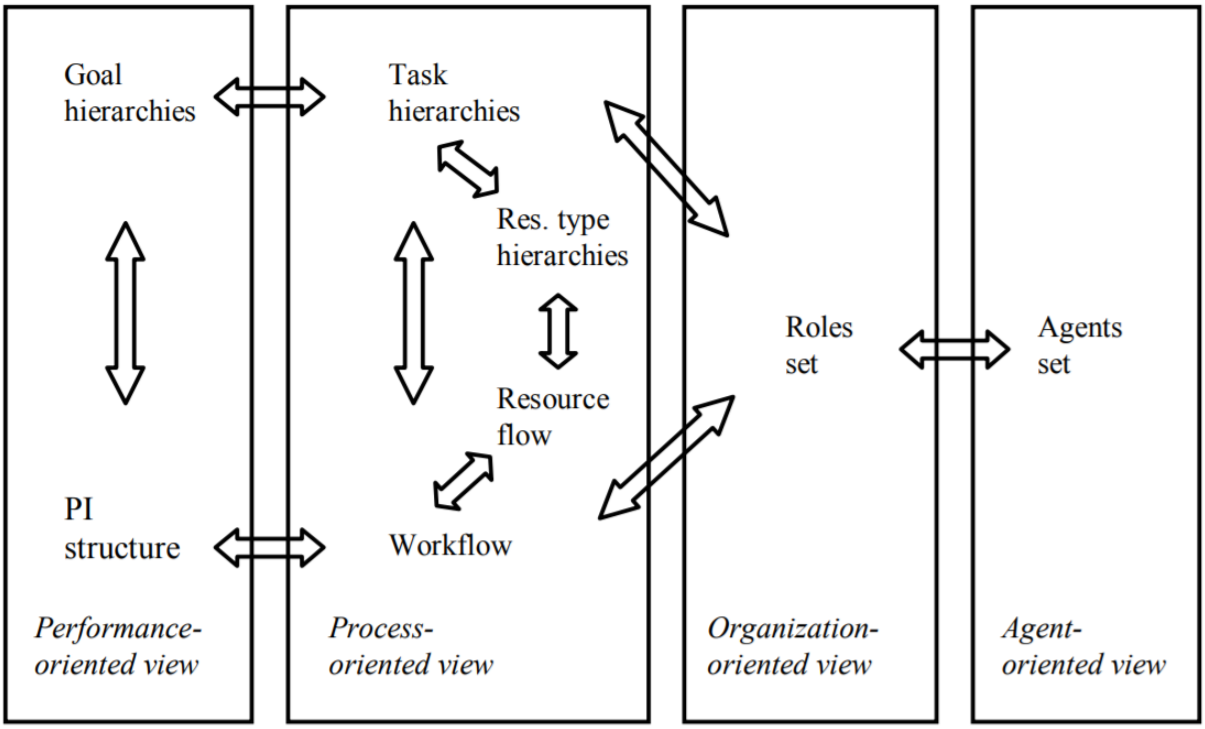

Figure 4.4: Relationships between the performance, process, organizational and agent oriented view [9]

In the security risk scenario the environment in which the airport security system needs to operate is somewhat fixed to a large extend. The main environmental characteristics are modeled as inputs as well in order to analyze the performance of the airport security system as efficiently as possible. Other than the main environmental characteristics there are more environmental characteristic still present that could influence the airport security system, and these could be changing over time. This changing environment should induce a more flexible organizational structure such that the airport security system is ready for every situation possible in the environment [85]. In a sense the airport security system should be adaptive to account for these changes, and the more integrated security system designed later would have this more flexible approach. Although security related situations should be handled as efficiently as possible in order to identify the threat as early and completely as possible as well. This on the other hand induces a more well-defined hierarchal structure for the agents. With the security risk scenario fixed already the more well-defined hierarchical structure suits the airport security system best such that the key performance indicators really show the performance relative to this security risk scenario.

The following sections put the aforementioned framework for conceptual modelling in practice. In the next section, Section 4.4.2, the organization-oriented and process-oriented view of the current airport security system are determined. Section 4.4.3 first shows the approach to integrate the airport security system, where after in Section 4.4.4 a similar approach is adopted to design the organization-oriented and process-oriented view for the newly proposed integrated airport security system. Lastly, Sections 4.4.5 and 4.4.6 respectively show the components of the agent-oriented view for both the current airport security system and newly proposed integrated airport security system and the performance-oriented view for both the current airport security system and newly proposed integrated airport security system.

4.4.2 Establishing the organization-oriented and process-oriented views of the current airport security system

The airport security system is a complex socio-technical system with many individual components. The organizational and process oriented view illustrate respectively the structure and the tasks of the airport security system [8]. With respect to the organizational structure, interaction levels can be shown at various degrees of aggregation. The higher the level of aggregation the more detailed the organizational structure is illustrated. It is important to know the roles of the airport security system in its most detailed configuration in order to analyze the performance. The airport security system is in itself already a more detailed aggregation level of the entire airport organization. Therefore only three aggregation levels are established. The organizational oriented view of the current airport security system can be seen in Figure 4.5 to 4.7. The names of the roles are presented in the blocks, while the links between the blocks represent the interaction between two roles. All roles of the airport security system are present and thus affected by the airport terminal environment. This environment is only shown in the first aggregation level for convenience, but is present at all aggregation levels. Additionally to the organizational oriented view the roles present in the airport security system need to perform certain tasks. The process oriented view shows the most important tasks to achieve the organizational goals and is described after the presentation of the organizational oriented views.

The first and second aggregation level, respectively Figure 4.5 and Fig 4.6, show the less detailed generic roles. First, two generic roles can be identified that interact with each other such that the overall airport security system is constructed. These main roles are the airport/airline services provider and the airport terminal security services provider. The difference between these two roles is that the airport/airline service provider consists of roles providing a service to the passengers not directly related to security however the information obtained can be used for security purposes, while the security services provider fulfills tasks in the security domain. Second, the view goes a bit more in depth in the two generic roles. Here the different types of services can be identified. The airport/airline services provider consist of a check-in service provider and a gate access service provider. The airport terminal security service provider consists of more roles, namely the security check provider, the baggage security service provider, the customs service provider and the airport terminal environment security provider. These generic roles in the second aggregation level can be seen as the checkpoints present in the airport environment through which passenger move from arrival to aircraft. These checkpoint all have their own unique type of actions that need to be executed.

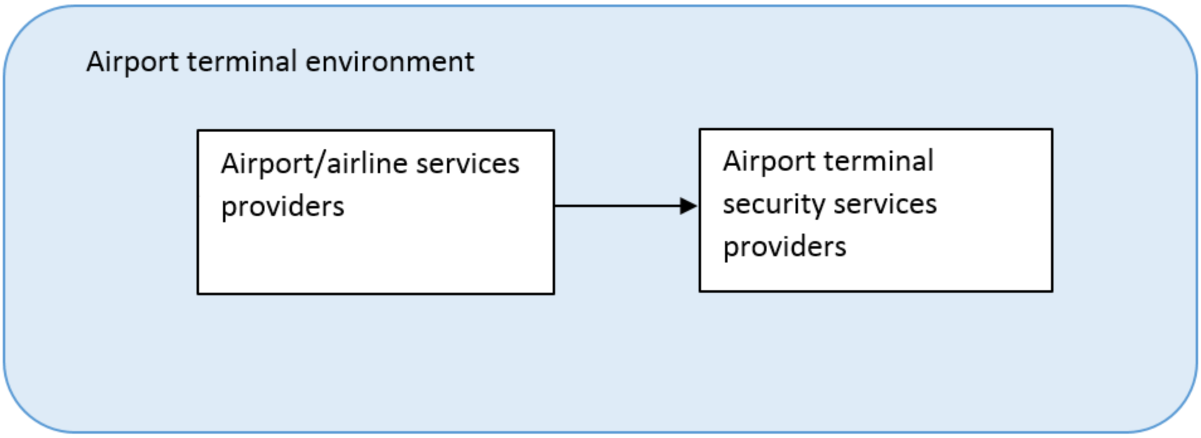
Airport terminal environment
Airport/airline services providers
Airport terminal security services providers

Figure 4.5: First aggregation level of the organizational view of the current airport security system

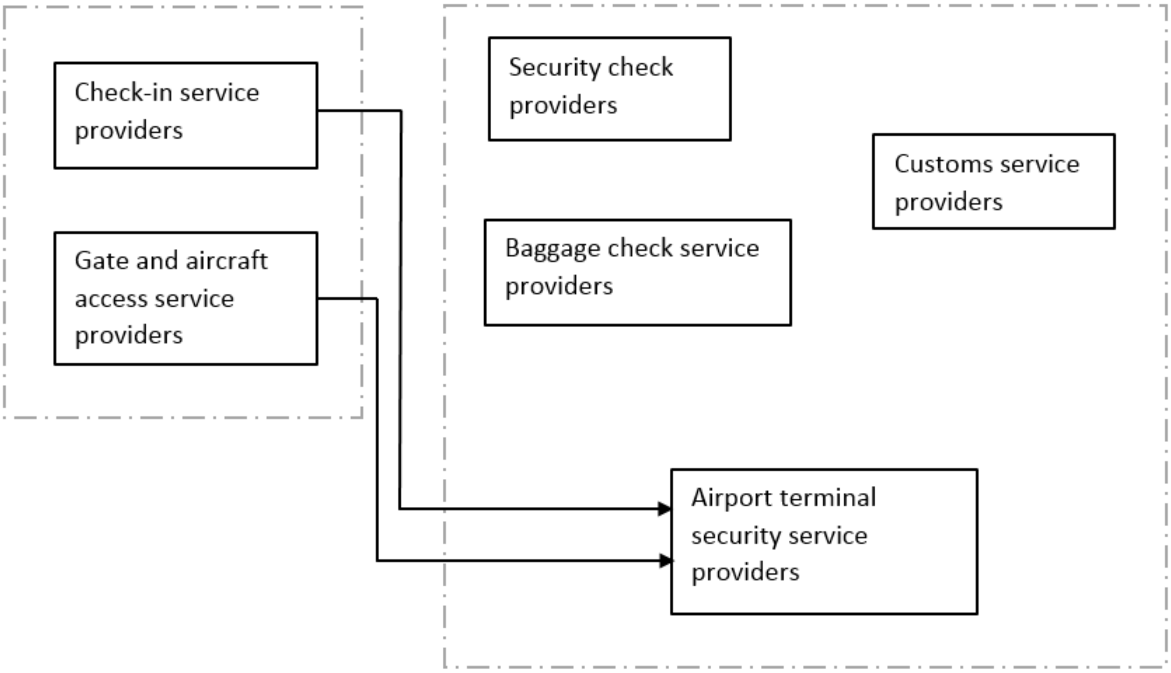
Check-in service providers
Gate and aircraft access service providers
Security check providers
Customs service providers
Baggage check service providers
Airport terminal security service providers

Figure 4.6: Second aggregation level of the organizational view of the current airport security system

The third aggregation level, Figure 4.7, shows the airport security system in its most detailed level. The generic roles illustrated in the second aggregation level consist of roles which can actually perform tasks by themselves. This level is the most important, as the detailed roles are used to be implemented in the model as individual agents. The process oriented view and this third aggregation level of the airport security system are closely related to each other and should be considered together as the tasks need to be executed by certain roles.

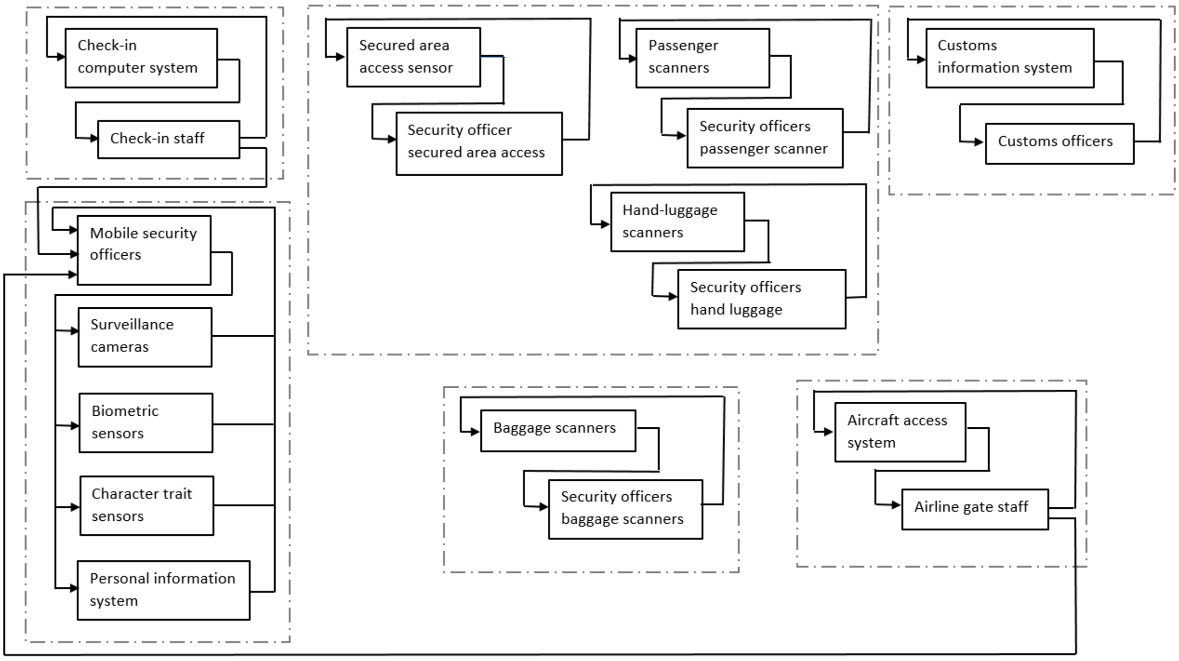

Figure 4.7: Third aggregation level of the organizational view of the current airport security system

The most detailed organizational view shows the socio-technical nature of the airport security system. All checkpoints and the airport terminal environment security providers make use of a mix of human operators and technical systems like cameras, sensors and scanners. The most striking of the organizational view is the lack of links between different checkpoints. This is the main characteristic of the current airport security system. The agents executing tasks operate in an isolated stand-alone mode. Only within a specific checkpoint there is interaction between the agents. Mainly, because human operators need to work directly with technical systems, as can be seen by the links. The technical systems mostly perform the actual scanning and checking, while the human operators make observations and analyze the data from these technical systems and form decisions.

The organizational roles within the general role of airport terminal security service providers which address a sensor can be present throughout the entire airport terminal environment and are mostly located at multiple checkpoints in order to maximize their operational contribution. Furthermore, all human operators and certain sensors and the surveillance cameras have the ability to observe behavior or motion of passengers. This is a separate type of activity, therefore this task is shown separate and not as next step in the flow of tasks for the overall airport security system process through the checkpoints.

There are many processes and actions that need to be performed by the individual roles of the airport security system. These actions can be described in a very detailed level on a step to step basis. For the airport security system it would be interesting and necessary to know all these steps on the most detailed level. However in order to model the performance of the airport security system a more general view of the to be performed actions can be used.
Processes can be mainly divided into the unique processes of each checkpoint, respectively check-in, security check, baggage check, customs, gate services and the terminal areas. Check-in processes consist of the identification of the passenger, checking-in the passenger and the baggage and providing a valid ticket. The security check processes comprise of checking a validity of access to the secured area, putting the hand-luggage to the hand-luggage scanner, scanning of the hand-luggage, analyzing the results of the hand-luggage scan, putting the passenger to the passenger scanner, scanning of the passenger and analyzing the results of the passenger scan. Similar processes can be identified at the baggage scan where the baggage needs to be put to the baggage scanner, to be scanned by the baggage scanner and results of the baggage scan needs to be analyzed. At customs the main action only consist of the checking of the personal information of the passenger. While at for the gate service providers the actions relative to security are the checking of a valid personal identification and ticket. The roles present in the airport terminal environment, and thus without a fixed checkpoint, all have their unique observation or checking action to be performed. Hereafter the security officers analyze the output.

Furthermore, all human operators need to have communication with the passengers in order to guide them efficiently through all the processes. When an alarm is observed a security officer either needs to arrest the passenger or needs to perform a second opinion and when no alarm is observed the passenger needs to be cleared for the checkpoint.

4.4.3 Data fusion for integration of the airport security system's components

The second setup, introduced in this section, of the airport security system takes a more integrated perspective of the agents present in the organizational structure. Nowadays there is still a possibility that a threat source and object circumvents all the security measures at an airport and achieves its goal by bringing the threat object to the airside environment. However, the various agents, resources, security systems and technologies present in these systems used at the moment at the airports could be utilized in a more efficient way by connecting them such that significantly more information could be extracted regarding these possible threat sources and objects [5]. The rapid and universal distribution of security systems among commercial airports as threats nowadays increase in these environments resulted in minimal coordination and communication compatibilities among these different security systems, also because there are many different manufacturers. The security systems often work in a stand-alone setting and only the security officer working directly with the equipment has a type of manual communication with the specific equipment. Not only the possibility of a threat source and object slipping through is present but also an undesirable high rate of false positives and slow throughput is induced by the current way of working of the airport security system. A more effective way of operating the airport security system could be achieved in a real time way of working with each agent operating in a stand-alone setting like in the current configuration although all agents are integrated to communicate with each other and thus decide when and how to perform their task more efficiently. The agents are integrated by means of data fusion [5].

The current widespread presence of these stand-alone equipment and security systems make the airports more vulnerable to all kinds of possible threat scenarios than in the case of using a more integrated airport security system. The stand-alone systems make the airport security system a single point of failure. If a threat source successfully circumvents a single security check, this threat source and its threat object are permitted to continue to secure parts of the airport environment. The presence of a threat source and threat object in this part of the airport environment is highly undesirable. Improving the identification of all possible threat scenarios requests combining data from multiple security systems across the entire airport environment on the basis of a framework which uses this data as input to estimate the threat level of a specific situation present in the airport environment [86]. Data fusion means that the data from multiple sources of security systems is combined into a single output which can be exploited to make more informed decisions about how to deal with specific situation. The airport security system is a complex socio-technical system. When implementing data fusion the socio-technical nature of the system is actually a benefit. Human agents and automated systems differ in their way of working and therefore in their qualities. Human agents are better at identifying difficult to prescribe but very noticeable situations, while automated systems are better at identifying easy to prescribe and recurring events. Using both the human and the technical inputs for data fusion combines their complementary qualities and thus would provide a greater potential for identifying threat sources and objects.

In order to fully employ data fusion several steps need to be performed before the actual fusion is achieved. Data sharing and data integration are actions to be fulfilled as well [5]. Data sharing is the exchange of data among all security systems and agents within the airport security system and among other security organizations. Data integration is the transformation of data outputs from all security systems and agents into a single common data format such that all agents understand and can process the used data when it is shared.
Combining all the stand-alone agents of the airport security system using data fusion thus could lead to a more informed decision to identify a possible threat source and object. Furthermore another advantage of data fusion is that it enables an adaptive approach to airport security. The detection threshold for a possible threat source and object could be dynamically changed on an individual basis for every passenger propagating through the airport environment [87].

The data fusion system overall used to integrate a certain system, in this case the airport security system, may have to deal with enormous amounts of information. This information is obtained from the independent data sources, where after the data is processed and then communicated to all other resources that need the data, all as quick but thorough as possible. Situations within an environment can change very abruptly, so the quicker data is available the better in order for the airport security system to make effective decisions. The best way to deal with this is to perform the data fusion in real time across many interfaces. Figure 4.8 gives a brief abstract schematic overview of the procedure and impact of a data fusion system. Combining multiple parts of the entire airport security system could improve the ambiguity existing at this time in many situations and thus identify the threat source and object before it can successfully propagate through the entire airport environment.

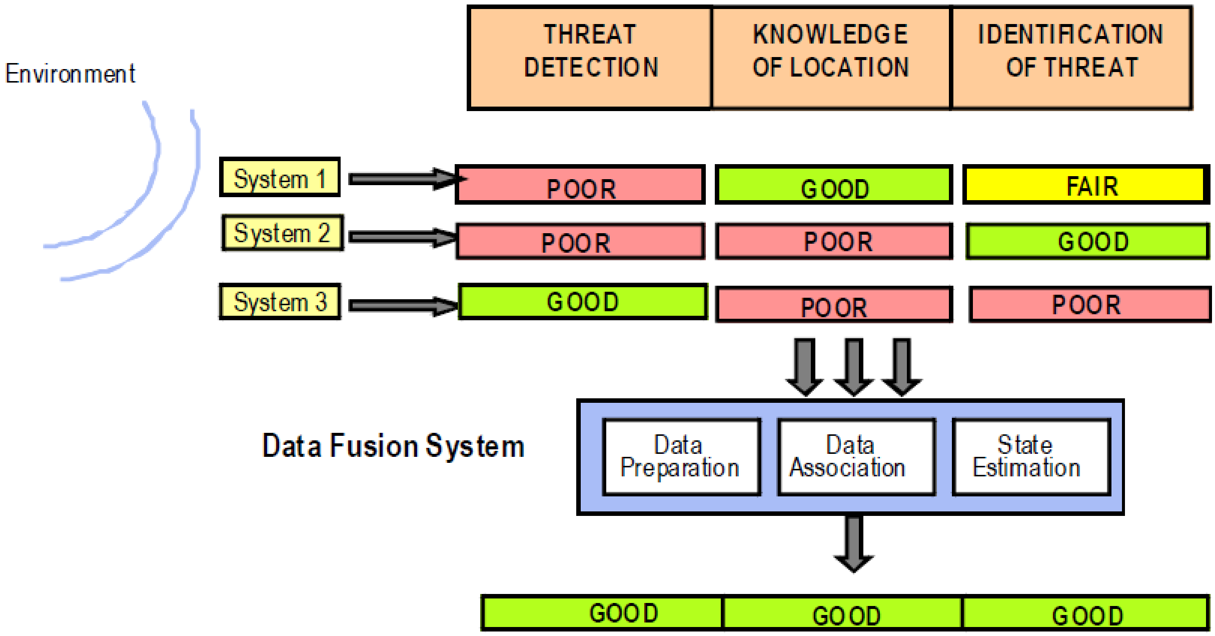

Figure 4.8: Impact of data fusion with respect to individual security system's performance [5]

As can be seen from Figure 4.8, the data fusion approach consists of three main parts, respectively data preparation, data association and the estimation of the specific state [5] [88]. Data preparation is the execution of transforming the obtained data into a form that will allow the fusion of this data. The second step involves data association which is the combining of the data with a similar property or subject from different individual security systems. In this research the connecting property among the data is the passenger. All data from a single passenger is linked with each other. The final step in data fusion is the actual estimation of the threat level. Once the data is prepared and associated it can be applied in an estimation of a current state of a certain passenger. The state of a passenger shows the level of risk this passenger has upon the airport environment and thus whether or not the passenger should be identified as an attacker.

In the security risk scenario the goal of the airport security system is thus to identify whether or not the passenger is a threat source carrying threat objects. The estimation depends on parametric characteristics of the resources used during the data fusion. There are different ways to calculate the estimate of a threat level of a certain situation. The difference between the methods can be categorized in decision data fusion and parametric data fusion. The easier of the two categories is achieved by using the decisions of the individual security systems as input data for the data fusion system. All steps before the actual estimation of the threat level, thus involving data preparation and data association, will be performed with the decisions made by the individual security systems based on their measurement data. These individual decisions will be combined in the data association step into an overall decision for the airport security system. Decision data fusion can be executed by using AND or OR logic to combine the decision output of the individual security systems. The difference between AND or OR logic is that for AND logic all security systems used in the data fusion need to have a positive identification of the threat source and by using OR logic only one of the individual security systems has to give a positive identification. Parametric data fusion takes another approach than decision data fusion. Each individual security system has an observation measurement, called a response. The decision is based on this response. Parametric data fusion uses the response before the decision by the individual security system is made and combines these measurement responses from all security systems present in the overall security system. Figure 4.9 to 4.12 show the operational process of a security system without data fusion, with decision data fusion using AND logic, with decision data fusion using OR logic and with parametric data fusion respectively. Although the data from security resources nowadays is not being used for data fusion the current airport security system operation looks similar as the system using OR logic as in the current airport security system there are multiple security systems following each other up to check the passenger and his baggage and all these systems can raise an alarm for the identification of a threat source and object.

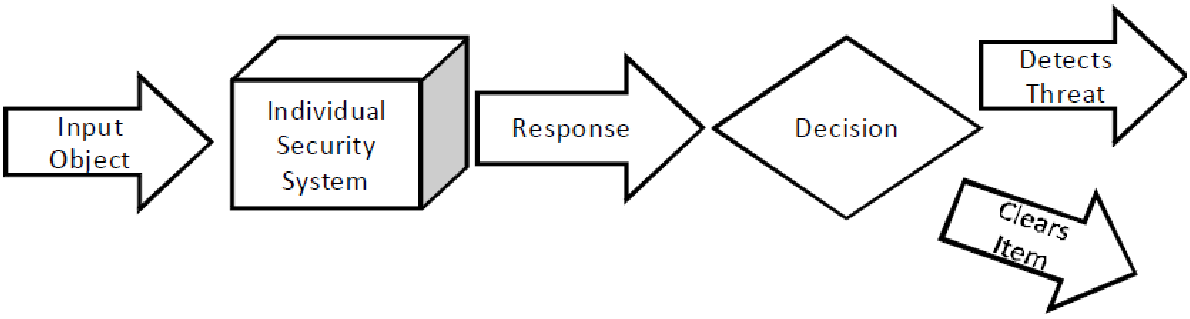

Figure 4.9: Process of a system without data fusion [5]

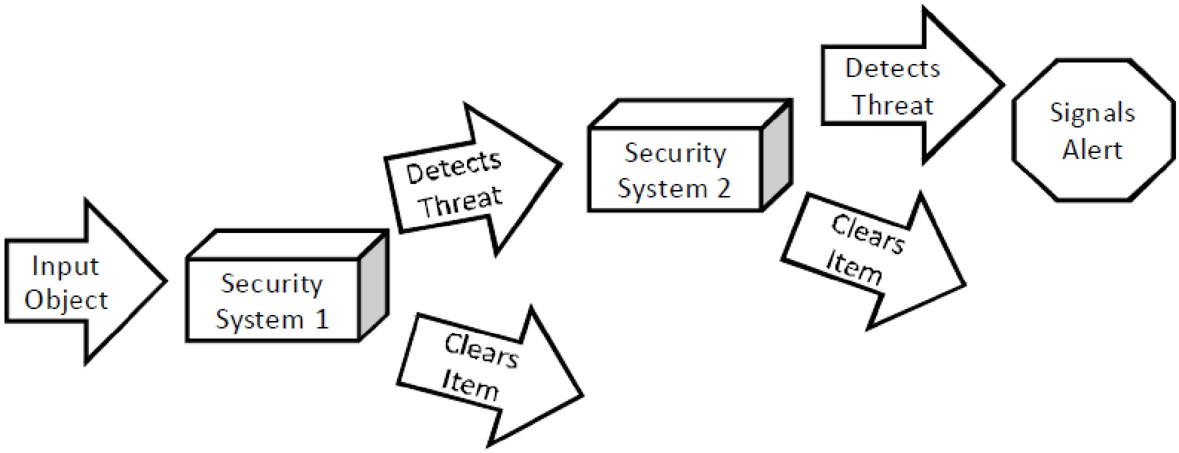

Figure 4.10: Process of a system using decision data fusion with AND logic [5]

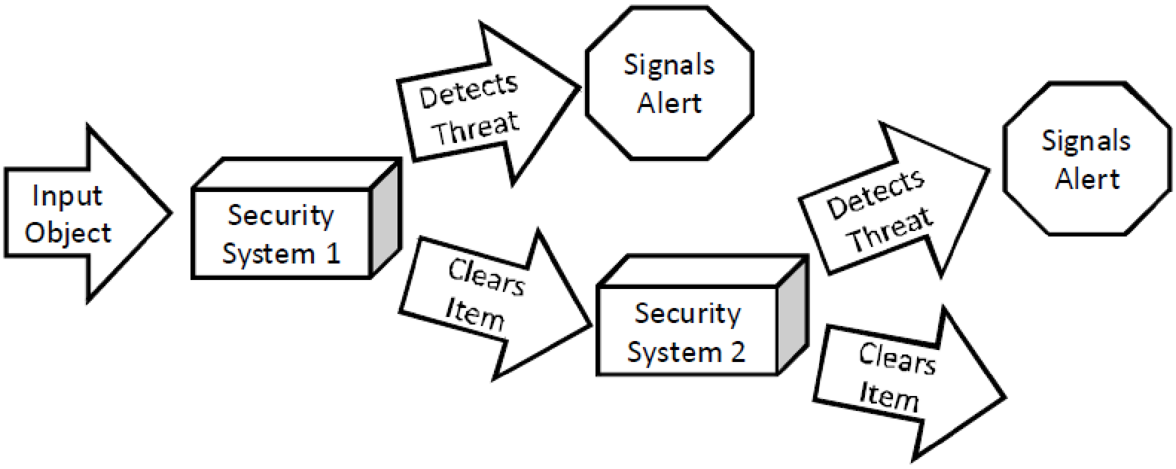

Figure 4.11: Process of a system with decision data fusion using OR logic [5]

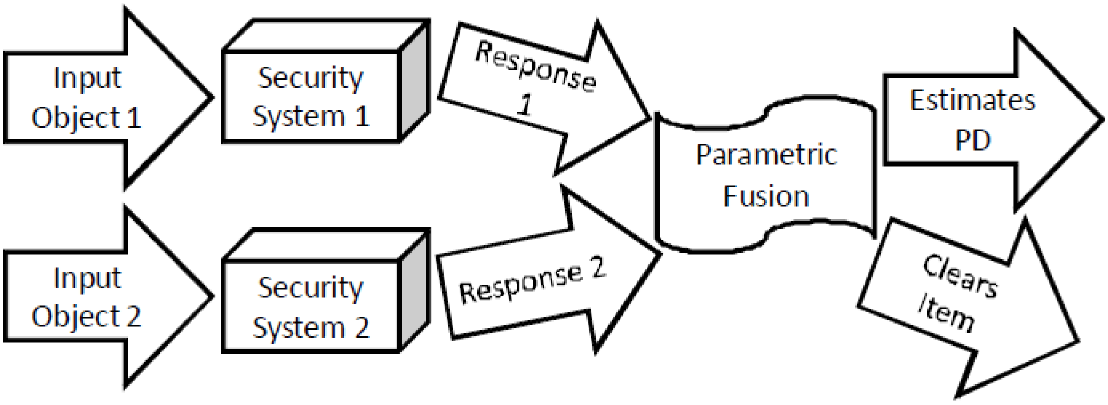

Figure 4.12: Process of a system with parametric data fusion [5]

Data fusion in general can improve the performance of the overall airport security system with respect to individually operating security systems. The intensity of the improvement of performance differs with the type of data fusion approach used during the implementation. Analyzing all different types of data fusion is out of scope of the thesis. This means that only specific configurations of the above described types will be implemented. Therefore it is important to not only know the differences of the operational aspect, but also the differences of expected improvement and implementation feasibility.

Decision data fusion with AND or OR logic uses the outputs of individual security systems. The outputs are the detection decisions from the security systems. These detection decisions have a certain probability. The manufacturers of the security systems can implement this probability as a threshold for detection, it is namely a characteristic of the security system used. The threshold induces a sensitivity and specificity for the security system, respectively a probability that a true positive or a false positive will be detected. These two variables are the main operational characteristics of a security system and plotted against each other in a ROC (receiver operating characteristic) curve. As these are the two main characteristics these will be used as key performance indicators in the implementation of the two airport security systems, the exiting stand-alone airport security system and the proposed integrated airport security system.

Both decision data fusion approaches, respectively using AND and OR logic, aim on the improvement of the operational processing and decision making of existing individual security systems. The aim of the approaches is to decrease the detection rate of false positives while maintaining or even increasing the detection rate of true positives. Above that using decisions rather than other data is an easy to implement approach and the process time for the data fusion system is quick. Looking at test results in literature [5] it can be seen that using AND logic has more than only implementation advantages, also the performance results relative to the false positives and true positives detection seems to increase with a well amount. The approach using OR logic shows something different. Decision data fusion with OR logic can on the one hand decrease the false positive detection rate in some situations, but this can come at a cost of increasing missed detections relative to individual security system results. And the other way around, if all true positives want to be found there are many false positives as well.

On the other hand parametric data fusion aims at constructing better operational characteristics of the overall security system. The approach only uses the operational characteristics of individual security systems in order to design one new overall security system with improved operational processing and decision making. This could result in a better rate of identification of true positives and false positives as well, just like both the decision data fusion approaches. Again following test results in literature [5] it can be seen that parametric data fusion has better performance results relative to decision data fusion, on significant regions of the ROC curve [89] but not in every situation though.

Apparently the use of responses rather than decisions induces less erroneous data to be fused and thus more effective outputs to base the overall detection decision on. The downside of parametric data fusion is the huge amount of processing of data which is needed in order to firstly get the right reference frame for all data and secondly to derive an useful overall security system response. This will induce extensive software use in the data fusion system which leads to more maintenance and life-cycle costs.

The test results used to accompany the vision on decision and parametric data fusion is only a simple example of using data fusion in a security system. The results form a valid basis for the notion of the performance of all the different types of data fusion, however in more complex environments such as an entire airport security system the results could differ. The different approaches of data fusion have their own goals and qualities as explained before. This can lead to different optimal configurations in different scenarios. The outputs, respectively the response and the decision, need to be thoroughly analyzed before selecting a better approach. However the analysis of the outputs is out of scope of this thesis. Security nowadays is a very strict and many operational characteristics are needed to perform this analysis, especially when working with parametric data fusion. Based on the improved performance of decision fusion with AND logic and the notion that in more complex cases OR logic can increase the performance as well, even outperform AND logic, the decision data fusion is used in the new design integrated airport security system. Also feasibility is taken into account as at the moment decisions data fusion could be more easily implemented in real life then parametric data fusion which needs a new designed interface and more extensive processing. Furthermore, parametric data fusion can only be performed when individual security systems operate in a short time period from each other as all responses need to be incorporated in the data fusion system before an overall decision can be made about the object, while decision data fusion uses decisions of individual security systems, which means that a risk profile can already be set up for this particular object. Both AND and OR logic will be used in the implementation of the new designed airport security system. Different configuration used for the integrated form of the airport security system will be analyzed on their performance.

4.4.4 Establishing the organization-oriented and process-oriented views of the newly proposed integrated airport security system

Similar as for the current airport security system conceptual model, an organizational view and a process view can be constructed for the new designed airport security system integrated by the use of data fusion. Due to the use of a data fusion system to integrate the airport security system the organizational and process view will change and needs to be designed from scratch as it is not used at present airports. The change on the organizational structure and the tasks that need to be executed induced by the use of a data fusion system will be explained using the organizational oriented view, Figure 4.13 to 5.15 and the process oriented view of the integrated airport security system. More important for the implementation of the integrated airport security system is the way of working that can be derived from these views. The airport terminal environment in which all agents operate is for convenience again only showed in the first aggregation level, although it is present in all levels.

The organizational view can be divided into three aggregation levels again. The first aggregation level, Figure 4.13, shows three generic roles where there were only two in the current airport security system. However, because the first aggregation level cannot show that much detail, the way of working of the integrated airport security system cannot be read from this aggregation level yet. The new block that is introduced is a very important newcomer in the organizational structure though. It hosts the data fusion system that will integrate the data from the individual systems into a fused data output that could be more efficient and increase the performance of the goals of the airport security system. The second aggregation level, Figure 4.14, shows the same checkpoints in the airport terminal environment as roles as the current airport security system. Furthermore, the data fusion block is drawn in a more detailed level, showing the data preparation, data association, data estimation and data fusion interface systems. The more detailed representation of the overall data fusion system shows the individual systems for the separate activities that needs to be performed by the data fusion system. It can already be seen that there are more links present in the view compared to the current airport security system, which means that there is more interaction between the identified roles. The black links in the second aggregation level represent the more important and dominant relationship to the data fusion system, while the blue links represent the data communication between individual security systems, mostly used when the data fusion system is not operational.

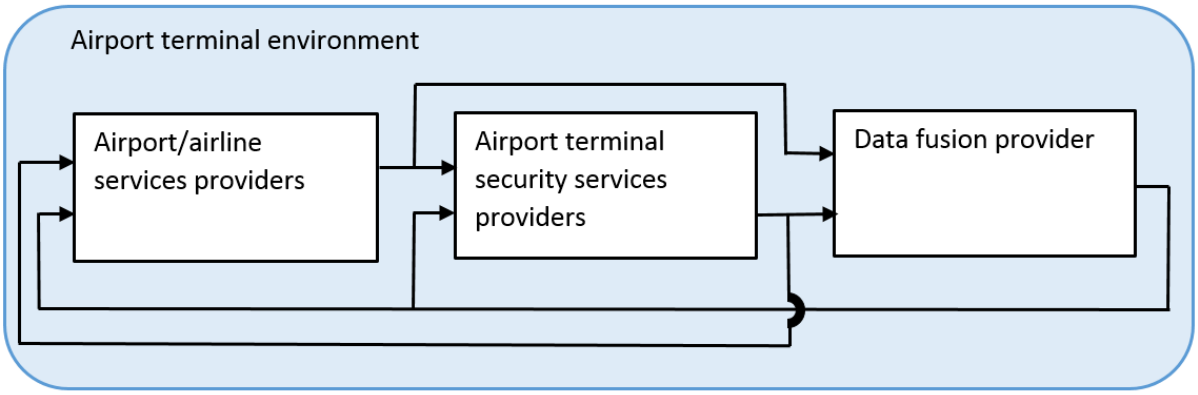
Airport terminal environment
Airport/airline services providers
Airport terminal security services providers
Data fusion provider

Figure 4.13: First aggregation level of the organizational view of the integrated airport security system

The third aggregation level, Figure 4.15, shows again the airport security system in the most detailed form needed to implement this integrated airport security system into the programming software. The actual agents present in the integrated airport security system are the same as in the current airport security system. The only additional agents, and the most important agents as these induce the integration of the entire system, are the data fusion system agents. However the data fusion system agents already had their most detailed configuration in the second aggregation level in Figure 4.14. Therefore, now only one block is presented. This has a different color to show that it has a different aggregation level as the other blocks. Furthermore only big arrows are illustrated in this figure. This is done due to convenience as otherwise too many links needed to be shown, which would have made the figure unreadable. The big orange links show are drawn from the outer lines, the dashed rectangles, of the detailed block which represent the higher aggregation level of the detailed roles. All detailed roles have individual communication with the data fusion system about their obtained data about passengers. This communication goes back and forth. First the raw data obtained by the individual roles is communicated to the data fusion system, and after processing this data the new integrated data is sent back.

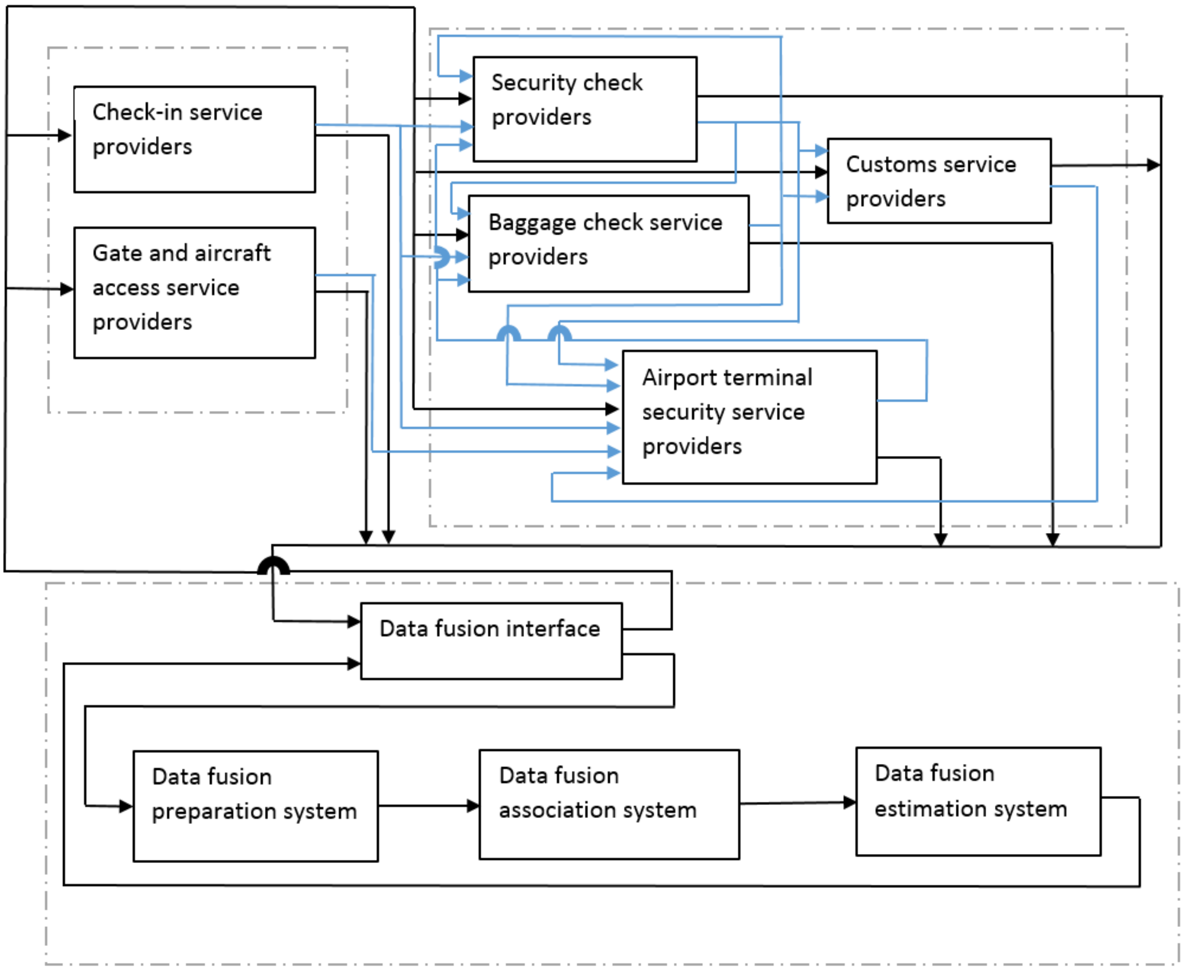
Check-in service providers
Gate and aircraft access service providers
Security check providers
Customs service providers
Baggage check service providers
Airport terminal security service providers
Data fusion interface
Data fusion preparation system
Data fusion association system
Data fusion estimation system

Figure 4.14: Second aggregation level of the organizational view of the integrated airport security system

The blue links indicate again communication between the individual roles of the current airport security system rather than with the data fusion system. More communication between the technical systems in the airport security system is established. The advantage of integrating the entire airport security system means that there is not only hierarchical integration. Hierarchical integration means that there is one major system communicating with the individual systems. Not only the data fusion system has the risk profile it builds about the passengers. A copy of a simple version of the risk profile and the updates that the individual systems make on these are stored and communicated by these individual systems to others, such that the airport security system stays integrated when the data fusion system has troubles functioning. These links are shown as well from the outer lines of the separate higher level aggregation levels as a new system should structure this individual communication. However, in this research it is assumed that the data fusion system works in the most optimal way and thus the lower level communication does not have to be modeled as extensively.

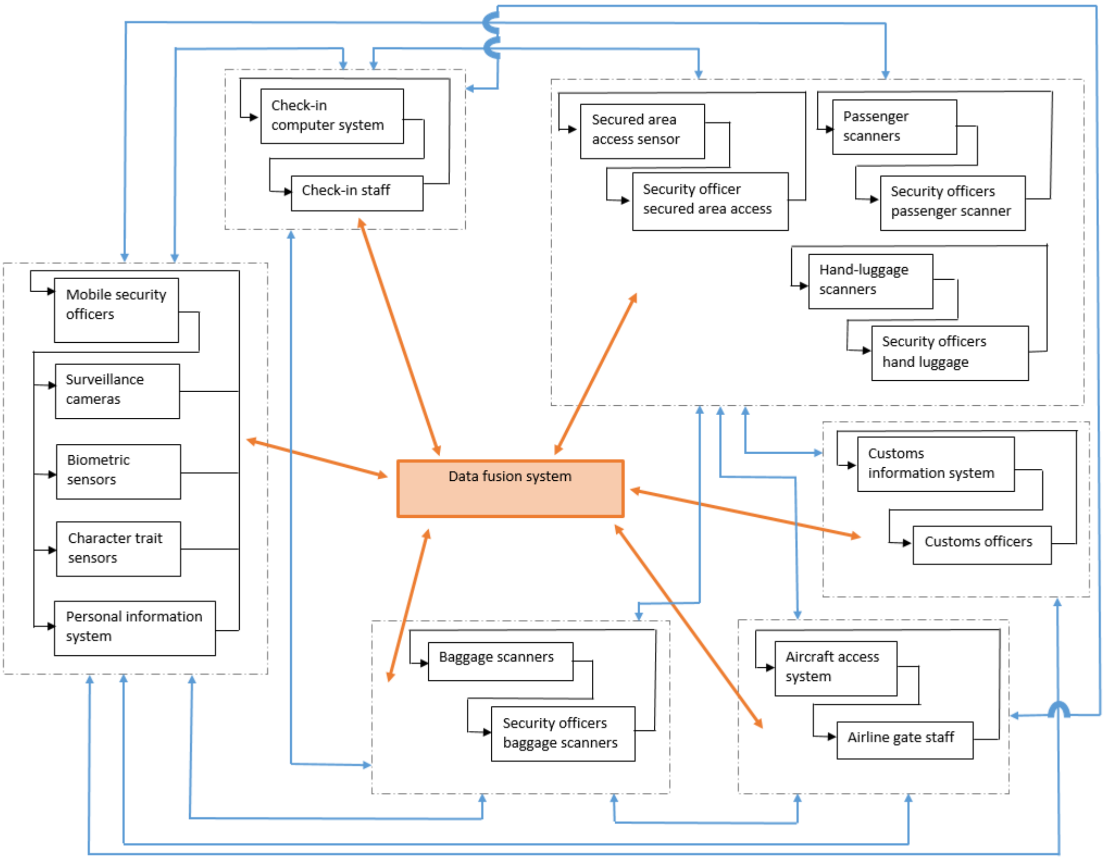

Figure 4.15: Third aggregation level of the organizational view of the integrated airport security system

Closely related to the third aggregation level of the organizational oriented view the process oriented view of the integrated airport security is constructed. This process oriented view is quite similar as for the current airport security system. Actually nothing changes for the individual security systems which just need to perform the basic actions specific to the checkpoint where the individual security systems are located. The difference is the incorporation of the tasks from the data fusion system. This seems rather little difference, however the fact is that the tasks of the data fusion system need to be executed for every passenger after every new observation of an individual security system. This means that the data fusion system needs to analyze a huge amount of data.

In order to analyze the difference in performance between the current stand-alone airport security system and the proposed integrated airport security system, various configurations of the integrated security system will be modeled. In total three different integrated configurations, based on data fusion will be used. The first integrated security system will make use of a simple decision data fusion approach using AND and OR logic. Any three individual security systems should raise an alarm in order for the passenger to be identified as an attacker. The second integrated security system will make use of a more advanced weighted decision data fusion scheme. Still three alarms of individual security systems are needed to identify the passenger as an attacker, however one of these alarms should be an alarm of a security system that directly identifies a threat object, namely the passenger scan, hand-luggage scan or baggage scan. The third and last integrated security system will have a more advanced decision data fusion approach, using an adaptive approach of the passenger scan, hand-luggage scan and baggage scan. Every alarm of any other individual security system will increase the risk profile of a passenger and will be fed to the individual security systems that directly identify a threat object. Then the operational characteristics will be adjusted as such for every passenger, based on their risk profile.

4.4.5 Elaborating the components in the agent-oriented view for the current and newly proposed integrated airport security systems

The organizational oriented view and the agent oriented view are closely related to each other. The organizational view describes the structure of the organization within a certain environment by means of roles and relationships between these roles. The agents view fills in these roles with actual agents to perform the tasks that belong to a certain role. The organizational views of the current and integrated airport security system configurations however are quite detailed as it was already known which type of agents had to perform the roles in the airport security system. Therefore it can be said that the organizational oriented view and the agent oriented view are merged into one overall view that shows how the airport security system looks like. With a graphical representation of the structure, agents and relationships, based on the threat scenario, only the boundaries can be constructed when implementing the model into programming software. In order to fully implement the airport security system model into a programming software a modeling ontology needs to be formed.

Agents can describe human operators or artificial systems. This makes it an effective approach to represent a complex socio-technical system like the airport security system. This means as well that there are different types of characteristics that need to be defined. Relationships between agents which exert certain behaviors or actions are the foundation for the rules in the ontology which are the basis for the simulation of the airport security system problem. Below the characteristics which the agents can possess are explained.

The most complex aspect of an agent is that it can reason. There are several steps in the way agents reason that need to be modeled in the ontology as well in order to get the right progression of the simulation. These steps can be described as states of an agent. When an agent gets information and needs to reason about it, the agent will think about what just happened and remember what happened, this is called the memory state [9]. When a next situation emerges in the scenario and the agent needs to act upon that, the agent needs to prepare itself for the to be performed task, this is called the preparation state [9]. Before the memory state and after the preparation state are respectively the input and output states. These states are characteristics all agents described below will have as it is part of the ontology how to describe the reasoning of agents.

Human agents

The airport security system problem consist of multiple types of human operators. These human operator can be derived from the roles of the organizational view. A combination with the threat scenario is needed in order to get the full picture of all the human agents present in the model. From all these types three classes of human operators can be established, respectively the human security agents, the neutral human agents and the human threat agents.

- Security agents

The category of human security agents consist of all human agents who need to perform a role in the security domain. Throughout the airport environment there are human operators working who fulfil this profile, but this means that different types of agents with their individual characteristics as well. These characteristics can be transformed to state properties for the implementation of the model. All properties can be present in a certain range. An example of a property is work experience [90]. The main locations in which the security agents are located are the passenger and baggage checks, the customs control and moving free in the airport environment.

  - Mobile security officers

The security officers moving freely through the airport terminal in either the public or secured area are the first personal line of defense of the airport security system. The task of the security officers is to identify any suspicious behavior of people in the airport environment. Their goal is thus to identify all suspicious situations as result that all threat sources and objects can be found before they propagate through the entire airport environment [2]. This goal can only be achieved by interaction with the passengers, either indirect interaction or direct interaction. This means that the security officers need to have the ability to observe and communicate as leading characteristics, next to the ability to move to several location within the airport environment. Observation is done with respect to movements and behaviors of other agents, while communication is used with other security officers, in case of the integrated airport security system using data fusion as well with the data fusion system or with a passenger when possible suspicious behavior is noticed. Because security officers are human there are some characteristics that influence their performance [17]. These characteristics can be divided in two groups, respectively personal behavioral characteristics or indirect induced by properties of the environment. Personal behavioral characteristics emerge from the security officer himself. Although all security officers are professionals it is rather difficult for a human being to perform one hundred percent. While modeling personal characteristics these do not have to be in such a detail that they really describe what happens in the personal life of a security officer. State properties identified are; the emotional level in which a security officer finds himself, a less stable security officer due to personal reasons is likely to perform less and the professional level which a security officer has, a security officer who works in the domain for many years is likely to execute his task more efficient than a security officer who just starts in the job. State properties of the environment can affect the performance as well, mainly the amount of passengers in the airport environment has a key role. The more crowded the airport terminal, the more difficult for a security officer to spot a specific passenger and thus possible suspicious behavior. Furthermore, states of the security officer define if the security officer is busy or available to identify its task of observing. This means while a security officer is busy communicating with passengers or other agents of the security system it has not time to perform other tasks in his role.

- Security officers at a stationary checkpoint

All other security officers are located at a certain checkpoint within the airport environment, rather than having the possibility to move freely. The goals, and characteristics, of the security officers depend on the location where they are stationed. However, the main states the security officers can possess are similar throughout all checkpoints, the only thing that differs is the object they are checking or the type of communication they have to perform [17].

The checkpoints where security officers are stationed are the passenger and hand luggage check, the baggage check and customs [8]. The different roles that the security officers need to execute are an access officer at the passenger and hand luggage check, security officers that perform the passenger, hand luggage and baggage check and a customs officer. These security officers all mainly have common states they can obtain. All security officers need to observe, communicate either to passengers or other airport security system agents, process tasks relative to their checkpoint and analyze data from other non-human airport security systems. The goals of the access officer, checkpoint officers and customs officer serve the same overall goals but can be formulated differently, respectively identify unlawful access to the secured area of the airport environment, identify threat object during the performed check and identify passengers who do not meet the customs requirements. Furthermore, all these security officers have the ability to observe suspicious behavior and communicate to the passengers as well. The only boundary condition is that when security officers are busy executing one of their tasks they are not available to execute other tasks at the same time [91].

Similarly to the freely moving security officer the personal characteristics and environmental properties can introduce deficiencies in the performance of the security officers. Level of expertise of performing the actions, circumstances in the personal life and workload relative to the amount of passengers present at the checkpoint and the amount of time a security officer already works are all state properties that are modeled in order to simulate the conditions of a security officer as efficient as possible.

- Non security or threat agents

This category consists of all agents present in the airport environment, but do not have anything to do with the airport security problem rather than being in the airport environment and performing their tasks. Although these agents have no direct role in the security domain it is important that these agents are present as well. Among this type of agents are namely the airport or airline personnel who need to perform tasks with respect to passenger and passengers themselves who are no threat source or do not carry a threat object. The personnel agents have an important role in the overall airport process and can contribute to the airport security system with information. While the neutral passengers are present to mimic a normal day at the airport and check the performance of the airport security system.

  - Airport and airline personnel

There are more processes that need to be performed within the airport environment than only the security checkpoints with the associated security agents. Although the artificial systems are a component of the airport security system, the human operators performing the tasks that work together with these artificial systems are not staff from the airport security system. The human operators fitting this neutral group are the operators located at the check-in checkpoint and the gate checkpoint [8]. Because these operators are not really part of the airport security system their main goal does not involve the identification of threat sources an objects.

The check-in checkpoint has one main human operator and in the current airport configuration a human operator only present in specific situations, respectively the check-in steward and the check-in manager. The main goal of the check-in steward is to perform the check-in process as efficient as possible with as much service as needed such that it is pleasant for the passengers. The manager needs to make sure the check-in process goes as smooth as possible in cases that the performance deviates from its norm. Both agents have the ability to communicate, either with each other, with other human agents or with the artificial systems of the airport security system. The communication can be done verbally or by means of transferring objects. Communicate is thus one of their possible states. Other states of the check-in officer is being busy performing a check-in procedure or not, checking and analyzing the obtained information from passengers and observing data from other security agents. Furthermore the check-in steward can observe suspicious behavior as well, although it is not the main goal of this agent. In the current airport security system lay-out the check-in manager will deal with a suspicious situation, either when it is concerning a passengers' behavior or an invalid ticket for example. The manager communicates this to the airport security system after which an alarm is raised or not, based on the decision of the manager if needed to communicate. In case of the new integrated airport security system using data fusion the check-in steward notifies the data fusion system himself. As well as for all other human operators in the airport environment, properties concerning personal situations which could affect the behavior and performance of the check-in staff are modeled. The properties are work experience, stability of the personal situation and the workload regarding amount of passengers and working hours.

The gate check steward possess the same characteristic properties that influence the performance as the human agents at the check-in checkpoint. The difference with the check-point personnel is the goal this agent wants to achieve. The goal of the gate check steward is to identify all people who are not a passenger for that specific flight boarding at the gate the steward is located. The main operations of the gate check steward is to communicate, observe passengers and objects of passengers and analyze data from security agents. Similarly, when present in the current airport security system lay-out the gate check steward needs to notify a manager higher in the hierarchy about a suspicious situation. The manager will then decide what is done with the situation and if an alarm for the airport security system is needed. While present in the integrated airport security system the gate check steward communicates with the data fusion system directly in order to share and obtain information.

- Normal passengers

Next to all the human agents which are working in the airport environment, either in the security domain or execution airport terminal processes, there is also another type of human agents, namely the passengers. As a control group normal passenger are introduced to analyze the performance of the airport security system not only with respect to threats but in general. With the presence of normal passengers among threat sources a normal day at an airport environment is simulated. The passengers follow the route through the airport environment undergoing all airport terminal processes in order to arrive at the aircraft to depart to their destination. The passengers are free to move around the airport terminal, but need eventually to arrive at the aircraft. The checkpoints within the airport terminal, respectively arrival hall, check-in, passenger check and baggage check, customs, the gate and the aircraft form the states the passengers can have when moving through the airport environment. The passenger follows the order of checkpoints described before and cannot move backwards to previous spatial points. If a passenger tries to skip one of the checkpoints and continues without accomplishing that process, it will be marked as suspicious behavior. The environmental characteristic of business influences the behavior of certain passengers. At these checkpoints it is usually the case that there are multiple passenger waiting for their turn. Queuing is introduced such that this situation is simulated as well. So, at every spatial state of a passenger a queuing state is present as well.

Apart from the spatial characteristics passenger also have personal characteristics and objects [92]. The behavioral characteristics can also influence the propagation through the airport environment. Same people want to move quickly through all airport processes in order to be at the gate, others would like to avoid queues when they see it is busy and stay longer in the public area before going to the security checkpoint or at the leisure area of the secured airport environment before going to the gate. Furthermore, there are personal characteristics which do not influence the spatial characteristics but reveal a passenger’s behavior. There is a wide range of behaviors which is labelled by security officers as suspicious behavior possibly shown by a threat source. Although not being a threat source even normal passengers can show these behavioral characteristics. Considered behaviors are described by a document from the TSA [76]. In the model the majority will be under one state property called behavior and the level of presence of behaviors will result in a higher or lower level of suspicious behavior. The difficulty with behaviors is that these are not present all the time, this makes them hard to spot and security officers or other sensors need to be at the right location and the right time to identify suspicious behavior [2]. There are more than only behavioral characteristics that can be identified, also other personal characteristics can be useful to look for threat sources and objects. These sensors are known from use in public areas already, for example in airports [93]. Certain character traits are triggered and measured. For example a provocative image or message is shown and the reaction of passengers are analyzed or traits like heartbeat and metabolism which can be measured by sensors. Also these traits have a certain intensity for every passenger at a certain point in time, where the environment can add to this intensity.

Additionally there are properties or objects a person has who are not linked to behavior but are more private. Every passenger has a unique biometric identity which is used to identify, track and analyze a person, the communication a passenger performs to the requests of security officers can have levels of suspiciousness and the criminal history of a passenger adds to the risk profile [87]. Aforementioned were all related to the person itself, the passenger also has a ticket and a passport which are important for the airport processes and which can be normal or invalid. Finally, the passenger can also have baggage and/or hand-luggage, which may or may not contain suspicious items.

- Attacker agents

Threat agents are the attackers in the airport security system problem. Where normal passengers just intend to go to their aircraft to board a flight to their destination, the attacker has the intention to execute an attack in that aircraft and thus wants to succeed in bringing the threat object into the aircraft [2]. The type of attacker is described in Section 4.3. The same behavioral properties, personal properties and objects are present for an attacker as for a normal passenger. That an attacker is named as such does however not mean that all these properties are labelled as suspicious or as being a threat. The attacker is not known as an attacker beforehand by the airport environment. That is why the attacker will be processed just like any other normal passenger. The behavior and the two main interesting character traits of the attacker are modeled as its properties as well, just like the verbal communication if it happens, its history and the biometric characteristics. The level of expertise in performing an attack and the personal character of the attacker will define the level of intensity of the suspiciousness of the properties. Similarly can the environment contribute to actions and decisions made by the attacker. As explained in section 4.3 there will be three levels of attacker, all with their own intensity and approach. Additionally the baggage, hand luggage, ticket and passport are present for the attacker as well.

- Artificial system agents

Next to the human agents there are many components which serve the technical part of the so called socio-technical airport security system. All artificial systems present in the airport environment which need to be modeled serve the security purpose. Two different groups can be distinguished, respectively the established security systems present in most of the airport terminals at the moment and the data fusion systems to serve the new designed integrated airport security system. Although artificial systems do not have the same mental capacity as humans, in their own way they are able to reason and make decisions. However, they lack the behavioral characteristics. On the other hand sensor properties which define the performance can be seen as the behavioral of the artificial systems.

  - Conventional artificial security agents

The conventional security agents are all the security systems that are present in the current airport security system lay-out. These security systems are present throughout the entire airport environment. Different types of systems and sensors are installed in order to achieve the overall goal of identifying a threat source and object in the most efficient way [17] [8] [93] [94]. The individual security systems are mainly located at or near the checkpoints of the airport processes, although some are present at many places in either the public or secured areas of the airport terminal. To the conventional security agents belong the surveillance cameras, the check-in system, an access scanner at the entrance of the secured area of the terminal, a passenger scanner, two hand luggage scanners, two baggage scanners, a customs security system, the aircraft access system, a biometric sensor and two types of character traits sensors. Those systems that are present throughout the airport environment are the surveillance cameras and type 1 of the character trait cameras that measures the reaction of passengers' reaction on provocative information. The baggage and hand-luggage scanners are equipped with two types of sensors. The normal millimeter wave x-ray imaging sensors and sniffer sensors, such that all possible aspects of a threat object can be analyzed.
All these artificial security agents have their states in common, the only thing that differs is the object they have to deal with. All agents are not available to execute a task if they are busy performing analysis with an object already. Apart from that the agents can communicate, perform their security task, analyze the measurements and make decisions. Compared to human agents this decision making is fairly simple and is the same all the time. A receiver operating characteristics (ROC) curve is used in order to establish the settings of each artificial agent individually. The ROC curve cannot change over time for an individual system, as it is an operating characteristic set by the manufacturer. The probability of true positives relative to false positives can be read in such a curve. Only one point on the curve can be used per execution of a task, which means that the probabilities of detection of true positives and false positives are set during working hours and determine the performance efficiency of a security system. These operational characteristics can be seen as the behavioral characteristics of human agents.

- Data fusion agents

The new designed airport security system is different than the current airport security system with respect to the overall operation. The new designed airport security system is an integrated system where at the moment the airport security system lacks this integration. The integration is performed by using data fusion [5]. Data fusion is an approach performed by a special data fusion system that connects all the individual security systems on the basis of their individual decisions. Using these individual decisions as input data for the performance of other security systems later on in the overall airport process could eventually lead to a more efficient way of working regarding the goals of the overall airport security system. The data fusion system therefore needs to have the ability to communicate with all other security systems. Apart from that it has its own states when performing the data fusion steps. The data fusion system needs to be able to handle a lot of data at the same time as some information needs to be processes in real time and there are many passenger present in the airport environment from whom data can be communicated any time. The steps the data fusion system performs next to communicating are, data preparation, data association and data estimation. These steps are the states the data fusion can possess. All steps are important to get data which is efficiently fused and where decisions can be based on, but the data estimation is can be called the actual data fusion. The data fusion system finds the individual security systems that can be linked to increase the performance of the overall airport security system relative to an individual security system. It does this for every passenger present in the airport environment by following the passenger moving past all the individual security systems present and developing a security risk profile for every passenger. The security risk profile contains all important information about a passenger arriving at the airport and going to board a flight. This information consist of the behavioral actions, character traits, personal history and security check results. A security risk profile is labelled with a certain level of threat based on the aforementioned information. Four levels are identified, with level one being no threat at all to level four being an absolute threat. When a passenger comes arrives at level three or four action need to be taken and an alarm is raised for this passenger. The security risk profile already contains information as the passenger enters the airport or when the passenger checks-in. Personal history and flight information will immediately be made available on which a preliminary threat level is based.

4.4.6 Elaborating the performance-oriented view of the current and newly proposed integrated airport security systems

The fourth and last view is the performance view. All views from the organizational theory need to be analyzed as they work closely together. The performance oriented view describes the goals present in the organizational structure and the performance indicators needed to analyze the performance of the organization with respect to their goals. This means that relevant performance indicators need to be established with their relationships to the formulated organizational goals.

Each organization, the airport security system even so, exists in order to achieve one or more goals. To guarantee the continued achievement of these goals, the organization should keep an eye on its performance. In order to establish the right performance indicators, the organization should thoroughly investigated the real goals which are present. The organizational goals are achieved by selecting roles which need to execute appropriate tasks performed by relevant agents to fill in these roles. Furthermore, the organization should manage the complex interactions with a dynamically changing environment. A change in the environment could imply a change in actions in order to satisfy the goals.

Different types of goals can be set up for an organization, respectively hard goals and soft goals. The main difference between the goals can be made on the basis of the level of satisfaction that can be achieved. When the success can be measured in a precise manner, i.e. checking certain requirements

defined in the goal expression, the goal is called a hard goal. While in some cases the fulfillment for some goals in real life may be more difficult to evaluate as they do not have directly determinable conditions, these goals are called soft goals. The fulfillment of the goals can only be established in an efficient way as the goals are linked to the other views in the organizational theory and with the environment in which the organization operates.
It is obvious that an organization should have one or more goals in order to perform its overall tasks in the most efficient way. Furthermore, the individual agents present in the organization, who are designated a certain role and need to execute a subtask with respect to the overall tasks, have their personal goals during the execution of their tasks as well. These goals may be similar, completely different and even interfere with the goals of the overall organization. The performance of the individual agents can be measured in the same manner as the performance of the organization.

A goal is an objective that prescribes a desired state to be fulfilled by either an overall organization or individual roles. Many characteristics can be adhered to a goal description. These characteristics consist of the level of priority, the type of evaluation, the time interval for which it lasts, the owner, the point of view, the hardness (hard or soft goals) and the negotiability [9].

The presence of all the individual agents in the airport security system leads to many different individual goals, which could be difficult for the overall airport security system to build overarching goals. However, as most of the individual agents execute tasks in the same domain, namely the security domain, the intention of individual agents should always be as well to perform towards the security purpose. The overall goals of the airport security system are the leading goals in the analysis of its performance in the established security risk scenario. The three main goals of the airport security system with their characteristics are presented below:

Goal 1
Definition: It is required to identify all threat sources and objects within the airport environment
Priority: high
Horizon: long-term
Evaluation type: achievement goal
Ownership: organizational
Perspective: management
Hardness: hard
Negotiability: non negotiable

Goal 2
Definition: It is required to identify all normal passengers and objects within the airport environment
Priority: high
Horizon: long-term
Evaluation type: achievement goal
Ownership: organizational
Perspective: management
Hardness: hard
Negotiability: negotiable

Goal 2
Definition: It is required to provide and maintain a high level of service to all passengers going through the sequence of airport processes in order to board their plane
Priority: high
Horizon: long-term
Evaluation type: development goal
Ownership: organizational

Perspective: management, passengers
Hardness: soft
Negotiability: negotiable

These goals form the basis of the tasks needed to be performed in the airport security system. Moreover, they stay the same in both airport security system models, even though the approach of achieving the goals will be different. The tasks are performed by agents who have all the competences to fulfill the roles designated to the tasks. An individual agents also have goals for themselves. This can be personal goals or goals related to a more detailed level of the execution of a specific task. The aim of this thesis is however not to show the detailed performance of individual agents. The aim is to analyze if an increase in performance of the overall airport security system can be achieved by means of integrating the system using data fusion with respect to the current individual approach airport security system. Nevertheless can these goals be differentiated from the character properties and operational properties of the agents. Examples of goals at an individual level concern the execution of the individual task, such as: it is required that the execution of a certain task may not exceed a certain time limit, it is required to identify objects that are not complying to the regulations of a certain process, it is required that communication about data may not exceed a certain time limit, it is required that the amount of involved security systems not informed about updates of a security risk profile is zero, it is required to maintain high efficiency during operational hours.

Goals are not set without a reason. They describe a certain aim of the airport security system. An organization should be aware of the satisfaction of the defined goals. In order to say something meaningful about realizing the goals, performance indicators are set up. For every goal one or more performance indicators can be established, the amount depends on the level of detail needed and whether a small amount of performance indicators can cover all the domains. The overall goals of an organization are the drivers of the behavior of the organization. Performance indicators measuring these goals are called key performance indicators (KPI) and are widely used to analyze an organizations' performance. A KPI is a measure that expresses the performance of an organization or individual system.
Within the airport security system there are many organizational and individual goals. However, in order to analyze the performance of the overall airport security system only the organizational KPIs will be addressed. The goals are defined before and appropriate KPIs should be defined such that all aspects are covered. All KPIs should be hard indicators such that a meaningful conclusion can be made about the performance of the airport security system. The identified KPIs are defined below:

KPI 1
Definition: Amount of threat sources and object identified

KPI 2
Definition: Percentage of normal passenger identified as threat sources

KPI 3
Definition: Time to move from the moment of arrival to the aircraft for a passenger

The above described three KPIs form are elementary to analyze the performance of the airport security system. The KPIs will be used for both the current airport security system and the new designed integrated airport security system. On the basis of these KPIs a comparison can be made between the two lay-outs with respect to satisfying the goals of the organization. The first three KPIs relate to the first two goals which deal with the performance relative to identification of threat sources, while the fourth KPI relate to the third goal which deals with the performance relative to the service provided to passengers. Although these KPIs are measurements for the overall airport security system, these can be used to measure the individual security systems' performance as well.

5 Model formalization and implementation

Following the methodology for this research, after all knowledge is gathered about the research problem and the conceptual model is created, the formalization and implementation phase is performed. Section 5.1 will first discuss the general language in which the model will be modeled in order to get a good understanding. Subsequently, the actual model language, approach and main rules are presented in Section 5.2. A more comprehensive overview of the rules used in LEADSTO can be found in Appendix A.

5.1 A language for modeling system dynamics

The last step in the methodology followed in this thesis is the formalization and the implementation and analysis phase of the model. The model is set up using all the knowledge gathered, analyzed and designed during the previous steps. The implementation of the model requires a formal modeling method. Approaches for formal modeling and analysis have been established in all kind of domains and two main groups could be identified, as also explained earlier from literature. These two categories are the traditional modeling methods and the agent-based methods [52].

In an organization like an airport security system there is a high complexity of social dynamics as well rather than only the system dynamics properties. This is the result from all the interactions on a more local level between the agents in the organization and from the agents with the environment. Because of these relationships at a local level it benefits more when the organization is analyzed on a more detailed level with respect to the performance of the organization. Agent-based methods on the other hand can include the local interactions of the multiple agents present in the overall organization, including the individual behaviors of the agents. Both human agents and artificial systems can be implemented in the same model such that the socio-technical nature of the organization can be best exploited [52]. The organization theory, as used with the different views, is effective when using an agent-based approach as it can improve computational properties based on the agent system. Especially the organizational view where agents are set up by roles improves working with high complex and poor predictable dynamics of the organization. The ontology used in agent-based methods can be used to conceptualize many different concepts and relations, which could lead to the analysis of many different scenarios [9]. Introducing the behavioral rules into the model to analyze the performance of the individual agents and overall system could benefit the airport security system problem as the performance depends on interaction with the environment as well which can change over time. The agents in the model have a certain behavior, reasoning and coordination which is better implemented by using agent-based methods than traditional system dynamics models. There are also many system components as processes, alarms, switches and thresholds present in the airport security system which are better described by discrete transitions. Therefore it can be said that continuous modeling methods can have limitations for implementing the airport security system problem, thus agent-based modeling is used.

The airport security system is defined both by qualitative and quantitative aspects. The internal states and behavioral rules that agents possess demand the usage of a different type of modeling language and software than the established continuous modeling techniques, such that the reasoning and dynamics of the entire system implement both these qualitative and quantitative aspects. The rules can be defined from simple predicate logic to complex algorithms. The most suitable language for the airport security system problem is the Temporal Trace Language (TTL) [95]. Temporal logics form the basis of the TTL language, although also differential equations can be defined. Additionally, TTL can describe the behavioral characteristics of the system at the three different levels, respectively the macro, meso and micro level, which makes scalability easier and modeling and analysis less complex.

The TTL language is derived from the so called order-sorted predicate logic [96]. TTL extends this standard language by implementing dynamic properties of the system as well. The states of the agents present in the model are defined by using a special ontology. The ontology consist of different sorts, predicates, constants, variables, functions. For every agent within the system various uses of this ontology can be witnessed. These various domains within the ontology are used to indicate different state properties an agent can have [97]. Three different types of ontologies are distinguished, namely IntOnt(agent), InOnt(agent), OutOnt(agent) and which describe respectively the internal, input and output state properties of an individual agent. As an example, when describing agents the input ontology is used to how the agent sees its environment, while the reaction of the agent on the environment is expressed by an output ontology. The special characteristic of TTL to define dynamic properties is generated by specific sorts present in the language. The sorts needed to build a dynamic property are; TIME, sequences integers that define time points, STATE, a collection including states the agents can possess, TRACE, a collection of the timelines with attached to each time point the states present, STATPROP, a set including state properties present in the system, and VALUE, an ordered set of numbers. The state of an agent is expressed by the function TRACE x TIME → STATE. Sorts VALUE and TIME are connected by a formal expression: TIME x VALUE → TIME. States of agents, STATE, and state properties, STATPROP, are connected in such way that a certain state property should be satisfied such that the agent can have a certain state. The possible states and the state properties are described by terms within the TTL language. These terms are based on variables, constants and functions including the aforementioned sorts. The dynamic properties are needed to describe a change in state an agent has. These dynamic properties can be formulated in a formal way by various standard TTL expressions [98]:

1. *If v1 is a term of sort STATE, and u1 is a term of the sort STATPROP, then holds(v1,u1) is an atomic TTL formula.*
2. *If $\tau 1$, $\tau 2$ are terms of any TTL sort, then $\tau 1 = \tau 2$ is a TTL-atom.*
3. *If t1, t2 are terms of sort TIME, then $t1 < t2$ is a TTL-atom.*
4. *If v1, v2 are terms of sort VALUE, then $v1 < v2$ is a TTL-atom*

The exact derivation of the interpretation is explained by [9] as the semantics of the TTL language, but this is out of scope of this thesis, although the semantics are by itself used when implementing the model with a TTL language. Implementation of the model with TTL language requires a programming software that can handle the TTL language. Such programming software generally uses an executable language form which is a sublanguage of TTL.

One of these executable languages is the LEADSTO language [99]. The LEADSTO language can be operated in a simple manner, although having the ability to simulate qualitative and quantitative aspects and that the results often can be shown graphically. Furthermore, TTL and thus the LEADSTO language presents much expressivity as states defined over time can be used in dynamic properties. This means that multiple traces can be followed at once.
Direct temporal or causal relationships are modeled such that different state properties can be linked at specific time instances. Using the semantics of TTL the standard LEADSTO language formula can be

formulated as follows: There are two state properties, respectively α and β, and there are variables e, f, g, h which are nonnegative real numbers which means they are present as constants in sort VALUE, then α and β can be linked by the formula, with definition and an example to explain [99]:

$\alpha \ \rightarrow_{e,f,g,h} \ \beta$

"If state property α holds for a certain time interval with duration g, then after some period of delay between constants e and f, state property β will hold for a certain time interval with duration h" [99] *(Also see Figure 5.1)*

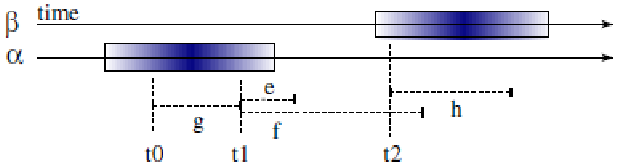

Figure 5.1: Executable dynamic property in LEADSTO [99]

An easy example of such a dynamic property relation is used to show how this formula would look like, this is not an implementation of the airport security system model:

$observes(agent\_A, food\_present) \ \rightarrow_{2,3,1,1.5} \ beliefs(agent\_A, food\_present)$

The formula is the formal way of describing the dynamic property relation. Informally this relation can be described as the fact; if agent A observes that for a time period of 1 time point food is present at a certain location, after a random delay of the duration between 2 and 3 time points, agent A will believe for 1.5 time points that there is food present at a certain location.

States are not stationary as there is a sort TIME available in the LEADSTO language in order to describe these dynamic properties. A trace is built based on the dynamic properties concerning the states which are present at every time point for the duration of the time interval set when implementing the model. A trace, γ, is defined for a certain type of ontology for a certain agent, this means that there can be many traces which need to be simulated in a model with multiple agents. The aforementioned standard LEADSTO formula only holds for a certain trace γ if [99]:

$$\forall t1 \ [\forall t \ [t1 - g \leq t < t1 \ \Longrightarrow \ \alpha \ holds \ in \ \gamma \ at \ time \ t \ ] \ \Longrightarrow \ \exists d \ [e \leq d \leq f \ \& \ldots$$
$$\ldots \ \forall t' \ [t1 + d \leq t' < t1 + d + h \ \Longrightarrow \ \beta \ holds \ in \ \gamma \ at \ time \ t' \ ]$$

The trace introduced in this formula incorporates the temporal aspects of actions performed by agents in the system. The trace shows when and how the agent and thus the environment changed throughout the specified time interval for the simulation of the model.

The LEADSTO language will be implemented in the especially designed LEADSTO software. The software program consist of two separate parts, the property editor and the simulation tool. These two tool eventually work together but are individually used. The property editor, as the name already implies, is used to describe all the LEADSTO specifications. When building a model which need to represent a certain phenomenon many dynamic property relations need to be described such that every possible scenario and every possible behavioral response and action of all agents are prescribed for the case that the environment takes this shape that a certain action need to be executed by an agent. The LEADSTO specifications thus include all the dynamic properties as the standard formulas were explained above, which form the key driver for the model to act how it will act, as well all other inputs needed for a model to run, which includes the sort, initial conditions, time intervals, variables and constants, etc.. LEADSTO does not allow functional symbols to be used, which means that all functions in the executable language to define state properties are replaced by predicates [99]. The same transformation into a predicate is done for the holds relation. The simulation tool can be used once the entire model is constructed in the property editor. The simulator tool calls the model from the property editor and loads the model into its environment. Based on the rules set up in the property editor a simulation can be made and the output is displayed graphically. Apart from the results also the traces existing after the model has run can be visible in order to see which states hold with which state properties during the simulation time interval.

5.2 Ontology and modeling dynamics

An ontology forms the basis of the implementation of a model into a programming software. The ontology can be used to implement behavioral characteristics and rules in a temporal aspect such that dynamic properties are formed. These dynamic properties, as well as constants and variables, are defined in a predicate logic language. As described in Section 5.1, the TTL language will be followed to implement the airport security system problem. An executive form of this language is called LEADSTO. The executive form of the TTL language is needed in order to transform standard formulae into programming formulae which can be implemented into a software environment, in this case thus LEADSTO [99]. The information in Section 5.1 is provided because the general semantics of the TTL language and LEADSTO should be known before implementing a complex model like the airport security system and its environment. In fact the aforementioned formulae are an abstract representation of the formulae which need to be used to model the airport security system. Therefore the different types of ontologies for the agents present in the system need to be defined, where after the relationships between agents and dynamic properties of the behavioral rules can be set up such that the security risk scenario is simulated in LEADSTO.

The aforementioned modeling method, language and programming software will be used such that the airport security system problem can be analyzed in the most optimal way. The implementation of a model needs in any case a conceptual model which defines the boundaries, relationships and main principles already on paper before the actual computational model is built. In Chapter 4, organizational theory was adapted in such a way that could be used for the airport security system as well. Four different views, respectively the performance view, process view, organizational view and agent view, were developed using this organizational theory. The combination of these four views can be seen as the conceptual model of the airport security system problem. The threat scenario built in Section 4.3 is the scenario that needs to be simulated in LEADSTO as well. The threat scenario completes the conceptual model on the basis of initial values and explanation of behavioral rules which are inputs for the dynamic properties.

Dynamic properties are set up using the ontology. The ontology holds for every agent and is used in all expressions, states, dynamic properties or formulae that describe the principles of the airport security system threat scenario. The ontology is used to describe interaction channels, as agents have internal, external, input and output states. First, different sorts with associated elements are established. These sorts and elements are the foundation for the state properties, states and rules described by the predicates. These predicates are used to describe the rules and dynamic properties. An important type of rule used in order to indicate the state a certain agent has and this state remains longer than one time unit and only changes when a state properties changes is the persistence rule.

Sort	Elements
Passenger	{pax1, pax2, pax3,….., pax15}
Agents_human	{check_in_staff, pax_check_officer1, pac_check_officer2, pax_check_officer3, pax_check_officer4, bag_check_officer1, bag_check_officer2, customs_officer, gate_staff}
Agents_technical	{check_in_system, pax_scan1, pax_scan2, hand_luggage_scan1, hand_luggage_scan2, bag_scan1, bag_scan2, sniffer_scan, passenger_system, personal_info_system, boarding_system, surveillance_camera, biometric_sensor, history_system, trait_sensor1, trait_sensor2, data_fusion_system}
Location	{entrance, check_in, security_check, baggage_check, customs, gate, aircraft}
Check_result	{clear, alarm, accept}
Baggage	{baggage1, baggage2}
Object	{hand_luggage, passport, ticket, behavior, biometrics, history, traces, trait1, trait2, story}
State_object	{normal, suspicious, threat, valid, invalid}
Object_security	{image, info, risk_profile}
threat_level	{normal, suspicious, substantial, high}
Amount	{0, 1, 2, 3, 4, 5}
Task	{ask, answer, provide, accept, clear, alarm}

Table 5.1: Sorts and associated elements in the ontology of the agent-based model

The main sorts and the associated elements are shown in Table 5.1. The elements in these sorts are used in the predicates that describe state properties and states. The basic predicates and their description are shown in Table 5.2. These basic predicates consist of a predicates that are very frequent and the predicates used to describe initial conditions. The initial conditions are expressed as an interval. These intervals form the constraints for the progression of the simulation. Predicates which induce a reaction or can change over time have a starting range from time unit 0 to 1, while predicates which describe a rigid property hold from time unit 0 to end time.

Predicate	Description
Agent initial conditions	
Arrived_at(entrance, passenger)	The agent *passenger* arrives at the *entrance* of the airport environment
Has(passenger, state_object)	The agent *passenger* possesses a certain *state* of risk, carrying a threat object on its body or not
Has(passenger, object, state_object) *i.e. has(pax1, behavior, normal)*	The agent *passenger* possesses a certain *object* with a certain *state* of risk
Has(passenger, baggage, state_object)	The agent *passenger* possesses *baggage* with a certain *state* of risk
Present(agents_technical, object, passenger)	*Information* about an *object* of an agent *passenger* is present in the information of a certain *technical security system*

General situation predicates	
Is_at(agents_human, location)	A *human security system* is present at a certain *location*
Is_at(agents_technical, location)	A *technical security system* is present at a certain *location*
Is_connected(location, location)	Two *locations* are connected with each other, enabling movement between them *passengers*
Is_connected(location, location, baggage)	Two *locations* are connected with each other, enabling movement between them for *baggage*
Follows(passenger, passenger)	A *passenger* follows the *preceding passenger*
Follows(passenger, passenger, baggage)	The *baggage* of a passenger follows the *baggage* of the *preceding passenger*
Exist(passenger)	A *passenger* exists in the airport environment
Move_to(location, passenger)	A *passenger* moves to a *location*
Is_at(location, passenger)	A *passenger* is at a *location*
Is_in_queue(location, passenger)	A *passenger* is at a queue at a *location*
Start_process(location, passenger)	An airport process is started for a *passenger* at a *location*
Concluded_process(location, passenger)	An airport process is concluded for a *passenger* at a *location*
Process_busy(location, passenger)	An airport process is busy handling a *passenger* at a *location*
Arrest(location, passenger)	A *passenger* is arrested at a *location*
Start_process(location, passenger, baggage)	An airport process is started for the *baggage* of a *passenger* at a *location*
Concluded_process(location, passenger, baggage)	An airport process is concluded for the *baggage* of a *passenger* at a *location*
Process_busy(location, passenger, baggage)	An airport process is busy handling the *baggage* of a *passenger* at a *location*
Is_in_queue(location, passenger, baggage)	The *baggage* of a *passenger* is at a queue at a *location*
Predicates of main actions of agents	
Communication(location, FROM, TO, task, object)	An agents communication FROM this agent TO another agent at a location with a certain *intend or task* about information of an *object*. FROM and TO are used as communication can be established between sorts *passenger*, *agents_human* and *agent_technical*
Perform_check(location, agents_technical, object, passenger)	A check is being performed on an *object* of a *passenger* at a *location* by a *technical security system*
Perform_check(location, agents_human, object, passenger)	A check is being performed on an *object* of a *passenger* at a location by a *human security system*
Perform_scan(location, agents_technical, object, passenger)	A scan is being performed on an *object* of a *passenger* at a location by a *technical security system*
Perform(check_result, location, object, passenger)	A result of the performed check is being made from an object of a passenger at a location
Perform(object_security, location, object, passenger)	An *object* as output of the performed check or scan is made of an *object* of a *passenger*
Observe(check_result, location, object, passenger)	The result of the performed check from an object of a passenger is observed at a location
Observe(object_security, security, location, object, passenger)	The output object of the performed check from an object of a passenger is observed at a location
Observe(location, object, passenger)	An object of a passenger is observed at a location

Table 5.2: Common predicates and their description in the agent-based model

The predicates of the main actions of agents only show the part that describes the type of action and the information and other agents involved. The perception and performance can be seen from different points of view for an agent, respectively the input and outputs states. Therefore an additional predicate is added before the predicate of the action. These predicates are either *input(passenger)|…*, *input(agents_human)|…* or *input(agents_technical)|…* and *output(passenger)|…*, *output(agents_human)|…* and *output(agents_technical)|…*. The input ontology can be seen as the observation from the agent of actions happening, while the output ontology describes the actual performance of a certain action of that agent. Furthermore, if an agents observes a certain action, an environmental characteristic or behavioral characteristic from another agent, then it is assumed that the agent beliefs what was observed in all instances.

In order to introduce time as a variable, which makes the observation of certain states at certain time points more visible and calculations with time easier, a simple rule is introduced that describes the continuation of time, until the end time of the simulation with t being an integer that illustrates the current time point.

$current\_time(t) \rightarrow_{[0,0,1,1]} current\_time(t+1)$

The organizational structure and the airport environment are defined such that a passenger can propagate through the environment from entrance to aircraft, if the passenger still exists in the environment. Below the rules for the movement are described, starting with the identification of the unique predicates that describe how the passengers and their baggage can flow through the airport environment stopping at the checkpoints to undergo the associated process.

Is_connected(entrance, check_in)
Is_connected(check_in, security_check)
Is_connected(check_in, baggage_check, baggage)
Is_connected(security_check, customs)
Is_connected(customs, gate)
Is_connected(gate, aircraft)
Is_connected(baggage_check, aircraft, baggage)

Follows(pax1, pax2) & follows(pax1, pax2, baggage)
Follows(pax2, pax3) & follows(pax2, pax3, baggage)
Follows(pax3, pax4) & follows(pax3, pax4, baggage)
…
Follows(pax14, pax15) & follows(pax14, pax15, baggage)

Exist(passenger) & not arrest(location, passenger) → exist(passenger)

Follows(passenger1, passenger2) & exist(passenger1) & exist(passenger2) → follows(passenger1, passenger2)

Follows(passenger1, passenger2) & follows(passenger2, passenger3) & exist(passenger1) & exist(passenger3) & not exist(passenger2) → follows(passenger1, passenger3)

Follows(passenger1, passenger2, baggage) & exist(passenger1) & exist(passenger2) → follows(passenger1, passenger2, baggage)

Follows(passenger1, passenger2, baggage) & follows(passenger2, passenger3, baggage) & exist(passenger1) & exist(passenger3) & not exist(passenger2) → follows(passenger1, passenger3, baggage)

Arrived_at(entrance, passenger) & is_connected(entrance, location) → move_to(location, passenger)

Move_to(location, passenger) → is_at(location, passenger)

Is_at(location, passenger) → is_in_queue(location, passenger)

Is_in_queue(location, passenger) & not start_process(location, passenger) → is_in_queue(location, passenger)

Is_in_queue(location, passenger2) & concluded_process(location, passenger1) & follows(passenger1, passenger2) → start_process(location, passenger2) & process_busy(location, passenger2)

Process_busy(location, passenger) & not concluded_process(location, passenger) → process_busy(location, passenger)

Arrest(location, passenger) → concluded_process(location, passenger)

Clear(location, passenger) → concluded_process(location, passenger)

Concluded_process(location1, passenger) & exist(passenger) & is_connected(location1, location2) → move_to(location2, passenger)

Is_at(aircraft, passenger) → board(passenger) & not start_process(aircraft, passegner) & not is_in_queue(aircraft, passenger)

Passengers can propagate through the airport environment following the rules above. It is assumed that the passengers can only follow the preceding passengers and that the flow of checkpoints is kept at all times. The human and technical security systems have a fixed location in the airport environment. Passengers will encounter them along their way from the entrance to the aircraft. Communication between passengers and security systems and between multiple security systems is founded in order to execute the airport processes. The predicates of the main actions of agents in Table 5.2 with their preceding predicates are used to describe the situation at a certain checkpoint.

Below some of the rules for the checkpoint performing the security check are highlighted in order to show how the model works regarding communication between agents and actions agents perform. A comprehensive view of the model based on the example of the security check checkpoint can be found in Appendix A for clarity reasons.

output(security_officer2)|communication(security_check, security_officer2, passenger, ask, hand_luggage, passenger) → input(passenger)|communication(security_check, security_officer2, passenger, ask, hand_luggage, passenger)

input(passenger)|communication(security_check, security_officer2, passenger, ask, hand_luggage, passenger) & has(passenger, hand_luggage, state_object) → output(passenger)|communication(security_check, passenger, security_officer2, provide, hand_luggage, passenger)

The rules shown above present the communication between two agents in the airport environment. Communication was already established before and is continued following the elements and predicates shown in Table 5.2 and the different ontologies agents can have. In the rules above a security officer communicates to the passenger and shows this as an output ontology. The security officer asks the passenger for hand-luggage. After a normal delay of one time unit this request is noticed by the passenger and as such described by the input ontology. A separate rule describes the reaction of the passenger after the passenger noticed the request of the security officer. The passenger internally processes the request and if the passenger possesses hand-luggage, the passenger will provide this hand-luggage to the security officer described by the output ontology of the passenger.

Next to the communication defined between agents, the individual security systems perform security actions as well. The KPIs are eventually based on the outcomes of these actions. The rules shown below present an action of an individual security system present in the airport environment. If the hand luggage scanner gets the signal that it can perform its task it will make an image of the hand-luggage as described by the output ontology of the hand-luggage scanner. If this image is made the hand luggage scanner can process this image and eventually provide an output to the environment which results in an alarm or a clearance. A second property is needed before the hand-luggage scanner knows how to react. This is the type of hand-luggage the passenger possesses. If the passenger would not possess any hand-luggage the action of performing the hand-luggage scan would not be possible. The type of hand-luggage of the passenger possesses defines if the hand-luggage scanner should treat the hand-luggage as being from an attacker or a normal passenger, which means the associated characteristic of the operational point on the ROC curve is implemented in the probabilities of the output of the hand-luggage scanner.

output(hand_luggage_scan)|perform(security_check, image, hand_luggage, passenger) & has(passenger, hand_luggage, normal) → **prob.** Output(hand_luggage_scan)|perform(clear, security_check, hand_luggage, passenger) v **otherwise** output(hand_luggage_scan)|perform(alarm, security_check, hand_luggage, passenger)

output(hand_luggage_scan)|perform(security_check, image, hand_luggage, passenger) & has(passenger, hand_luggage, threat) → **prob.** Output(hand_luggage_scan)|perform(alarm, security_check, hand_luggage, passenger) v **otherwise** output(hand_luggage_scan)|perform(clear, security_check, hand_luggage, passenger)

Additional rules are applied in order to incorporate integration by means of decision data fusion. Different configurations of integration are established. Additionally to the communication between the security agents and the passengers, there is additional communication between the security agents and the data fusion system about the obtained data during observations, checks and scans. This communication is modeled in a similar way as normal communication between agents. Also the actions the security agents and passengers perform are similar, although additional activities are performed in order to achieve the integration for the specific configurations. Special predicated and dynamic properties are set up in order to establish the different configurations of integration. The dynamic properties describing the integrated airport security system configurations can be seen in Appendix A.

6 Analysis & Results

Multiple steps were performed in order to set up the analysis of the performance of the airport security system. These steps were laid out by the adapted NIST methodology followed in this thesis. First the environment with all possible threat sources, threat objects and weaknesses were identified such that a threat scenario could be built. Subsequent, the actual airport security system configuration needed to be established. Two configurations of the airport security system were set up, respectively the current stand-alone lay-out and a new designed integrated lay-out using data fusion. These configurations of the airport security system were designed making use of an organizational oriented view, agent oriented view, process oriented view and performance oriented view which respectively showed the structure, participants, tasks and goals of the airport security system. The conceptual models of the two configurations of the airport security system were then used to found an ontology for the agents to implement the airport security system in the programming software LEADSTO. The final step after implementation is the actual running of the model and the analysis of the outcomes. This chapter discusses the analysis performed on the implementation of the models.
As discussed before, two configurations of the airport security system are established. The first configuration is the current airport security system which is characterized by a more stand-alone way of working of the individual security systems. The second configuration is the new designed airport security system integrated by using data fusion. In order to investigate the performance of the integration of the airport security system not one but three possible integration approaches are modeled during the implementation phase. The configurations of the current and integrated airport security system are analyzed in Sections 6.1 to 6.4 respectively.

6.1 Case study 1: current airport security system

The current airport security system as defined earlier is the most simplest of the applied configuration. It tends to simulate the current state of the way of working of the airport security system at most airports worldwide. The organizational structure seen in Figure 4.7, the processes, the agents with their capabilities and characteristics described in Section 4.4.5 and the goals established in Section 4.4.6 form the basis for this configuration which will be addressed in the first case study. Based on these views and the security risk scenario constructed in Section 4.3 the ontology for the implementation of the model into the programming software LEADSTO could be set up.

All agents with their individual characteristics are included in the model. The current airport security system has a stand-alone way of working, which means that there is little to no communication between security agents. Agents however have a close relationship with the environment as they need to perform their tasks in this airport environment. A stable environment is set up in order to compare results from all cases without needing to adjust for a highly dynamically changing environment. This means that the passengers which move through the airport environment follow all checkpoints present in the order they arrive at the airport and that all information concerning the airport environment is present at the same time for every passenger or security agent. Furthermore, in order to mimic a normal day at an airport multiple passengers will move through the airport environment instead of just one threat source. The airport security system then needs to identify normal passengers and threat sources instead of just a threat source. This is important to illustrate as a threat source can be identified in a situation where all normal passengers could be identified as threat sources as well, which is highly unwanted of course. However, the downside of

LEADSTO is the implementation of a high amount of similar agents. In contrast to other programming software where similar agents can be defined in a large number, here all agents present in the environment need to be implemented by hand. This makes it very time consuming if 50 passengers need to be implemented, which is still a low number for an airport. Therefore it is chosen to implement 15 passengers and only one station per checkpoint in the airport environment is used. The amount of passengers combining with only one station per checkpoint will still simulate a busy airport where queuing is needed for the individual checkpoints. From this 15 passengers 3 will be a threat source. The percentage of threat sources relative to normal passengers is therefore 20% which is rather high for an airport. However, the attackers will be used in order to analyze the performance of the airport security system for different ways of working of the attackers. The characteristics of passengers can either be normal or suspicious. The individual security systems relative to a specific characteristic should then analyze this characteristic and identify the type. Suspiciousness can be identified in certain degrees which induce a certain decision by the individual security system. This decision is the output identification of a normal or suspicious characteristic of a passenger.

These aspects of the airport security system are affected by the individual security agents present in the overall airport security system. The individual agents all have their own characteristics and their unique measurement subject. The probability of identifying true positives and false positives is already set up by the manufacturer, however there are always certain levels on which the equipment can execute its tasks. The probabilities can be found in a so called ROC curve of the individual security system. Although the ROC data of equipment used in the security domain is most of the times classified, literature is used to establish operational points on the ROC curve such that the operation of a normal airport is approached [5]. There could be more individual security systems present in this model than in normal airports. Security systems which are nowadays only used in modern more integrated airports. However this is the case such that the same equipment is used as in the cases where the new integrated airport security system is used in order to get comparable outputs.

The characteristics of the 15 passengers present in the airport environment can be seen in Table 6.1 and the individual security agents which form the overall airport security system with their ROC operational point can be seen in Table 6.2. Below some motivation for these choices is provided.

The tables show the characteristics of all passengers present in the airport environment and the performance probability of the individual security systems of the airport security system. These are the final inputs for the implementation of the security risk scenario. As can be seen there are many different variations of passengers. As explained in the agent oriented view there are two main groups, respectively normal passengers and attackers. Attackers are characterized by the possession of a threat object. This threat object can be present either on their body, in their hand luggage, in their hold baggage or a combination of these. Furthermore, all passengers have a range of personal characteristics which identify the uniqueness of each passenger. These personal characteristics are chosen such that security systems of the airport security system can identify the attackers among the normal passengers, based on the attacker types used in the security risk scenario. The amount of suspicious characteristics for the attackers is based on the type of attacker present in the system. More professional attackers have less suspicious characteristics than less professional attackers. However, as can be seen normal passengers can possess personal characteristics which have a certain degree of suspicion as well. Normal passengers are chosen to have these suspicious characteristics as well in order to simulate a more real life problem of the airport environment. These personal characteristics can be formed by any day to day situation, for instance a passenger who flies for the first time shows nervous behavior which can be identified as suspicious.

It is the task of the overall airport security system though to identify the normal passenger as a normal passenger and not as attacker and the attacker as such. The operational characteristics of the individual security systems give an indication on how these systems operate. The operational points on the ROC curve used for the specific data that can be seen in Table 6.2 are derived from literature for similar types of sensors such that a more real world scenario is created during the simulations. Although not a single airport or exact figures are used for these individual security systems, because of the bottom-up approach.

Pax	Body	Hand-luggage	Hold baggage	Compound traces	Behavior	Biometrics	History	Communications	Character trait 1	Character trait 2
1	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal
2	Normal	Normal	Normal	Normal	Suspicious	Normal	Normal	Normal	Suspicious	Suspicious
3	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal
4	Normal	Threat	Normal	Normal	Suspicious	Normal	Suspicious	Suspicious	Suspicious	Suspicious
5	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Suspicious	Suspicious	Normal
6	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal
7	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal
8	Normal	Normal	Threat	Normal	Normal	Suspicious	Suspicious	Normal	Normal	Suspicious
9	Normal	Normal	Normal	Normal	Normal	Normal	Suspicious	Normal	Normal	Normal
10	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal
11	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Suspicious	Normal
12	Threat	Normal	Normal	Suspicious	Suspicious	Normal	Normal	Suspicious	Suspicious	Suspicious
13	Normal	Normal	Normal	Normal	Suspicious	Normal	Normal	Normal	Normal	Normal
14	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Suspicious
15	Normal	Normal	Normal	Normal	Suspicious	Normal	Normal	Suspicious	Suspicious	Suspicious

Table 6.1: Passengers present in the simulation with their characteristics

Security agent	**True positive** (probability)	**False positive** (probability)
Security camera	0,60	0,35
Security officers	0,60	0,35
Access sensor	0,98	0,02
Passenger scanner 1	0,73	0,19
Passenger scanner 2	0,86	0,15
Hand-luggage scan 1	0,71	0,19
Hand-luggage scan 2	0,78	0,18
Baggage scan 1	0,71	0,19
Baggage scan 2	0,78	0,18
Sniffer sensor	0,74	0,23
Biometric sensor	0,85	0,10
Trait 1 sensor	0,80	0,19
Trait 2 sensor	0,69	0,26
Passenger history system	0,97	0,02
Check-in system	0,98	0,02
Ticket recognition system	0,98	0,02
Customs passenger system	0,97	0,05
Gate passenger system	0,98	0,02

Table 6.2: Operational ROC characteristics of the individual security systems

One of the personal characteristics is the behavior of passengers, such as being nervous described before. The special element of this personal characteristic is that only in one time unit in the model not a good impression can be obtained from this behavior. As in real life, the security system measuring the behavior of a passenger should identify the suspiciousness of the behavior for more than 1 time units. The wide variety of passengers is chosen such that all aspects of the airport security system are utilized, in this current airport security system configuration and in the next case studies when the integrated security system is analyzed.

The performance characteristics of the individual security systems in the model are based on probabilities, which means that there is a certain chance that a specific situation emerges from the simulation. Only one simulation would leave space for a lucky shot or outlier outcomes. Taking into account the amount of passengers and the probabilities of the ROC operational points of the individual security systems, 25 simulations are performed in order to get useful outputs and eliminate the outlier results.

The 25 simulation runs per scenario during every case study can be assumed to be reliable enough to compare the results among the scenarios and case studies. Although more simulation runs would induce more reliability concerning the overall output of the simulations. When following and implementing the formula below an indication of the reliability of the simulations can be given.

$$N = \left[\frac{Z * s_0}{\varepsilon * \bar{x}_0}\right]^2$$

Where N stands for the number of needed simulations, Z shows the quantile of the standard normal distribution, ε shows the level of error, s_0 shows the standard deviation of a sample amount of runs already performed and $\bar{x}_0$ shows the mean of a sample amount of runs.

In this case the number of detections are used to determine the reliability. From the main form of the current airport security system the first ten simulations are performed. The obtained mean and standard deviation are respectively 10.1 and 0.831. Additionally, an uncertainty of the confidence interval of 5% is implemented, which is generally used. The associated quantile for the implemented uncertainty is 1.96. Then when performing only 25 simulation runs the induced level of error for the outputs is 3.2%. For this low amount of simulation runs that level of error is not too significant. As well because the outputs are generated via a bottom-up approach and are used to be compared with similar obtained outputs for other case studies. The constrains that forces only 25 simulation runs to be performed is the amount of different configuration that needs to be analyzed and the time that it took to define these configurations and the time consuming nature of only one simulation run of the model.

The stand-alone way of working of the current airport security system means that only one alarm by any individual security system is enough to give an overall identification that the passenger is a threat source and needs to be detained. The 15 passengers, which can be seen in Table 6.1, can be categorized into three different classes. These three classes can help analyze the performance of the airport security system in a more structured way. First of all, there are attackers present in the airport environment, these are easily recognized by the presence of threat objects on them or in their baggage. The airport security system should identify these attackers as threat source, which will give an output on the performance of the detection of true positives. If an attacker is not identified as such, it is called a missed detection. The second and third category both consist of normal passengers. The second category includes normal passengers which possess one or more characteristics with a certain degree of suspiciousness. This suspiciousness does not relate to a threat source or object. The task of the airport security system is to identify this difference. If the airport security system fails to identify the passenger as a normal passenger, it is seen as a false positive. The third category are the entirely normal passengers without any suspicious characteristic. For these passengers the airport security system should not give an alarm at all. If the airport security system does so, it is diagnosed as a false positive as well. The performance of the overall airport security system can in the end thus be indicated by three main detection rates, respectively the true positive rate, the missed detections and a false positive rate. Table 6.3 shows the outputs of these detection rates for all 25 simulation runs.

Simulation runs	**True positives** *[pax numbers]*	**False positives, with suspicious characteristics** *[pax numbers]*	**False positives, without suspicious characteristics** *[pax numbers]*
1	4, 8, 12	2, 5, 9, 11, 13, 14, 15	
2	4, 8, 12	2, 5, 9, 11, 13, 15	6
3	4, 8, 12	2, 5, 9, 11, 14, 15	3
5	4, 8, 12	2, 5, 9, 11, 14, 15	3
5	4, 8, 12	2, 5, 9, 11, 14, 15	
6	4, 8, 12	2, 5, 9, 11, 13, 14, 15	6, 10
7	4, 8, 12	2, 5, 9, 13, 14, 15	7
8	4, 8, 12	2, 5, 9, 11, 14, 15	
9	4, 8, 12	2, 5, 9, 11, 13, 14, 15	
10	4, 8, 12	2, 5, 9, 11, 13, 14, 15	1
11	4, 8, 12	2, 5, 9, 13, 14, 15	3
12	4, 8, 12	2, 5, 9, 11, 13, 14, 15	3, 10
13	4, 8, 12	2, 5, 9, 11, 13, 15	7
14	4, 8, 12	2, 5, 9, 11, 13, 15	10
15	4, 8, 12	2, 5, 9, 11, 13, 14, 15	
16	4, 8, 12	2, 5, 9, 11, 14, 15	1

17	4, 8, 12	2, 5, 9, 11, 13, 14, 15	6
18	4, 8, 12	2, 5, 9, 11, 14, 15	10
19	4, 8, 12	2, 5, 9, 11, 13, 15	1, 7
20	4, 8, 12	2, 5, 9, 14, 15	6, 10
21	4, 8, 12	2, 5, 9, 11, 13, 14, 15	
22	4, 8, 12	2, 5, 9, 11, 13, 14, 15	
23	4, 8, 12	2, 5, 9, 11, 13, 15	1, 6
24	4, 8, 12	2, 5, 9, 11, 15	10
25	4, 8, 12	2, 5, 9, 11, 14, 15	3

Table 6.3: Simulation output current airport security system

As can be seen from Table 6.3, in all simulation runs all three types of attackers were identified as such. In case of the airport security system that is the most important goal to achieve. This means that the detection performance of true positives is really well, actually 100%. This shows that the current airport security system actually is a secure system, if all individual security systems are in use as in this case study. The achievement of this good performance of the detection of true positives comes at the expense of the normal passenger. Almost all passengers who possess a certain characteristic with a certain degree of suspiciousness is identified as a threat source as well, respectively a detection rate of false positives of normal passengers with a suspicious characteristic is 98%. However with the lack of information about the normal passenger it is hard for the current airport security system to identify a normal passenger with suspicious characteristics as a normal passenger. Even in a rare occasion a completely normal passenger is found to be a threat source. In total the detection rate of false positives in the system is around 58%. This is a relatively weak performance of the airport security system, which leads to additional unnecessary workload and annoyance by the passengers.

Although all threat sources are identified, it does not mean that all individual security systems would have identified the attackers as threat sources. The organizational structure of the current security system is based on the most comprehensive modern airport possible as the broad variety of individual security systems needs to be used for the integration of the airport security system. However, there are many medium sized airports that do not have the resources to implement all these sensors already. They commonly only use the security systems at the airport processes checkpoints, respectively at check-in, passenger and hand-luggage check, baggage check and customs. In order to see what kind of influence the absence of the more specialized individual security systems have, a similar analysis for the current airport security system is performed but only with the passenger scan, hand-luggage scan, baggage scan and the sensors for behavioral characteristics. The behavior characteristics are included as most airports have implement these type of sensors, for example security cameras, special access sensors or just security officers. By only considering these individual security systems the stand-alone way of working arises more prominently. The results can be seen in Table 6.4.

At first glance, a big difference between the performances of the current airport security system with specialized sensors and without specialized sensor can be noticed. Less passengers are detected by the security system without specialized sensors. However, less sensors are present and thus less characteristics are analyzed by the airport security system. Where the airport security system with specialized sensor had the opportunity to identify 7 normal passengers with suspicious characteristics, the system without specialized sensors only has 4 normal passengers with suspicious characteristics in the airport environment. This means that still almost all normal passengers with a certain level of suspicious behavior could not be identified as a normal passenger. Additionally, due to the stand-alone way of working and the operational characteristics of the individual security systems entirely normal passengers are still occasionally identified as well. Although this induces a higher workload it is however not the most striking result. Due to the fact that the suspicious behavior needs to be identified for a longer period of time and a few instances and the operational performance of the individual security systems is not one hundred percent, not all attackers are identified as threat source. The detection of all threat sources in the airport environment is from utmost importance. In this security risk scenario it is intolerable that this can happen.

Simulation runs	**True positives** *[pax numbers]*	**False positives, with suspicious characteristics** *[pax numbers]*	**False positives, without suspicious characteristics** *[pax numbers]*
1	4, 8, 12	2, 13, 15	
2	4, 8, 12	5, 13, 15	3
3	4, 12	15	7
5	8, 12	2, 14, 15	
5	4, 8, 12	2, 13	10
6	4, 12	9, 15	3
7	8, 12	2, 5, 13, 15	1,6
8	8, 12	2, 5, 13	
9	4, 8, 12	2, 13, 15	7
10	4, 8, 12	2, 11, 15	1
11	4, 8, 12	13, 14, 15	1
12	4, 8, 12	13, 15	10
13	4, 8	2, 15	
14	4, 8, 12	15	
15	4, 8, 12	2, 11, 15	
16	4, 8, 12	2, 13	6
17	4, 12	2, 13, 15	10
18	4, 8, 12	13, 14, 15	
19	4, 8, 12	2, 13	7
20	8, 12	9, 13	10
21	4, 8	13, 15	7
22	4, 8, 12	2, 13, 15	
23	4, 8, 12	2, 13, 14	1
24	4, 12	2, 13	3
25	4, 8, 12	2, 9, 15	

Table 6.4: Simulation output current airport security system without specialized sensors

Another notion of performance is the level of service, which is a goal of the airport security system as well. However, there could be a conflict between security and level of service. In general a high level of security generates a low level of service and vice versa. A sound equilibrium should thus be found, while still all attacker are identified as threat sources. Level of service can be translated into time, respectively time for a passenger to be processed and delay for other passengers to become processed.

When considering the main current airport security system it is obtained that there are a lot of false positives. These false positives are the key driver of the level of service. An identification of a false positive means additional workload such that the passenger is cleared. In the current airport configuration two actions can be taken concerning the passengers which have been identified as attacker. These passengers are either taken out of the environment of the airport processes and are checked out of scope of the airport environment considered in this research or a second opinion is done at the location of the positive identification. The time units used to represent the level of service

are not intended to simulate a real airport configuration, but are used to compare the level of service with one of the integrated airport security system configurations.
If passengers whom are identified as attacker are taken out of the environment this means additional processing time for this specific passenger. However the normal passengers still in the environment do not experience delay on the nominal processing time of that checkpoint. Moreover, because passengers are taken out of the environment, at a next checkpoint the queuing time is getting less. The average overall processing time is found to be 2775 time units in this case.
A more realistic way of working is the implementation of a second opinion rather than taking the passenger directly out of the environment. If passengers whom are identified as attacker are expected to undergo a second opinion this has a lot of influence on the processing time. As example the time of the second opinion is as much as the normal processing time of the first check that positively identified the passenger as attacker, which means that the processing time doubles at that checkpoint. This means that for every passenger after this false positive the delay increases by the amount of the processing time. As assumption a passenger identified as false positive will be identified as a normal passenger after the second opinion, while an attacker will still be identified as an attacker. This means that a normal passenger with more suspicious characteristics can be checked multiple times throughout the airport environment. The average overall processing time in this case increases to 4545 time units.

Sensitivity analysis is performed additionally. This is done to check if changes in the individual equipment used in the airport security system have an effect on the outcomes of a normal operating airport security system. The sensitivity analysis is performed in a negative and positive scenario. The negative scenario can be related to equipment that cannot operate to their full capacity or an airport that does not use the latest equipment there is. While the positive scenario accommodates for the implementation of newer more sophisticated equipment in the future. In both cases a change in the operational point on the ROC curve is induced or even a new ROC curve is composed. For the negative case the operational point moves down, which means that a decrease in probability of detection of true positives can be noticed. At the same time this implies a small decrease in the detection of false positives as well. For the negative case a decrease of 0.15 for the probability of detection of true positives is handles, while at the same time there is a decrease of 0.05 for the probability of detection of false positives. In case of the positive scenario a new ROC curve is used in the implementation to address the improvement of the security equipment. The ROC curve moves to the top and left of the graph, which means there is an increase in the probability of detection of true positives and there may be a decrease in probability of detection of false positives. For the simulation a similar amount of change is used as in the negative case, however this time an increase of probability of detection of 0.15 and a decrease of 0.05 in probability of detection of false positives is adopted. These changes are only implemented for the individual security systems and not for the airport/airline service provider systems, respectively the check-in system, ticket system, customs passenger system and gate system. Similarly as for the normal case study, the sensitivity analysis simulations use 25 runs of the model in order to get useful outputs.

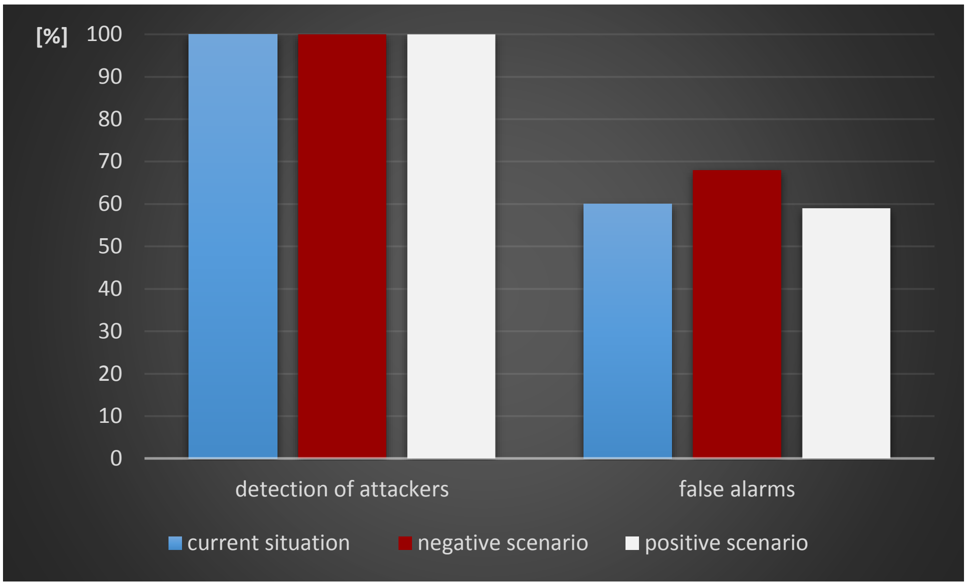

Figure 6.1: Sensitivity analysis results current airport security system

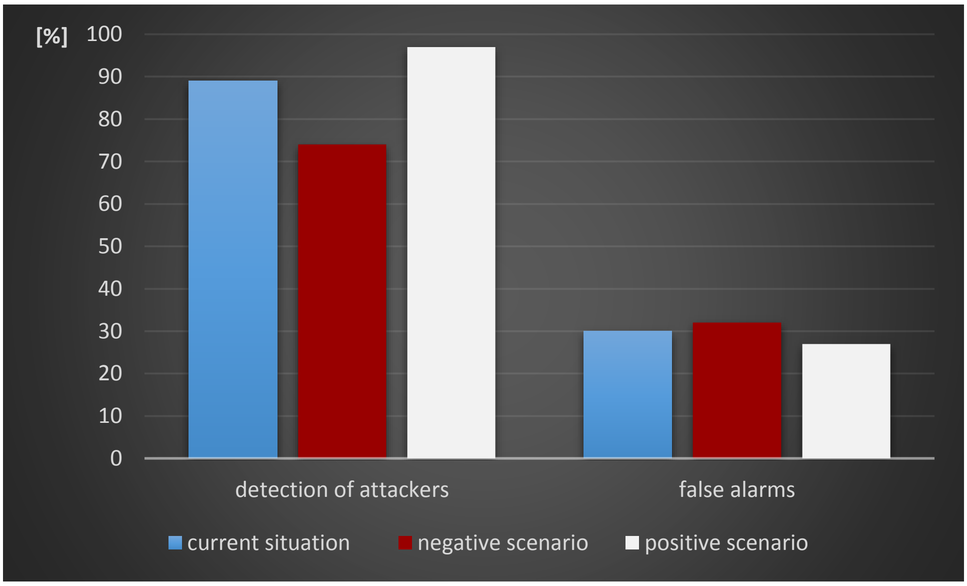

Figure 6.2: Sensitivity analysis results current airport security system without specialized sensors

The differences between the detection rates of the normal, negative and positive scenario are shown in Figure 6.1 and 6.2 for respectively the main current airport security system of this research and the current airport security system without the specialized sensors.
Taking into account the current airport security system constructed for this research, which is the extended airport security system with specialized sensors, the differences made by the sensitivity analysis are well visible for the false positives, but not at all for the attackers. The presence of the multiple types of sensors and the need for only one alarm for the identification of a threat source makes a shift of this proportions in operational performance visible. In the negative case, although the performance of the security system is going down, due to the large variety of sensors there an alarm is easily raised. Above that, the performance of detection of false positives is less as well, which increases this kind of alarms. In the positive scenario all normal passengers with suspicious characteristics were identified as threat source, while completely normal passengers were identified as normal due to the increased performance of detection of false positives.

When considering the current airport security system without the specialized sensors the outputs show less change for the false positives but more for the attackers. Because now less individual security systems are involved, a change in a decision would influence the outcome more. Especially the performance of detection of an attacker shows its downside if there are no other sensors to help out. However, for the normal passengers there are now so little sensors that the probability of a false positive is much less. This can be seen in the negative scenario where the detection of threat sources and drops dramatically and in the positive scenario where the detection of these groups increases relatively much. Normal passengers with suspicious characteristics benefit from this small amount of sensors, as many of them are missed detections instead of being identified as normal passengers. The false positive rates of entirely normal passengers remains relatively the same as the change in detection probability of the operational point was only 0.05.

6.2 Case study 2: integrated airport security system

The second case study uses the new designed airport security system integrated by means of data fusion. Data fusion is already adopted in other domains as an interesting approach to integrate individual systems, especially for security resources. In contrast to the current airport security system the integrated airport security system is designed from scratch using the available security agents. The integrated airport security system is proposed as an alternative for the current airport security system. As it is newly designed it is not the purpose to simulate an existing airport security system. The organizational structure seen in Figure 4.14 and 4.15, the processes, the agents with their capabilities and characteristics described in Section 4.4.5 and the goals established in Section 4.4.6 form the basis for this integrated configuration. Based on these views, the data fusion theory and the security risk scenario constructed in Section 4.3 the ontology for the implementation of the model into the programming software LEADSTO could be set up.

Similarly as for the current airport security system modeled in the first case study, the specific agents have their individual characteristics. The new introduced data fusion system and integrated approach of the way of working of the airport security system effects the behavior of the individual agents. Instead of analyzing and making final decisions themselves all outputs are communicated and linked such that a more thorough risk profile of a passenger can be constructed. Based on this risk profile a final decision about a certain passenger is made by the overall airport security system. In theory it is shown that there are many different approaches to integrate the system, even within the data fusion method. In this thesis the decision data fusion method is used. This means that the decisions made by the individual security systems are used as inputs for the data fusion system and the risk profile of a passenger. Decision data fusion can be implemented using different types of fusion techniques. The most common once are AND and OR logic.

In this second case study the AND and OR logic is combined to integrate the individual agents of the airport security system. Where in the current airport security system only one alarm already triggers action by the overall security system to detain the passenger, now three individual security systems need to identify the passenger as a threat source in order for the passenger to be actually identified as a threat source and detained. Any three security systems can be used for this overall decision. The three individual decisions are coupled using the AND logic, but there are more than three security systems present in the airport security system which means that the OR logic needs to be applied in order to make it possible that any three security systems are used. If the three positive identifications are not met yet the passenger will continue to move through the airport environment until the aircraft is reached.

The same environmental characteristics as in the first case study are set up in this second case study in order to get the same type of outputs. Moreover the data provided in Table 6.1 and 6.2 are applicable for respectively the passenger characteristics and the individual security agents' performance as well. These tables show the main inputs of the model in this security risk scenario and define predominantly the direction of the simulation. Again 25 simulation runs are performed for the integrated airport security system needing any three positive identifications.

Simulation runs	**True positives** *[pax numbers]*	**False positives, with suspicious characteristics** *[pax numbers]*	**False positives, without suspicious characteristics** *[pax numbers]*
1	4, 8, 12	2, 15	
2	4, 8, 12	15	
3	4, 8, 12	15	
5	4, 8, 12	2, 5	
5	4, 12	2, 15	
6	4, 8, 12	2, 15	
7	4, 12	9, 15	
8	4, 8, 12	15	
9	4, 8, 12	15	
10	4, 8, 12	2	
11	4, 8, 12	2, 15	
12	4, 12	2	
13	4, 8, 12	2, 15	
14	4, 8, 12	2, 5, 15	
15	4, 8, 12	15	
16	4, 8, 12	2, 9, 15	
17	4, 8, 12	2, 15	
18	4, 8, 12	15	
19	4, 8, 12	2, 15	7
20	4, 8, 12		
21	4, 12	2	
22	4, 8, 12	5, 15	
23	4, 8, 12	15	
24	4, 12	2, 11, 15	
25	4, 8, 12	2, 15	

Table 6.5: Simulation output integrated security system, any three alarms needed

The outputs for this second case study can be seen in Table 6.5. This first simple integrated airport security system using decision data fusion changes the results dramatically compared to the results of the current airport security system. The fact that information from all the sensors are fused and the identification of suspicious characteristics of three sensors is used pleads many normal passenger free, as it should be, even if they have some suspicious characteristics. Only a small group of normal passengers with many suspicious characteristics are regularly identified and thus presented as false positives. The detection rate of the attackers stays high as well, a missed detection is found only in a rare occasion. This is due to the fact that a missed detection of an individual security system is compensated by fusing the information from all systems present in the airport security system. The use of this integrated configuration looks promises, at least it is for this security risk scenario. However, when analyzing the way of working, the use of three suspicious identified characteristics can shoot the airport security system in its own foot. Although the workload has dropped dramatically due to less false positives, in case of an attacker who does not possess three two suspicious characteristics additionally to the threat object, this attacker would not be found.

With the results of the integrated airport security system in mind it would be interesting to see how this approach would work out when only using the basic configuration without the specialized sensors. To recap, only the individual security systems that belong to the checkpoints which perform the airport processes are used and the surveillance cameras and security officers. This only uses five characteristics that can be measured instead of the 11 in case of the main form of the airport security system. Looking at these characteristics only one attacker has three suspicious characteristics, while the other two have only 2. The information about other personal characteristics is missing as there are no sensors in the environment that can measure the presence of these characteristics. The attackers which are failed to be identified as threat source are missed detections. All normal passengers have either one suspicious characteristic or none. The normal passengers with suspicious characteristics are identified as suspicious however not identified as attacker in this case. In rare occasions it can happen that the suspicious characteristic is not identified, which means that the normal passenger is cleared incorrectly for this characteristic. However this does not influence the continuation of the entire airport security process and the passenger does not have to be mentioned as missed detection as this passenger is not a threat source. The results are shown in Table 6.6.

Simulation runs	**True positives** *[pax numbers]*	**False positives, with suspicious characteristics** *[pax numbers]*	**False positives, without suspicious characteristics** *[pax numbers]*
1	12		
2			
3	12		
5	4, 12		
5	12		
6	12		
7			
8	4, 12		
9	12	6	
10	12		
11			
12	12		
13	12	13	
14	12		
15	12		
16	12		
17			
18	12		
19			
20	4, 12		
21	4		
22			
23	12		
24	12		
25			

Table 6.6: Simulation output integrated airport security system without specialized sensors, any three alarms needed

The sensitivity analysis introduces again the negative and the positive situations that can occur for the airport security system. For the negative case the operational point on the ROC curve for the security systems moves down on this curve, such that a decrease of 0.15 is applied on the probability of detection for true positives and a decrease of 0.05 on the probability of detection for false positives. In the positive scenario the entire ROC curve will again move to the top left corner, introducing an increase of 0.15 on the probability of detection for true positives and a decrease of 0.05 on the probability of detection for the false positives. After again 25 runs of the simulation the outputs are analyzed.

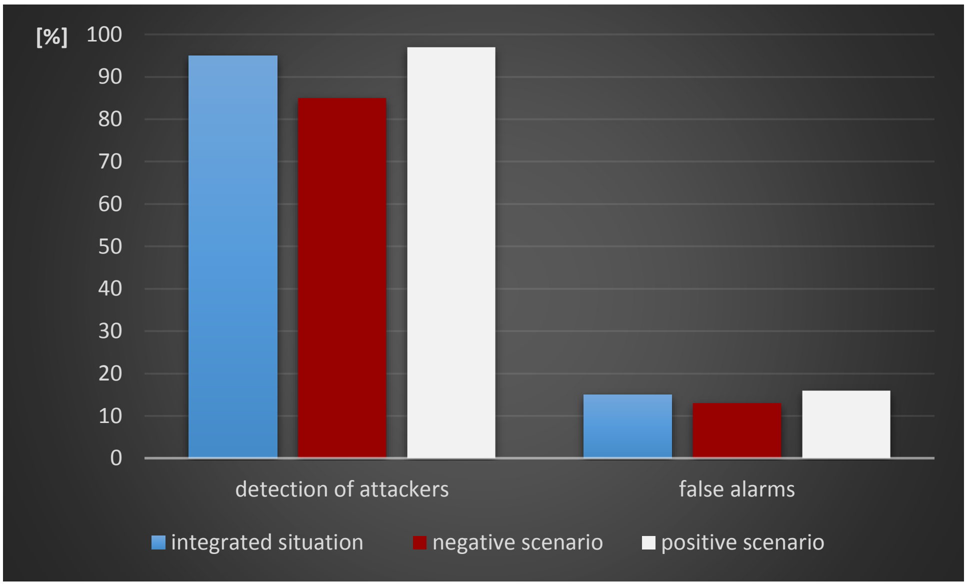

Figure 6.3: Sensitivity analysis results integrated airport security system, any three alarms needed

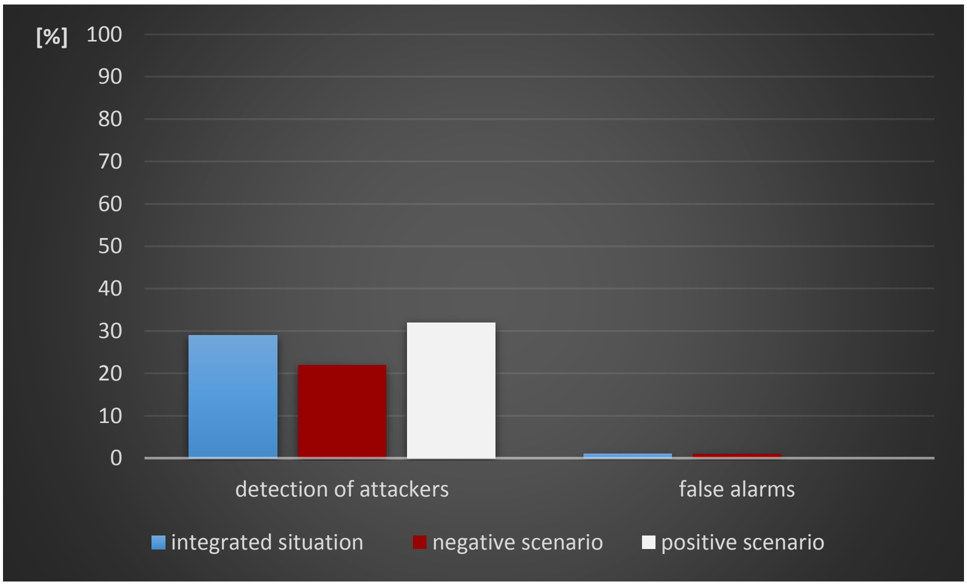

Figure 6.4: Sensitivity analysis results integrated airport security system without specialized sensors, any three alarms needed

The differences between the detection rates of the normal, negative and positive scenario are shown in Figure 6.3 and 6.4 for the main integrated airport security system and the integrated security system without specialized sensors. The sensitivity analysis for the integrated airport security system without the specialized sensors does not provide additional results, it is clear that integration with a constraint on the amount of positive data does not work in case of a small amount of basic sensors. The sensitivity analysis introduces more missed detections in case of the negative scenario, but only by a little and stays the same for a the positive scenario, as there are still three positive identifications of sensors needed while those characteristics are not present. The main finding is thus that for the integration of the current airport security system a wide variety and a decent amount of sensors should be used.

For the main integrated airport security system the sensitivity analysis has more value. Although the results will be in line of expectations after seeing the results in the first case study with the current airport security system. The operational performance for all individual security systems decrease significantly in the negative scenario. Although this leads not to a major increase in missed detections. This happens because the attackers all have more than three characteristics on which they can be identified. Only in case of the normal passengers there is one passenger, number 2, which is not identified occasionally despite having three suspicious characteristics. This passenger is unjustly identified as a normal passenger and is thus a missed detection. The positive scenario does not make a big difference as well concerning the detection of attackers and identification of normal passengers. The percentages of detection of the groups of passengers all lay in the same range.

6.3 Case study 3: weighed integrated airport security system

In reality not every security system gets the same degree of importance. The configuration presented and analyzed in the second case study was nevertheless an interesting configuration to investigate the influence of integration in the airport security system. To implement a more realistic configuration of integration the AND and OR logic of the integrated airport security system will be adjusted in this third case study. The organizational structure, agents present, processes needed to be performed and goals all stay the same for this configuration. The basic framework of the integrated airport security system will be used such that a comparison can be made between the approaches of data fusion adopted. This third case study, using the integrated organizational structure, is performed in order to seek a more optimal configuration than seen in the second case study.

The passenger characteristics and the performance inputs of the individual security systems can be seen again in Table 6.1 and 6.2 respectively. All environmental characteristics remain unchanged once more and the simulation will be executed a total of 25 times.
The AND and OR logic used in decision data fusion are once more both implemented at the same time. A total of three independent alarms raised by individual security systems are needed again for a passenger to be identified as attacker. Compared to the second case study where just any three alarms were allowed now a weighted alternative is proposed. So still three individual security system have to identify a passenger as a threat source. However, if only behaviors or other personal characteristics are taken into account normal passengers who are not actually a threat source can be identified wrongly as positive as well. A threat source is characterized by the possession of one or more threat objects. The threat object can either be carried on the body, in the hand luggage, in the hold baggage or a combination of all of these. In Table 6.1 can be seen how the threat sources carry their threat objects. In order to take into account the need of possession of a threat object in the overall decision of the airport security system after data fusion is performed, the weighted security systems are the individual security systems that directly identify the presence of a threat object. These individual security systems are the passenger scanner, hand-luggage scanner and baggage scanner. Using the AND and OR logic of the decision data fusion approach at least one of three raised alarms which are needed, need to come from an individual security system that directly identifies the threat object. Which means that the passenger scanner, hand-luggage scanner and baggage scanner have a weight

that can be seen as a veto right. If there is no alarm of one of these sensors the passenger will not be identified as an attacker. Additionally, from the other remaining security systems which measure more personal characteristics two should raise an alarm, which ones and when in the environment does not matter.

Simulation runs	**True positives** *[pax numbers]*	**False positives, with suspicious characteristics** *[pax numbers]*	**False positives, without suspicious characteristics** *[pax numbers]*
1	4, 8, 12		
2	4, 8	15	
3	4, 8, 12		
5	8, 12		
5	4, 12	2	
6	4, 8, 12	15	
7	4, 8, 12	5	
8	4, 8		
9	4, 12	2	
10	4, 8, 12		
11	4, 8, 12		
12	4, 12		
13	4, 8	15	
14	4, 8, 12		
15	8, 12	5	
16	4, 8, 12		
17	4, 8	9	
18	4, 8, 12	15	
19	4, 12		
20	4, 8, 12		
21	4, 8	2	
22	12	2	
23	4, 8, 12	15	
24	8, 12		
25	4, 12		

Table 6.7: Simulation output integrated airport security system, three alarms needed weighed configuration

The outputs for this third case study can be seen in Table 6.7. The need for a positive identification of a sensor that directly measures the presence of a threat object has a big influence on the detection performance of the airport security system. Furthermore, the need for two more positive identifications sets up some limitations. The outputs obtained in this case study with the security risk scenario as described for this research looks promising. At least when looking at the performance of the detection of false alarms. The amount of false alarms highly influences the level of service as well. In this configuration the detection of false alarms drops to only 4%, which is a very good measure. However, when looking closely, not all attackers are identified as threat sources. This is due to the fact that the threat object needs to be found for a positive identification. The detection rate for this configuration is only 80%, which might be too low for the likes of an airport security system that needs to identify attackers. The two additional characteristics that need to be identified help the airport security system to raise awareness, but the performance of the individual security system that needs

to identify the threat object remains similar as for the current airport scenario. On the contrary, almost no normal passengers, either with suspicious characteristics or without, are false positives.
When analyzing the results of this configuration it can be noted that it works efficient for a security system with many sensors and threat sources with many suspicious characteristics. This security risk scenario has provided this opportunity to be exploited. However, this approach uses a long-winded method to benefit of the AND logic in the decision data fusion to integrate the airport security system. It can be observed that in a security risk scenario where attacker do not have many suspicious characteristics this integrated configuration does not work, as the attacker would never be identified as threat sources.

For this case study as well a negative and positive scenario can be sketched for the sensitivity analysis. Again a drop of 0.15 in probability of detection of true positives and 0.05 in probability of detection of false positives can be noticed in the negative scenario and an increase of 0.15 in probability of detection of true positives and a decrease of 0.05 in probability of detection of false positives is adopted for the positive scenario. Still the output of the passenger scan, hand luggage scan and baggage scan is weighted with respect to outputs of the other security systems.

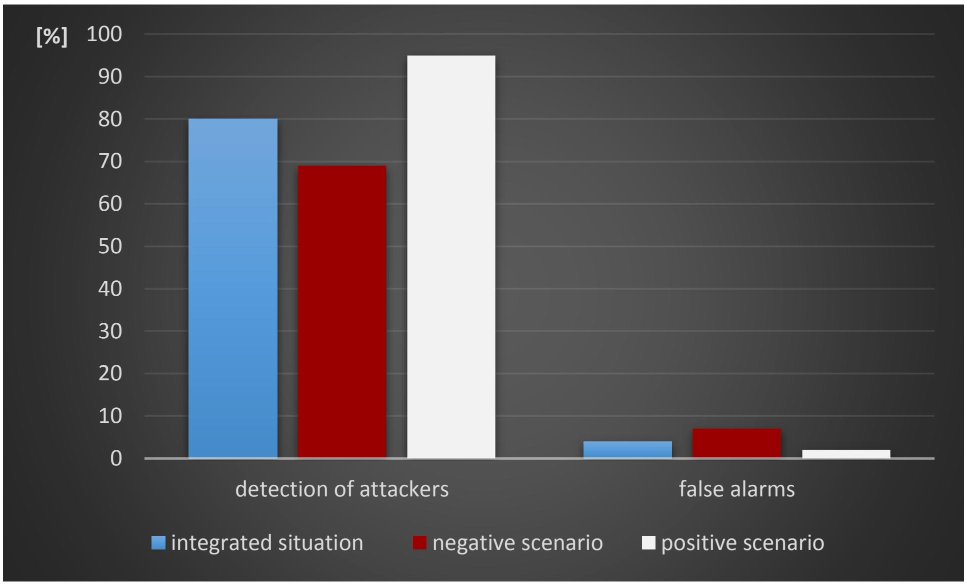

Figure 6.5: Sensitivity analysis results integrated airport security system, three alarms needed weighed configuration

The differences between the detection rates of the normal, negative and positive scenario are shown in Figure 6.5 for the integrated airport security system of this research presented in this case study. Similar to the sensitivity analysis in the previous two case studies is the influence of the negative scenario more negative for the performance and of the positive scenario it increases a bit. The impact of the negative and positive scenario can be seen in the detection of the attackers. A rare additional missed detection in the negative scenario and a solid 100% detection rate of attackers in the positive scenario. The fact that only this group of passengers is mainly influenced by the changes is the use of weighted decisions of the individual security systems directly measuring the presence of a threat object. As normal passengers do not possess a threat object they are not influenced by this change.

6.4 Case study 4: adaptive integrated airport security system

The fourth and last case tries to fully exploit the capabilities of integration using data fusion. The same basics of the new designed airport security system integrated using data fusion and the airport environment will be used for the configuration modeled in this case study. Additionally, the same passenger characteristics, Table 6.1, and individual security system performance characteristics, Table 6.2, are inputs for the model.

The difference in this last case study with respect to the other two case studies based on the integrated airport security system is the operational practice of the integration using data fusion. Data fusion can be used to facilitate the increase in effectively in the most difficult situations, while not putting a threshold on the minimum required positive identifications of a passenger as threat source. The former two case studies however only worked with fixed characteristics of individual security systems, while the data fusion can be applied for more innovative configurations. One of these configurations, which may be an interesting configuration for airports in the future, is analyzed in this case study. An adaptive mechanism in the by decision data fusion integrated airport security system is proposed.

All individual security systems and specialized sensors are present in the airport security system during this case study again. All individual security systems contribute to the efficiency of the overall airport security system and pinpoint a possible threat source before it actually is identified as threat source. The risk profiles set up by the data fusion system play an important role in this configuration. Based on outputs of the individual security systems the risk profiles are updated. These risk profiles then influence the performance characteristics of the individual security systems. A passenger based airport security system is constructed. As explained before the performance characteristics are set up by the manufacturer and a security system has different levels on which it operates. Normally it operates to balance the identification of threat objects and a high speedy throughput. However a security system has certain levels in which it can operate, either more loose or more strict. In this configuration these levels are used based on the degree of threat a risk profile communicates about a certain passenger. All individual security systems work on their normal performance characteristics, however if one of these security systems positively identifies a suspicious characteristic of a passenger the performance characteristics will be positively changed as the risk profile will be updated to a new threat level for this passenger. This positive change can only be achieved on a similar ROC curve. For the first positive identification of a suspicious characteristic an increase of 0.10 in the probability of detection for true positives of all individual security systems is applied while the probability of detection of false positives increase with 0.05. If a second positive identification of a suspicious characteristic is done than an additional increase of 0.05 in the probability of detection for true positives is applied and an increase of 0.05 in the probability of false positives is the results of that as the operational point moves further upward on the same ROC curve. As the individual security systems which directly measure the presence of a threat object are still weighted, a normal passenger should not be affected by the change in operational performance of a scan. Even though a normal passenger had a characteristic that was identified as suspicious, the increased performance of the other sensors should show the harmlessness of this normal passenger.

Simulation runs	True positives *[pax numbers]*	False positives, with suspicious characteristics *[pax numbers]*	False positives, without suspicious characteristics *[pax numbers]*
1	4, 8, 12	9, 15	
2	4, 8, 12	2, 5	7
3	4, 8, 12	2	
5	4, 8, 12		3
5	4, 8, 12	5, 15	6
6	4, 8, 12	2, 13, 15	1
7	4, 8, 12	5, 9, 15	
8	4, 12	2, 11, 14	
9	4, 8, 12	15	
10	4, 8, 12	2, 15	7
11	4, 8, 12	2, 5	6
12	4, 8, 12		3
13	4, 8, 12	5, 11	
14	4, 8, 12	2, 9, 15	
15	4, 8, 12	15	3
16	4, 8, 12	5, 14	
17	4, 8, 12	5, 9, 15	6, 7
18	4, 8, 12	2, 15	10
19	4, 8	2, 11, 15	10
20	4, 8, 12	13, 15	
21	4, 8, 12	5	
22	4, 8	2, 5	6
23	4, 8, 12	2, 14, 15	10
24	4, 8, 12	15	
25	4, 8, 12	2, 5, 9	3

Table 6.8: Simulation output adaptive integrated airport security system

Table 6.8 shows the outputs for this fourth case study. Identical as in the third case study, the need for a positive identification from a system that directly measures the presence of a threat object can be seen in the results. This time the performance of these individual security systems could be increased by using information from other individual security systems. The idea of a missed detection in case of the normal passenger with suspicious characteristics is thus abandoned as there are no fixed boundaries for the identification of a threat source using this configuration. Every new positive identification will raises the operational performance, but only if a threat object is found the passenger is identified as a threat source. This passenger based integrated airport security systems puts thus some pressure on the systems identifying these threat objects. However, the way of working is much more reliable with respect to the configuration in the third case where a minimum of positive identifications is needed.

As can be seen from Table 6.8, the outputs look promising, although relying on the performance of the security systems that directly identify a threat object. A more adequate investigation can be done using all data. Almost all attackers were identified as a threat source in all simulation runs performed. Actually only two could propagate through the airport environment as missed detections, which means that 96% of the attackers could be detected as such. In case of normal passengers though a more reliable results can be obtained. Normal passengers were identified 21% of the time as attacker, which is thus the false alarm rate. This is highly beneficial to the level of service towards all these passengers using the airport environment every day as they do not want to be identified as a threat source. In this configuration normal passengers with suspicious characteristics and entirely normal passengers have the same detection rate as both groups do not have threat objects, which is the driver of a positive identification of a threat source.

Interesting to analyze is what this supposedly increase in security performance means for the performance of the level of service. This adaptive integrated airport security system is used in the analysis of the performance of level of service as this is a trustworthy integrated configuration with probably the best increase in performance of level of security. Similar as in the current airport configuration two actions can be taken when a threat source is identified. Either a passenger is removed from the environment directly after this passenger is identified as an attacker or a second opinion at the place of the positive identification is executed. Which is in this case at one of the security systems that identifies a threat source directly. If a passenger is removed from the environment it influences the rest of the passengers in a similar way as in the current airport configuration. It leads to more time and hassle for the positively identified passenger, but the nominal process time for the checkpoint for other passengers remains the same and respectively less queuing time is witnessed at next checkpoints. The average overall processing time at the checkpoints, so from arriving at the check-in to arriving at the aircraft, taking all passengers in consideration in this case is 3637.5 time units. The processing times for the checkpoints are taken the same as in the current airport security system configuration but do not represent an actual airport configuration. For the case that the passenger needs to undergo a second opinion again is assumed that this second opinion takes as long as the first check performed at a certain checkpoint, which means that the processing time is doubled in case of a positive identification. For the adaptive integrated airport security system however not many passengers are identified as attacker and thus needing a second opinion. This means that the increase in overall processing time and thus possible delay is noticeable but not significant. The average overall processing time increases in this case to 4072.5 time units.

Also for this last case study a sensitivity analysis is performed. The general negative and positive scenarios will be implemented for this adaptive configuration as well. This means that the performance characteristics with which the individual security systems start the simulation will change by the same amount as in earlier case studies. However, the increase in probability of detection based on the adaptivity remain as well. In the positive scenario this can bring a probability of detection above 1, which is impossible. Even probabilities of detection from 1 are highly unlikely. Therefore a boundary is set at a probability of detection of true positives at 0.95 for all security systems if needed.

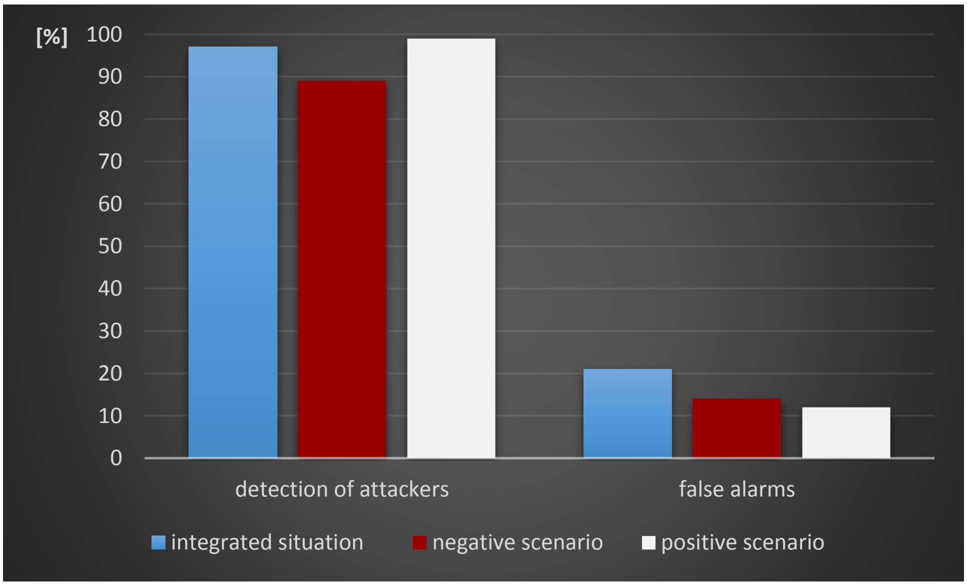

Figure 6.6: Sensitivity analysis results adaptive integrated airport security system

The results for the sensitivity analysis can be seen in Figure 6.6. The change in operational performance in both the negative and positive scenario have the most influence on the main drivers of the identification of a threat source, which are the passenger, hand-luggage and baggage scanners. A decrease in operational performance induces a decrease in detection rates of attackers. However, the decrease is compensated by the adaptive integrated way of working of the airport security system. By using other sensors to increase the knowledge about passengers, the operational performance of these main individual security systems stays at a reasonable level compared to the other case studies. The positive scenario would exceed the boundaries of the operational performance of systems. A performance rate of more than 100% is not feasible and thus the limit of 95% is used. The difference of performance with the normal case is therefore not really noticeable as the performance was already high.

7 Conclusion

The aim of the research is to analyze the performance of the airport security system and to achieve a method that can improve the efficiency of performance. The research is performed by implementing a security risk assessment and following a customized methodology laying out the steps which needs to be taken in order to obtain the knowledge to perform the security risk assessment, build the conceptual model and analyze the modelled case studies. The steps which were performed in order to obtain performance results are set up boundaries of the environment under consideration, analyze possible threats and their perceived risk for vulnerabilities of the airport security system, analyze possible types of attackers and their way of working, define the current airport security system and build a conceptual model, design configurations of a new integrated airport security system and build a conceptual model, implement the conceptual models in the agent-based modeling software and analyze the simulation results. Below the research questions and their conclusions are discussed.

How can the diverse components of the current airport security system be integrated to tackle threats in the airport environment? And how does the integrated airport security system react on specific airport threats?

First of all, the hypothesis was made that the current airport security system could be improved concerning its performance. The current airport security system consists of multiple individual security systems which can measure a wide variety of characteristics. These individual security systems are located throughout the airport environment. The main characteristic of this current airport security system is the stand-alone way of working of these individual security systems. Therefore it is expected that the achieved efficiency is not as high as it could be. A new designed airport security system is proposed. This airport security system has an integrated way of working instead of the stand-alone approach of the current airport security system. An innovative technological system is added to the current airport security system to achieve this integration, called data fusion. Data fusion exists in different forms. Due to the bottom up approach and the lack of real data about the individual security systems, decision data fusion is adopted to integrate the airport security system. Decision data fusion is used in order to exploit the available data from all individual security system in order to establish a more thorough picture of a passenger, such that a better identification can be made. The integration of the airport security system focuses on the communication between the individual security systems and the comprehensiveness of the available security data. Data fusion consist of a data preparation, data association and data estimation step performed by the associated sub-systems and an interface such that the newly fused data can be provided to all systems. Decision outputs from all individual security systems are sent to the data fusion system, there the data is put into a form that enables the actual fusion. A risk profile is made based on the obtained information. This risk profile is updated every time new information arrives at the data fusion system. The risk profile will activate a certain action, clear the passenger or identify the passenger as a threat, from the airport security system due to the data estimation performed.

Different configurations of the integrated airport security system are proposed. These configurations all react in a different way on the threats implemented in the security risk scenario. The first integrated security system makes use of the simplest decision data fusion configuration. Three independent alarms of individual security systems are needed in order for the airport security system to identify the passenger as an attacker. The second airport security system uses a similar approach with three independent alarms which are needed to identify a passenger as an attacker. Although for the second configuration the sensors that identify a threat object directly are weighed with more importance.

From the three independent alarms, at least one of these alarms should come from the passenger scanner, hand-luggage scanner or baggage scanner. The third integrated configuration uses a more adaptive passenger based approach. When an individual security system raises an alarm for a certain passenger, the operational point of the ROC curve changes to a more conservative point, which means that the passenger is checked more thoroughly. Similarly as in the second configuration, if the passenger scan, hand-luggage scan or baggage scan raise an alarm the passenger is identified as an attacker.

What is the difference in performance between the current airport security system working in a more stand-alone way and a new designed integrated airport security system?

A security risk scenario is used to analyze the performance change induced by the integration of the airport security system with respect to the current stand-alone way of working. Attackers with threat object want to propagate through the airport terminal onto the aircraft with their threat object. The results of the performance are therefore only representable for this specific security risk scenario, although the approach and way of detection by the types of airport security systems is similar for other security risk scenarios as well. To get a thorough idea of how an airport security system operates it is chosen to implement the conceptual model in an agent-based modeling approach. The behavior rules, goals and relationships of agents present in the model can be modeled with more precision towards their socio-technical nature than when using common computational methods. Performance of detection is analyzed in two ways, respectively detection of attackers and false alarms. Additionally, as a result of the detection rate of attackers and false positives, missed detections can also be identified.

As a start two forms of the current airport security system were analyzed in the first case study. The main current airport security system with all individual security systems and specialized sensors in place and a basic configuration which uses only a little amount of sensors, which could represent a small to middle sized airport without high-tech devices.

The main current airport security system has a very good performance concerning the detection of attackers. Due to the fact that there is a wide variety of unique sensors present and only one alarm is sufficient to identify a passenger as a threat source, 100% of the attackers were identified as threat source. However, as well 60% of the normal passengers is identified as such. Almost all passengers who had a suspicious characteristic were inappropriately identified as threat source and additionally some passengers without any suspicious characteristics were identified as attacker.

The basic configuration of the current airport security system has a much lower detection rate of false alarms, respectively 30% instead of the 60% in the main current airport security system. However, this is due to the fact that less characteristics can be measured, respectively only 5 instead of at least 11. The decrease in detection of false alarms has a positive outcome on the performance of service. However, a negative outcome of the decrease in sensors used can be seen in the detection of attackers. The detection of attackers dropped from 100% to 89%.

The second case study uses the simplest way of decision data fusion relative to the other configurations. A combination of three individual security systems is needed using AND and OR logic. Any three positive identifications of a suspicious characteristic are accepted to identify a passenger as attacker. Again the two forms are introduces, respectively a main form using all possible individual security systems and specialized sensors and a basic form using only a little amount of different sensors.

When analyzing the main form of the airport security system, the performance of false alarms improves a lot for the integrated airport security system compared to the current airport security system. The detection rate of false alarms dropped from 60% to 14%. On the other hand the performance of the identification of the attackers decreases, from 100% to 95%. The results make this configuration seem like a sound approach to implement, as the decrease in detection of attackers not

too substantial. However, it must have been noted that it only works in this security risk scenario. An attacker could not have been identified if this attacker has less than three suspicious characteristics. Even with just three suspicious characteristics the change of a missed detection of one of these is relatively high compared to the consequences.
This complication can be noticed when looking at the results of the basic integrated airport security system. The amount of characteristics that can be measured drops substantially. Passengers do only rarely have three suspicious characteristics, which leads to only very little false alarms, but also many missed detections. The false alarm detection rate is only 1%, which sounds really convenient. However, the detection rate of attackers is 29%. This detection rate is far too low. This allows to conclude that integration using decision data fusion can only be performed with a wide variety of sensors present in the airport security system.

The third case study continues on the integrated airport security system. In this case however a weighted variant is introduced. Still three independent alarms are needed from individual security systems. However, at least one of these alarms should come from a sensor that directly identifies the threat objects, which are the passenger scanner, hand-luggage scanner and the baggage scanner. After the conclusion that only a wide variety of sensors induce integration in a convenient way, only the main form with all individual security systems and specialized sensors is analyzed for this integrated airport security system.
The need for an alarm raised by a sensor that measures the presence of a threat object directly has a positive influence on the detection of false alarms and thus the level of service. Only 4% of the normal passengers is identified as an attacker. This is a major improvement compared to the current airport security system and the integrated airport security system proposed in the second case study. However, the approach is long-winded due to the limitations of the need to have an alarm raised by two additional sensors on top of the weighted security system that measures the presence of a threat object directly. This results in a decrease of detection of attackers, even more than for the second case. Respectively only 80% of the attackers are identified as such, compared to the 100% and 95% of the current airport security system and the integrated airport security system from the second case study respectively.

The conclusion can be drawn that there is an interesting integrated configuration of the airport security system that can be used to improve the conservative approach of the current airport security system. Especially the second case study proposes an integrated airport security system that, although lower than the current airport security system, has a high detection of attackers in combination with a much lower detection of false positives than the current airport security system. Although a wide variety of sensor should be present in the airport security system to implement integration in a convenient way.

How does an adaptive mechanism of the integrated airport security system influence the performance measures?
In the last case study data fusion is implemented in a more innovative way. Not only the data from all individual systems is fused in order to increase performance of the airport security system, as well adaptivity is introduced. This adaptivity means that the operational performance of certain individual security systems can be changed according to the level of risk the risk profile of a certain passenger gives. In such a way no constraints on the amount of sensors giving a positive identification is implemented, as was the case for the integrated airport security system in the third case study. This configuration of the airport security system can be seen as a more passenger based integrated airport security system. A passenger is still only really identified as attacker by the sensors that directly measure the presence of a threat object, such as the passenger scanner, hand-luggage scanner and the baggage scanner. The decisions of the other individual security systems are used to update the risk profile of the specific passenger.

The results are promising. A decrease in the false alarm rate can be found compared to the current airport security system, 60%, and the integrated airport security system used in the second case study, 30%. The detection rate of false alarms is found to be 21%. Moreover, this configuration has a better performance of detection of attackers than all other integrated airport security system proposed, with a percentage of 96% it outperforms the integrated airport security system used in the second case study, 95%, and used in the third case study 80%. The results of the integrated airport security system using the adaptive mechanism thus are very positive. Compared to the conservative current airport security system the detection of attackers is still high, where the detection of false alarms is much more convenient. Additionally, compared to the other integrated airport security system configurations the combination of detection of attackers and detection of false alarms is the most convenient, as both detection rates show really positive values, as in the other cases either one of the two performance measures showed a weakness.
Although the difference is not that obvious because of the passengers present in this security risk scenario. If there would have been more attackers with less than three suspicious characteristics the difference would have been more striking. The same applies for the second case, although in the security risk scenario used there is confined.

A conflict in security performance measures arises when taking into account security and level of service. In general a higher level of security means a lower level of service. In case of the airport security system this can be translated into time. Respectively the time a certain passenger is being processed or the time other passengers experience delay. The current airport security system has many false positives which has a negative influence on the level of service. Two different actions could be performed concerning the passengers whom were identified as attacker. The passengers are either taken out of the environment of the airport processes or a secondary check is performed at the location of the positive identification. The two forms are analyzed and compared between the current airport security system and the adaptive integrated airport security system, as this is the most promising integrated airport security system configuration. The time units implemented are used in order to show the difference between the two configurations and not to simulate a real life airport configuration.
When the passenger is taken out of the environment, the other normal passengers do not experience any delay on the nominal time it should take to process passengers. Even less delay during queuing is noticed further on in the airport environment as less passengers are present. However the passenger which is taken out experiences a lot of delay and hassle. The current airport security system has an average overall processing time of 2775 time units, while the adaptive integrated airport security system has an average overall processing time of 3637.5 time units. This is an increase of 31% in time in case of the adaptive integrated airport security system. This increase can be explained by the decrease in false positives in this integrated configuration.
A more real life approach to positive identifications however is the use of a second opinion. If a second opinion needs to be performed at the location of the positive identification, the processing time for the second opinion is assumed as much as the processing time of the first check. This means that the processing time is assumed to be doubled for the particular check for that specific passenger. A normal passenger whom is positively identified as an attacker is assumed to be declared a normal passenger after a second opinion, which means that the passenger can continue to move through the airport environment. An attacker is assumed to be still identified as an attacker and taken out of the environment. In this case the average overall processing time for the current airport security system increases to 4545 time units, while the average overall processing time of the adaptive integrated airport security system increases to 4072.5 time units. Comparing the times of the current and adaptive integrated airport security systems it means that a decrease of just above 10% is found in favor of the adaptive integrated airport security system. This makes an integrated approach for the airport security system very interesting to consider.

It must be noted that there is no such thing as 100% detection rate at all times. If the simulation runs would be performed indefinitely, even in case of the main current airport security system used in the first case study a missed detection of an attacker would occur. No matter what configuration is used, how the airport security system is integrated or how many sensors are used, in the best case there is always a very little probability that an attacker will get through. However, when putting reliable security precautions in place as in the adaptive integrate configuration in the fourth case study this probability can be brought back to nihil proportions.

In general, the way of working of the adaptive integrated airport security system is more trustworthy. It does not matter how many suspicious characteristics a passenger has, but if a passenger possess one it will be used to update the risk profile and increase surveillance on this passenger. If a passenger would not possess more suspicious characteristics, then a similar detection probability as the in a current stand-alone way of working is applicable. This increases both the performance of detection of attackers and normal passengers. The second case scenario showed a good performance of detection of attackers as well, at the cost of more false positives though. However, in order to build in a buffer, the adaptive configuration and the integrated configuration needing a certain amount of positive identifications could be combined. A more conservative approach will then be used for the detection of attackers, but the detection of false positives is still much better than compared to the current stand-alone way of working of the airport security system.

8 Recommendations

This research performed in this thesis, is an exploratory research and makes use of alternative approaches than commonly applied. The results of this research are interesting, however the exploratory nature induces the opportunity for recommendations for future studies continuing on this subject. Below an overview is given of the main recommendations that can contribute to future research:

Study additional and more comprehensive security risk scenarios

In this research a certain security risk scenario has been established. This security risk scenario formed one of the boundaries in the framework of the implementation of the airport security system models. A security risk scenario however consists of many different aspects. The environmental boundaries, threat sources, threat objects and the way of executing the attack are all described in this security risk scenario. Furthermore, the side of the defender is described as well by means of the actors, their abilities, their theoretical performance and their vulnerabilities.

For this research the entire airport environment with its threats was too broad. Only the airport terminal with its security and service checkpoints and the belonging security systems is taken into consideration, while the airport environment is much larger and thus there is more variety in the possible ways of performing an attack. For the attacker and the threat object only the most prominent and dangerous case in the current world is introduced in the research. Every other type of attacker and threat object can be seen as a research on itself. All these types of attackers and threat objects however can be present in the airport environment and thus needs the airport security system to be ready to identify these as well.

Combine LEADSTO software with common computational programming software

LEADSTO is a very useful tool in order to model the behavior of individual agents and the relationships between them. For the research of the interaction between attackers and defenders this software can illustrate a more real world representation. The downside of the LEADSTO tool was found to be the time consuming implementation of agents. Because each agent is considered to be unique they needed to be implemented one by one. However, in case of an airport environment there are many agents who are relatively similar and are normally present in large quantities, for example the passengers. Common computational software programs give the opportunity to model agents, although without behavioral rules, in large quantities at the same time. Merging an agent-based software program with a common computational software program allows to benefit from the best of both worlds.

Study the implementation of more types of data fusion or other integration methods

That integration of the airport security system can lead to interesting results compared to the current stand-alone way of working of the airport security system can be seen. However, alongside the study of all possible security risk scenarios, the implementation of all possible types of data fusion or other integration methods should be analyzed as well. Investigating these other possible approaches result in more essential insight on which type of approach suits the airport security system best and in which security risk scenario. From a perspective of using data fusion the parametric variant could be very interesting. For this type of data fusion however is more detailed information about the individual security systems needed. However, also other configurations of decision data fusion would already be interesting to analyze, as the configurations in this research could be improved as well. For instance the combination of configurations used in this research could lead to a more conventional approach for the identification of attackers, but still lead to a big reduction in false alarms. Furthermore, a study should be performed to other approaches of integration than data fusion.

Use other types of probabilities as input for the performance of individual security systems
Investigate the use of different probability density functions that generate the performance of the individual security systems. In this research the ROC curve was followed, although in an exploratory way as no manufacturing data was known. Real ROC curves for the current security systems or the use of different probability density functions for the current and future equipment can give better insight on which method approaches the real airport security system performance and what is needed to raise the performance of the airport security system.

Extend the characteristics and capabilities of the agents and environment in the model
Agents can be very complex. Human beings and technical systems both have their unique characteristics which can be exploited in agent-based modeling as can be seen in this research. However this is only the beginning. Assumptions are made in order to simplify the implementation of the security risk scenario. This has no influence on the outputs as these can still be used to compare the different configurations. However there are more characteristics and capabilities that can be used in future research in order to get a more comprehensive picture of how the airport environment actually operates. Many behavioral characteristics are given in an abstract way, although there are certain degradations of behavior and detailed descriptions of unique types of behavior. Similarly, the way the agents communicate and what type of information they provide to each other can be described in more detail. The environment plays an important role as well. Where the environment now is fixed to the boundaries of the airport terminal and the continuation of the airport processes it would be interesting to see how agents would behave if movement was entirely free, as it is in the real world. Moreover, one of the most interesting aspects of human beings is learning. Learning can be implanted in agent-based methods as well. Especially when analyzing a security risk scenario for a large time period learning for both the attacker agents and defender agents should be considered to get an actual view of the performance of the airport security system.

Extend the adaptivity possibilities of the airport security system
Adaptivity is briefly touched in this research. However it seems to be a very interesting way of working for the airport security system. The adaptivity of the airport security system needs to work in connection with an integration system, otherwise an adaptive approach would be randomly generated. The possible usage of adaptivity could be in the addition of certain individual security systems when the risk profile of a passenger meets a certain level. These individual security systems were not used before for other passengers, but are present in the airport environment. The adaptive use of security systems could lower the exhaustiveness of the tasks that the integration system needs to perform as less data is communicated in a normal situation. Furthermore, the adaptivity could lead to a higher throughput of the overall airport security system for passengers and to a higher efficiency in the accomplishment of the performance goals.
Another way of adaptivity can be found in the sharing of data between the individual security systems. A gap in the performance nowadays could be the lack of identification of threat objects that consists of multiple components. These components form apart from each other no risk and are not identified as threat object by the airport security system, however built together the components form a threat object. Integration of the airport security system could tackle this gap. Information about threat objects and components of threat objects are stored and when different security systems find all components the identification of a threat object is raised.

Implement the model into the real world in order to see the real effects

This research can be seen as an exploratory research. The outputs are useful to compare and discuss the different configurations based on a certain security risk scenario. However, usually when implementing systems into the real world, how well the model can simulate this real world or not, there are always differences that influence the results. Therefore it is wise to implement an integrated airport security system after the conceptual design and modeling phase in a real world scenario.

Bibliography

[1] E. Albrechtsen, "Security vs. Safety," Norwegian University of Science and Technology, Trondheim, 2003.

[2] TNO, "Deviant Behaviour," TNO, The Hague, 2014.

[3] G. Blalock, V. Kadiyali and D. H. Simon, "The impact of post-9/11 airport security measures on the demand for air travel," *The Journal of Law and Economics,* vol. 50, no. 4, pp. 731-755, 2007.

[4] P. Bouvier, "Airport Infrastructure Security Towards Global Security: A holistic security risk management approach," Thales Group, Velizy, 2008.

[5] Committee on Assessment of Security Technologies, "Fusion of Security System Data to Improve Airport Security," The National Academies Press, Washington D.C., 2007.

[6] M. Cole and A. Kuhlmann, "A scenario-based approach to airport security," *Futures,* vol. 44, no. 4, pp. 319-327, 2012.

[7] D. Landoll, The security risk assessment handbook: A complete guide for performing security risk assessments, Auerbach Publications, Tayler & Francis Group: Boca Raton, 2006.

[8] L. Magalhaes, "Depecting Airport Processes: Definitions, Activities and Modeling," Instituto Superior Tecnico Universidade de Lisboa, Lisbon, 201.

[9] A. Sharpanskykh, "On Computer-Aided Methods for Modeling and Analysis of Organizations," Vrije Universiteit Amsterdam, Amsterdam, 2008.

[10] K. Bite, "Improving on Passenger and Baggage Processes at airports with RFID," *Sustainable Radio Frequency Identification Solutions,* pp. 121-138, 2010.

[11] M. Gatersleben and S. van der Weij, "Analysis and simulation of passenger flows in an airport terminal," in *Simulation Conference Proceedings (Volume 2)*, Phoenix (AZ), 1999.

[12] M. Schultz and H. Fricke, "Managing Passenger Handling at Airport Terminals," in *Ninth USA/Europe Air Traffic Management Research and Development Seminar*, Berlin, 2011.

[13] J. Setti and B. Hutchinson, "Passenger Terminal Simulation Model," *Journal of Transportation Engineering,* vol. 120, no. 4, pp. 517-535, 1994.

[14] H. Jim and Z. Chang, "An Airport Passenger Terminal Simulator: a planning and design tool," *Simulation Practice and Theory,* vol. 6, pp. 387-396, 1998.

[15] G. Guizzi, T. Murino and E. Romano, "A Discrete Event Simulation to Model Passenger Flow in the Airport Terminal," *Mathematical Methods and Applied Computing,* vol. 2, pp. 427-434, 2009.

[16] D. Curcio, F. Longo, G. Mirabelli and E. Pappoff, "Passengers' Flow Analysis and Sceurity Issues in Airport Terminals using Modeling & Simulation," in *Proceedings 21st European Conference on modelling and Simulation*, Prague, 2007.

[17] G. H. Frederickson and T. R. LaPorte, "Airport Security, High Reliability, and the Problem of Rationality," *ASPA Public Administration Review,* vol. 622, no. 1, pp. 33-43, 2002.

[18] N. Ashford, P. Coutu and J. Beasley, Airport Operations, Whitby: McGraw-Hill Ryerson Lrd., 2013.

[19] S. Appelt, R. Batta, L. Lin and C. Drury, "Simulation of passenger check-in at a medium sized US airport," in *Proceedings of the 39th conference on Winter simulation* , Washington D.C., 2007.

[20] G. Mason and N. Barker, "Buy now fly later: an investigation of airline frequent flyer programmes," *Elsevier, Tourism Management,* vol. 17, no. 3, pp. 219-223, 1996.

[21] M. Paul, S. Haque and S. Chakraborty, "Human detection in surveillance videos and its applications," *EURASIP Journal on Advances in Signal Processing,* vol. 176, pp. 1-16, 2013.

[22] D. Lyon, "Surveillance, Security and Social Sorting Emerging Research Priorities," *International Criminal Justice Review,* vol. 17, no. 3, pp. 161-170, 2007.

[23] Amsterdam Schiphol Airport, "Airport Security; Security Scan," Schiphol Group, Amsterdam, 2015.

[24] A. Burns, J. McDermid and J. Dobson, "On the meaning of safety and security," *The Computer Journal,* vol. 35, no. 1, pp. 3-15, 1992.

[25] T. Aven, "On how to define, understand and describe risk," *Reliability Engineering, System Safety,* vol. 95, no. 6, pp. 623-631, 2010.

[26] O. Milbredt and J. Strer, "Key performance indicator for security measurement at airports," German Aerospace Center (DLR), Braunschweig, 2015.

[27] P. Chawdhry, "Risk modeling and simulation of airport passenger departures process," in *Simulation Conference (WSC), Proceedings of the 2009 Winter*, Austin (TX), 2009.

[28] R. Schmittling and A. Munns, "Performing a security risk assessment," *ISACA Journal,* vol. 1, pp. 1-7, 2010.

[29] COSO, "Enterprise RIsk Management - Integrated Framework," COSO, 2014.

[30] S. Kaplan and B. Garrick, "On the quantitative definition of risk," *Risk Analysis,* vol. 1, no. 1, pp. 11-27, 1981.

[31] S. Houmb, "Decision support for choice of security solution: The aspect-oriented risk driven development framework," Norwegian University of Science and Technology, Trondheim, 2007.

[32] J. Lowder, "The difference between quantitative and qualitative risk analysis and why it matters," in *Risk Analysis*, 2008.

[33] E. Zambon, S. Etalle, R. Wieringa and P. Hartel, "Model-based qualitative risk assessment for availability of IT infrastructures," *Software and systems modeling,* vol. 10, no. 4, pp. 553-580, 2010.

[34] G. Stoneburner, A. Goguen and A. Feringa, "Risk Management Guide for Information Technology Systems," National Institute of Standards and Technology, Gaithersburg (MD), 2002.

[35] Department of Homeland Security, "Risk Management Fundamentals," U.S. Department of Homeland Security, 2011.

[36] Standards Australia & New Zealand, "Risk management," Australian / New Zealand Standard, 2004.

[37] M. Lund, B. Solhaug and K. Stolen, "Model-driven risk assessment: the CORAS approach," Springer-Verlag, Oslo, 2002.

[38] ANSSI, "Ebois 2010 - Expression of needs and identification of security objectives," Agence Nationale de la Securite des Systemes d'Information, Paris, 2010.

[39] NEN, "NEN-ISO 31000 Risk Management - Principles and Guidelines," NEN, 2009.

[40] J. Lopez, R. Setola and S. Wolthusen, Critical Infrastructure Protection: Advances in Critical Infrastructure Models, Analysis and Defense, Springer Sceince & Business Media, 2012.

[41] R. Lazarick, "Airport vulnerability assessment: a methodology evaluation," in *IEEE 33rd Annual International Carnahan Conference on Security Technology*, Madrid, 1999.

[42] D. Porello, F. Setti, R. Ferrario and M. Cristani, "Multiagent Socio-Technical systems: An ontological approach," Institute of cognitive sciences and technologies, Verona, 2011.

[43] M. G. Stewart and J. Mueller, "Cost-benefit analysis of airport security: Are airports too safe?," *Journal of Air Transport Management,* vol. 35, pp. 19-28, 2014.

[44] J. Reason, "The contribution of latent human failures to the breakdown of complex systems," *Philosophical Transactions of the Royal Society of London,* vol. 327, no. 1241, pp. 475-484, 1990.

[45] N. Distefano and S. Leonardi, "Risk Assessment procedure for civil airport," *International Journal for Traffic and Transport Engineering,* vol. 4, no. 1, pp. 62-75, 2013.

[46] J. Leson, "Assessing and Managing the Terrorism Threat," U.S. Department of Justice, Office of Justice Programs, Washington D.C., 2005.

[47] V. Dumbrava, "Using Probability - Impact Matrix in Analysis and Risk Assessment Projects," *Journal of Knowledge Management,* pp. 76-96, 2013.

[48] P. Wu and K. Mengersen, "A review of models and model usage scenarios for an airport complex system," *Transportation Research Part A: Policy and Practice,* vol. 47, pp. 124-140, 2013.

[49] J. Ladyman, J. Lambart and K. Wiesner, "What is a complex system?," *Euro Journal Philosophy of Science,* vol. 3, pp. 33-67, 2013.

[50] L. Rocha, "Complex systems modeling: using metaphors from nature in simulation and scientific models," Computing, Information and Communications Division, Los Alamos National Laboratory, Los Alamos, 1999.

[51] A. Sharpanskykh and H. Blom, "Agent-based Safety Risk Analysis, AE4448 Lecture 2," Delft University of Technology, Delft, 2013.

[52] N. Gilbert, Agent-based models; Quantitative Applications in the Social Sciences, SAGE Pubblications, 2008.

[53] R. Coyle, System Dynamics Modelling: A practical approach, Volume 1, Chapman & Hall/CRC Press, 1996.

[54] P. Clemens and R. Simmons, Systems Safety and Risk management, NIOSH, 1998.

[55] D. Furno, V. Loia and M. Verniero, "A fuzzy cognitive situation awareness for airport security," *Control and Cybernatics,* vol. 39, no. 4, pp. 959-982, 2010.

[56] NASA, Fault Tree Handbook with Aerospace Applications, NASA Office of Safety and MIssion Assurance, 2002.

[57] S. Bradley, A. Hax and T. Magnanti, Applied Methematical Programming, Addison-Wesley, 1977.

[58] S. Yan and C. Chang, "A network model for gate assignment," *Journal of Advanced Transportation ,* vol. 32, no. 2, pp. 176-189, 1998.

[59] G. Lovas, "Modeling and simulation of pedestrian traffic flow," *Transportation Research Part B: Methodological,* vol. 28, no. 6, pp. 429-443, 1994.

[60] A. Armstrong-Wright, Critical path method: introduction and practice, Longman Group Ltd., 1971.

[61] I. Ben-Gal, "Bayesian Networks," in *Encyclopedia of Statistics in Quality & Reliability* , Oxford, John Wiley & Sons, 2007.

[62] L. Chen, "Agent-based modelling in urban and architectural research: a brief literature review," *Frontiers of Architectureal Research,* vol. 1, pp. 166-177, 2012.

[63] M. Wooldridge and N. Jennings, "Intellifent Agents: Theory and ptactice," *The Knowledge Engineering Review,* vol. 10, no. 2, pp. 115-152, 1995.

[64] E. Bonabeau, "Agent-based modeling: methods and techniques for simulating human systems," *Proceedings of the National Academy of Sciences of the United States of America,* vol. 99, no. 3, pp. 7280-7287, 2002.

[65] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya and Q. Wu, "A survey of game theory as applied to network security," in *Proceedings of the 43rd Hawaii International Conference on System Sciences*, Honolulu, 2010.

[66] J. Pita, M. Jain, F. Ordonez, C. Portway, M. Tambe, C. Western, P. Paruchuri and S. Kraus, "Using Game Theory for Los Angeles Airport Security," *AI Magazine,* vol. 30, no. 1, pp. 43-57, 2009.

[67] V. Bier, "Game-theoretic and Reliability Methods in Counterterrorism and Security," *CREATE Homeland Security Center, published articles and papers,* vol. 136, pp. 17-28, 2005.

[68] P. Adey, "Surveillance at the Airport: Surveilling Mobility/Mobilising Surveillance," *SAGE Journals, Environment and Planning A,* vol. 36, no. 8, pp. 1365-1380, 2004.

[69] D. H. Harris, "How to really improve airport security," *SAGE Journals, Ergonomics in Design,* vol. 10, no. 1, pp. 17-22, 2002.

[70] TASS project team, "TASS: Total Airport Security System," CORDIS, 2010.

[71] Intergraph, "Integrated Airport Security," Intergraph, 2012.

[72] H. Jimenez, I. Stults and D. Mavris, "A Morphological Approach for Proactive Risk Management in Civil Aviation Security," in *47th AIAA Aerospace Sciences Meeting Including the New Horizons Forum and Aerospace Exposition*, Orlando (FL), 2009.

[73] L. Guerra, T. Murino and E. Romano, "Airport system analysis: a probabilistic risk assessment model," *International Journal of Systems Applications, Engineering & Development,* vol. 2, no. 2, pp. 52-65, 2008.

[74] F. Rambach, "Taxonomies of Attackers," University of Auckland, 2015.

[75] M. W. Nance, Terrorist Recognition Handook, Boca Raton: CRC Press, Taylor & Francis Group, 2014.

[76] TSA, "Checklist terrorist," TSA, Washington D.C., 2013.

[77] D. Georgakopoulos, M. Hornick and A. Sheth, "An overview of workflow management: From process modeling to workflow automation infrastructure," *Distributed and Parallel Databases,* vol. 3, no. 2, pp. 119-153, 1995.

[78] W. R. Scott, Organizations: rational, natural and open systems, Upper Saddle River (NJ): Prentice Hall International Inc., 1998.

[79] L. Donaldson, The Contingency Theory of Organizations, London: SAGE, 2001.

[80] P. Bresciani, P. Giorgini, F. Giunchiglia, J. Mylopoulos and A. Perini, "Tropos: An agent-oriented software development methodology," *Journal of Autonomous Agent and Mulit-Agent Systems,* vol. 8, no. 3, pp. 203-236, 2004.

[81] J. Ferber and O. Gudknecht, "A meta-model for the analyis and design of organizations in multi-agent systems," in *Proceedings of 3rd International Conference on Multi-Agent Systems*, 1998.

[82] B. Curis, M. I. Kellner and J. Over, "Process modeling," *Communications of the ACM,* vol. 35, no. 9, pp. 75-90, 1992.

[83] C. Rolland, "A comprehensive view of process engineering," *Advanced Information Systems Engineering,* vol. 1413, pp. 1-24, 1998.

[84] M. Dowson, "Iteration in the Software Process," in *Proceedings of the 9th International Conference on Software Engineering*, 1998.

[85] W. R. Scott, Institutions and organizations, Thousand Oaks: SAGE , 2001.

[86] D. L. Hall and J. Llinas, "An introduction to multisensor data fusion," *Proceedings of the IEEE,* vol. 85, no. 1, pp. 6-23, 1997.

[87] A. K. Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 14, no. 1, pp. 4-20, 2004.

[88] M. Liggins, D. Hall and J. Llinas, Handbook of Multisensor Data Fusion: Theory and Practice, CRC Press, 2008.

[89] J. Hanley and B. J. McNeil, "The meaning and use of the area under a receiver operating characteristic curve," *RSNA Radiology,* vol. 143, no. 1, 1982.

[90] R. Lippert and D. O'Connor, "Security Assemblages: Airport Security, Flexible Work, and Liberal Governance," *SAGE Journals, Alternatives,* vol. 28, pp. 331-358, 2003.

[91] C. J. Cohen, K. A. Scott, M. J. Huber, S. C. Rowe and F. Morelli, "Behavior recognition architecture for surveillance applications," in *Applied Imagery Pattern Recognition Workshop*, Washington D.C., 2008.

[92] M. L. Tam, W. H. K. Lam and H. P. Lo, "Modeling air passenger travel behavior on airport ground access mode choices," *Transportmetrica,* vol. 4, no. 2, pp. 135-153, 2008.

[93] B. Hasisi and D. Weisburd, "Going beyond ascribed identities: the importance of procedural justice in airport security screening in Israel," *TOC,* vol. 45, no. 4, pp. 867-892, 2011.

[94] D. L. Wilson, "Use of modeling and simulation to support airport security," *IEEE Aerospace and Electronic Systems Magazine,* vol. 20, no. 8, pp. 3-6, 2005.

[95] A. Sharpanskykh and J. Treur, "Verifying Interlevel Relations within Multi-agent Systems," in *Proceedigns of the 17th European Conference on Artificial Intelligence*, Riva del Garda, 2006.

[96] A. Oberschelp, "Order sorted predicate logic," *Sorts and Types in Artificial Intelligence,* pp. 7-17, 2005.

[97] M. Manzano, Extensions of First Order Logic, Cambridge University Press, 1996.

[98] M. Iglewski and J. Mincer-Daszkiewics, "Internal design of modules specified in the trace assertion method," *Science of Computer Programming,* vol. 28, pp. 139-170, 1997.

[99] T. Bosse, C. M. Jonker, L. van der Meij and J. Treur, "A language and environment for analysis of dynamics by simulation," *International Journal of Artificial Intelligence Tools,* vol. 16, pp. 435-464, 2007.

[100] E. Casey, "Determining Intent - Opportunistic vs Targeted Attacks," *Computer Fraud & Security,* vol. 2003, no. 4, pp. 8-11, 2003.

[101] A. Kirschenbaum, "The cost of airport security: the passenger dilemma," *Journal of AIr Transport Management,* vol. 30, pp. 39-45, 2013.

[102] K. H. van Dam, I. Nikolic and Z. Lukszo, Agent-Based Modelling of Socio-Technical Systems, Springer, 2013.

[103] S. Franklin and A. Graesser, Is it an agent or just a program? A taxonomy for autonomous agents, Wooldridge, 1996.

[104] T. E. Burns and G. M. Stalker, "The management of innovation," University of Illinoins , 2009.

Appendix A

This appendix describes the formal ontology that was developed for the airport security system case studies. Section 5.2 already describes the main principles of the formal ontology and shows examples of the dynamic properties present. This appendix shows a more comprehensive view of the LEADSTO model used.

Below the rules for the checkpoint of the security check is provided in more detail. All the communication and actions of the agents present in this part of the airport environment can be observed. The dynamic properties are constructed with the sorts, elements and predicates described in Tables 5.1 and 5.2. All other checkpoints work in a similar way regarding communication and actions, however due to clarity reasons those rules are not provided here. The elements in the predicates can be changes for the concerned agents whom need to be active and objects under investigation.

Start_process(passenger, passenger) & is_at(security_officer1, security_check) → input(security_officer1)|start_process(passenger, passenger)

Input(security_officer1)|start_process(security_check, passenger) → output(security_officer1)|communication(security_check, security_officer1, passenger, ask, ticket, passenger)

Output(security_officer1)|communication(security_check, security_officer1, passenger, ask, ticket, passenger) → input(passenger)|communication(security_check, security_officer1, passenger, ask, ticket, passenger)

Input(passenger)|communication(security_check, security_officer1, passenger, ask, ticket, passenger) & has(passenger, ticket, state_object) → output(passenger)|communication(security_check, passenger, security_officer1, provide, ticket, passenger)

Output(passenger)|communication(security_check, passenger, security_officer1, provide, ticket, passenger) → input(security_officer1)|communication(security_check, passenger, security_officer1, provide, ticket, passenger)

Input(security_officer1)|communication(security_check, passenger, security_officer1, provide, ticket, passenger) → output(security_officer1)|communication(security_check, security_officer1, passenger, accept, ticket, passenger)

Output(security_officer1)|communication(security_check, security_officer1, passenger, accept, ticket, passenger) & is_at(access_sensor, security_check) → input(passenger)|communication(security_check, security_officer1, passenger, accept, ticket, passenger) & output(security_officer1)|communication(security_check, security_officer, access_sensor, provide, ticket, passenger)

output(security_officer1)|communication(security_check, security_officer1, access_sensor, provide, ticket, passenger) → input(access_sensor)|communication(security_check, security_officer1, access_sensor, provide, ticket, passenger)

input(access_sensor)|communication(security_check, security_officer1, access_sensor, provide, ticket, passenger) → output(access_sensor)|communication(security_check, access_sensor, security_officer1, accept, ticket, passenger) output(access_sensor)|communication(security_check, access_sensor, security_officer1, accept, ticket, passenger) → input(security_officer1)|communication(security_check, access_sensor, security_officer1, accept, ticket, passenger) & perform_check(security_check, access_sensor, ticket, passenger)

perform_check(security_check, access_sensor, ticket, passenger) & present(passenger_system, ticket, passenger) & has(passenger, ticket, valid) → **prob.** Output(access_sensor)|perform(clear, security_check, ticket, passenger) v **otherwise** output(access_sensor)|perform(alarm, security_check, ticket, passenger)

perform_check(security_check, access_sensor, ticket, passenger) & present(passenger_system, ticket, passenger) & has(passenger, ticket, invalid) → **prob.** Output(access_sensor)|perform(alarm, security_check, ticket, passenger) v **otherwise** output(access_sensor)|perform(clear, security_check, ticket, passenger)

perform_check(security_check, access_sensor, ticket, passenger) & not present(passenger_system, ticket, passenger) & has(passenger, ticket, state_object) → **prob.** Output(access_sensor)|perform(alarm, security_check, ticket, passenger) v **otherwise** output(access_sensor)|perform(clear, security_check, ticket, passenger)

output(access_sensor)|perform(alarm, security_check, ticket, passenger) → input(security_officer1)|observe(alarm, security_check, ticket, passenger)

input(security_officer1)|observe(alarm, security_check, ticket, passenger) → internal(security_officer1)|belief(alarm, security, check, ticket, passenger)

internal(security_officer1)|belief(alarm, security_check, ticket, passenger) → arrest(security_check, passenger)

output(access_sensor)|perform(clear, security_check, ticket, passenger) → input(security_officer1)|observe(clear, security_check, ticket, passenger)

input(security_officer1)|observe(clear, security_check, ticket, passenger) → internal(security_officer1)|belief(clear, security, check, ticket, passenger)

internal(security_officer1)|belief(clear, security_check, ticket, passenger) → output(security_officer1)|cleared(security_check, passenger, access) & output(security_officer1)|communication(security_check, security_officer1, passenger, clear, ticket, passenger)

output(security_officer1)|communication(security_check, security_officer1, passenger, clear, ticket, passenger) → input(passenger)|communication(security_check, security_officer1, passenger, clear, ticket, passenger)

input(passenger)|communication(security_check, security_officer1, passenger, clear, ticket, passenger) & is_at(security_officer2, security_check) & is_at(security_officer3, security_check) & is_at(pax_scan, security_check) & is_at(hand_luggage_scan, security_check) → output(security_officer2)|communication(security_check, security_officer2, passenger, ask, hand_luggage, passenger)

output(security_officer2)|communication(security_check, security_officer2, passenger, ask, hand_luggage, passenger) → input(passenger)|communication(security_check, security_officer2, passenger, ask, hand_luggage, passenger)

input(passenger)|communication(security_check, security_officer2, passenger, ask, hand_luggage, passenger) & has(passenger, hand_luggage, state_object) → output(passenger)|communication(security_check, passenger, security_officer2, provide, hand_luggage, passenger) output(passenger)|communication(security_check, passenger, security_officer2, provide, hand_luggage, passenger) → input(security_officer2)|communication(security_check, passenger, security_officer2, provide, hand_luggage, passenger)

input(security_officer2)|communication(security_check, passenger, security_officer2, provide, hand_luggage, passenger) → output(security_officer2)|communication(security_check, security_officer2, passenger, accept, hand_luggage, passenger)

output(security_officer2)|communication(security_check, security_officer2, passenger, accept, hand_luggage, passenger) → input(passenger)|communication(security_check, security_officer2, passenger, accept, hand_luggage, passenger) & output(security_officer2)|communication(security_check, security_officer2, hand_luggage_scan, provide, hand_luggage, passenger)

output(security_officer2)|communication(security_check, security_officer2, hand_luggage_scan, provide, hand_luggage, passenger) → input(hand_luggage_scan)|communication(security_check, security_officer2, hand_luggage_scan, provide, hand_luggage, passenger)

input(hand_luggage_scan)|communication(security_check, security_officer2, hand_luggage_scan, provide, hand_luggage, passenger) → output(hand_luggage_scan)|communication(security_check, hand_luggage_scan, security_officer2, accept, hand_luggage, passenger)

output(hand_luggage_scan)|communication(security_check, hand_luggage_scan, security_officer2, accept, hand_luggage, passenger) → input(security_officer2)|communication(security_check, hand_luggage_scan, security_officer2, accept, hand_luggage, passenger) & perform_scan(security_check, hand_luggage_scan, hand_luggage, passenger)

perform_scan(security_check, hand_luggage_scan, hand_luggage, passenger) & has(passenger, hand_luggage, state_object) → output(hand_luggage_scan)|perform(security_check, image, hand_luggage, passenger)

output(hand_luggage_scan)|perform(security_check, image, hand_luggage, passenger) & has(passenger, hand_luggage, normal) → **prob.** Output(hand_luggage_scan)|perform(clear, security_check, hand_luggage, passenger) v **otherwise** output(hand_luggage_scan)|perform(alarm, security_check, hand_luggage, passenger)

output(hand_luggage_scan)|perform(security_check, image, hand_luggage, passenger) & has(passenger, hand_luggage, threat) → **prob.** Output(hand_luggage_scan)|perform(alarm, security_check, hand_luggage, passenger) v **otherwise** output(hand_luggage_scan)|perform(clear, security_check, hand_luggage, passenger)

output(hand_luggage_scan)|perform(alarm, security_check, hand_luggage, passenger) → input(security_officer2)|observe(alarm, security_check, hand_luggage, passenger)

input(security_offcer2)|observe(alarm, security_check, hand_luggage, passenger) → internal(security_officer2)|belief(alarm, security_check, hand_luggage, passenger)

internal(security_officer2)|belief(alarm, security_check, hand_luggage, passenger) → arrest(security_check, passenger)

output(hand_luggage_scan)|perform(clear, security_check, hand_luggage, passenger) → input(security_officer2)|observe(clear, security_check, hand_luggage, passenger)

input(security_officer2)|observe(clear, security_check, hand_luggage, passenger) → internal(security_officer2)|belief(clear, security_check, hand_luggage, passenger)

input(passenger)|communication(security_check, security_officer2, passenger, accept, hand_luggage, passenger) → start_pax_check_proccess(security_check, passenger) start_pax_check_proccess(security_check, passenger) & is_at(pax_scan, security_check) → output(security_officer3)|communication(security_check, security_officer3, passenger, ask, passenger)

output(security_officer3)|communication(security_check, security_officer3, passenger, ask, passenger) → input(passenger)|communication(security_check, security_officer3, passenger, ask, passenger)

input(passenger)|communication(security_check, security_officer3, passenger, ask, passenger) → output(passenger)|communication(security_check, passenger, security_officer3, provide, passenger)

output(passenger)|communication(security_check, passenger, security_officer3, provide, passenger) → input(security_officer3)|communication(security_check, passenger, security_officer3, provide, passenger)

input(security_officer3)|communication(security_check, passenger, security_officer3, provide, passenger) → output(security_officer3)|communication(security_check, security_officer3, passenger, accept, passenger)

output(security_officer3)|communication(security_check, security_officer3, passenger, accept, passenger) → input(passenger)|communication(security_check, security_officer3, passenger, accept, passenger)

input(passenger)|communication(security_check, security_officer3, passenger, accept, passenger) & is_at(pax_scan, security_check) → output(passenger)|communication(security_check, passenger, pax_scan, provide, passenger)

output(passenger)|communication(security_check, passenger, pax_scan, provide, passenger) → input(pax_scan)|communication(security_check, passenger, pax_scan, provide, passenger)

input(pax_scan)|communication(security_check, passegner, pax_scan, provide, passenger) → output(pax_scan)|communication(security_check, pax_scan, passenger, accept, passenger) & output(pax_scan)|communication(security_check, pax_scan, security_officer3, accept, passenger) & perform_scan(security_check, pax_scan, passenger)

perform_scan(security_check, pax_scan, passenger) & has(passenger, normal) → **prob.** Output(pax_scan)|perform(clear, security_check, passenger) v **otherwise** output(pax_scan)|perform(alarm, security_check, passenger)

perform_scan(security_check, pax_scan, passenger) & has(passenger, threat) → **prob.** Output(pax_scan)|perform(alarm, security_check, passenger) v **otherwise** output(pax_scan)|perform(clear, security_check, passenger)

output(pax_scan)|perform(alarm, security_check, passenger) → input(security_officer3)|observe(alarm, security_check, passegner)

input(security_officer3)|observe(alarm, security_check, passenger) → internal(security_officer)|belief(alarm, security_check, passenger)

internal(security_officer3)|belief(alarm, security_check, passenger) → arrest(security_check, passegner)

output(pax_scan)|perform(clear, security_check, passegner) → input(security_officer3)|observe(clear, security_check, passenger)

input(security_officer3)|observe(clear, security_check, passenger) → internal(security_officer3)|belief(clear, security_check, passenger)

internal(security_officer3)|belief(clear, security_check, passenger) → output(security_officer3)|cleared(security_check, passenger, pax_scan) & output(security_officer3)|communication(security_check, security_officer3, passenger, clear, passenger)

output(security_officer3)|communication(security_check, security_officer3, passenger, clear, passenger) → input(passegner)|communication(security_check, security_officer3, passenger, clear, passenger)

output(security_officer3)|cleared(security_check, passenger, pax_scan) & not →
input(passenger)|cleared(security_check, passenger, pax_scan)

internal(security_officer2)|belief(clear, security_check, hand_luggage, passenger) →
output(security_officer2)|cleared(security_check, passenger, hand_luggage) &
output(security_officer2)|communication(security_check, security_officer2, passenger, clear,
hand_luggage, passenger)

output(security_officer2)|communication(security_check, security_officer2, passenger, clear,
hand_luggage, passenger) → input(passenger)|communication(security_check, security_officer2,
passenger, clear, hand_luggage, passenger)

output(security_officer2)|cleared(security_check, passenger, hand_luggage) →
input(passenger)|cleared(security_check, passenger, hand_luggage)

input(passenger)|cleared(security_check, passenger, pax_scan) &
input(passenger)|cleared(security_check, passenger, hand_luggage) → concluded_process(security_chcek,
passenger)

input(passenger)|cleared(security_check, passenger, pax_scan) & not concluded_process(security_check,
passenger) → input(passenger)|cleared(security_check, passenger, pax_scan)

input(passenger)|cleared(security_check, passenger, hand_luggage) & not
concluded_process(security_check, passenger) → input(passenger)|cleared(security_check, passenger,
pax_scan)

arrest(security_check, passenger) → conluded_process(security_check, passenger)

The main scanners used in the security check are incorporated in the rules above. More specialized sensors can be added to the process, for example the observation of behavior, biometric characteristics or other character traits.

Is_in_queue(security_check, passenger) & has(passenger, behavior, state_object) & is_at(security_check,
security_officer4) → input(security_officer4)|observe(security_check, behavior, passenger)

Input(security_officer4)|observe(security_check, behavior, passenger) & has(passenger, behavior,
normal) → **prob.** Output(security_officer4)|perform(clear, security_check, behavior, passenger) v
otherwise output(security_officer4)|perform(alarm, security_check, behavior, passenger)

Input(security_officer4)|observe(security_check, behavior, passenger) & has(passenger, behavior,
suspicious) → **prob.** Output(security_officer4)|perform(alarm, security_check, behavior, passenger) v
otherwise output(security_officer4)|perform(clear, security_check, behavior, passenger)

start_pax_check_proccess(security_check, passenger) & is_at(security_check, trait_sensor2) &
has(passenger, trait2, state_object) → perform_check(security_check, trait_sensor2, passenger)

perform_check(security_check, trait_sensor2, passenger) & has(passenger, trait2, normal) → **prob.**
Output(trait_sensor2)|perform(clear, security_check, trait2, passenger) v **otherwise**
output(trait_sensor2)|perform(alarm, security_check, trait2, passenger)

perform_check(security_check, trait_sensor2, passenger) & has(passenger, trait2, suspicious) → **prob.** Output(trait_sensor2)|perform(alarm, security_check, trait2, passenger) v **otherwise** output(trait_sensor2)|perform(check, security_check, trait2, passenger)

Above rules for immediate arrest of passenger. Passenger is thus taken out of the environment. Another possibility is that after an alarm first a second opinion is performed. The passenger is only taken out of the environment if that second opinion gives an alarm as well. An example of the rules used in this scenario is given below for an alarm at the passenger scan.

Internal(security_officer3)|belief(alarm, security_check, passenger) → output(security_officer3)|perform_recheck(alarm, security_check, passenger)

Output(security_officer3)|perform_recheck(alarm, security_check, passenger) & has(passenger, normal) → **prob.** Output(security_officer3)|perform(clear, security_check, passenger) v **otherwise** output(security_officer3)|perform(alarm, security_check, passenger)

Output(security_officer3)|perform_recheck(alarm, security_check, passenger) & has(passenger, threat) → **prob.** Output(security_officer3)|perform(alarm, security_check, passenger) v **otherwise** output(security_officer3)|perform(clear, security_check, passenger)

Additional rules are applied in order to establish integration of the airport security system by means of decision data fusion. Special predicates and dynamic properties are set up in order to implement the different configurations of the integrated airport security system. The actions agents can perform and the communication between the security agents and passengers or between individual security agents are defined in a similar way as can be seen in the comprehensive view of the security check checkpoint shown before, therefore the actions and communication rules are not shown and only the data fusion rules that implement the integration are explained.

The first integration configuration needs a total of any three security systems to raise an alarm on a certain passenger before this passenger will be identified as threat source and taken out of the environment.

Exist(passenger) & not arrest(passenger) → exist(passenger)

Store(alarm, passenger, amount), with initial condition store(alarm, passenger, 0)
Update(alarm, passenger)
Follows(0, 1), follows(1, 2), follows(2, 3)….

Store(alarm, passenger, amount) & not update(alarm, passenger) → store(alarm, passenger, amount)

Store(alarm, passenger, amount1) & update(alarm, passenger) & follows(amount1, amount2) → store(alarm, passenger, amount2)

Output(agents_human/agents_technical)|perform(alarm, location, object, passenger) → output(agents_human/agents_technical)|communication(location, agents_human/agents_technical, data_fusion_system, alarm, passenger) output(agents_human/agents_technical)|communication(location, agents_human/agents_technical, data_fusion_system, alarm, passenger) → input(data_fusion_system)|communication(location, agents_human/agents_technical, data_fusion_system, alarm, passenger)

input(data_fusion_system)|communication(location, agents_human/agents_technical, data_fusion_system, alarm, passenger) → update(alarm, passenger)

Store(alarm, passenger, 3) → arrest(passenger)

The second configuration can be constructed in a similar way. Then not any three alarms are needed, but the passenger and baggage scans are weighed to get more importance. This means that one of these alarms always need to be present in the combination of three alarms and that two other alarm are needed.

Store(alarm, passenger, 2) & update(passenger, alarm) → store(alarm, passenger, 2)

Store(alarm, passenger, 2) & output(pax_scan)|perform(alarm, security_check, passenger) → arrest(passenger)

Store(alarm, passenger, 2) & output(hand_luggage_scan)|perform(alarm, security_check, hand_luggage, passenger) → arrest(passenger)

Store(alarm, passenger, 2) & output(bag_scan)|perform(alarm, baggage_check, baggage1/baggage2, passenger) → arrest(passenger)

Not store(alarm, passenger, 2) & store(alarm, passenger, amount) & output(pax_scan)|perform(alarm, security_check, passenger) → store(alarm, passenger, amount, threat)

Not store(alarm, passenger, 2) & store(alarm, passenger, amount) & output(hand_luggage_scan)|perform(alarm, security_check, hand_luggage, passenger) → store(alarm, passenger, amount, threat)

Not store(alarm, passenger, 2) & store(alarm, passenger, amount) & output(bag_scan)|perform(alarm, baggage_check, baggage1/baggage2, passenger) → store(alarm, passenger, amount, threat)

Store(alarm, passenger, amount1, threat) & update(alarm, passenger) & follows(amount1, amount2) → store(alarm, passenger, amount2, threat)

Store(alarm, passenger, 3, threat) → arrest(passenger)

The final configuration uses an adaptive mode of the individual security systems. It generates a passenger based airport security system, utilizing the different levels, with associated operational performance, in which a security system can operate. All security systems start at a normal operational level with a moderate true positive false positive rate. For every alarm the operational performance of the other individual security systems will be increased to a more adequate level of operation with associated ROC curve operating point. Similar as in the second integrated configuration, the security systems that actively identify a threat object are weighed, respectively the passenger scan, hand luggage scan and baggage scan.

Has(passenger, risk_profile, threat_level)
update(risk_profile, passenger)
Follows(normal, moderate)
Follows(moderate, substantial)
Follows(substantial, high)

Store(risk_profile, passenger, threat_level) & not update(risk_profile, passenger) → store(risk_profile, passenger, threat_level)

Store(risk_profile, passenger, threat_level1) & update(risk_profile, passenger) & follows(threat_level1, threat_level2) → store(risk_profile, passenger, threat_level2)

Output(agents_human/agents_technical)|perform(alarm, location, object, passenger) → output(agents_human/agents_technical)|communication(location, agents_human/agents_technical, data_fusion_system, alarm, passenger)

output(agents_human/agents_technical)|communication(location, agents_human/agents_technical, data_fusion_system, alarm, passenger) → input(data_fusion_system)|communication(location, agents_human/agents_technical, data_fusion_system, alarm, passenger)

input(data_fusion_system)|communication(location, agents_human/agents_technical, data_fusion_system, alarm, passenger) → update(risk_profile, passenger)

perform_scan(security_check, pax_scan, passenger) & has(passenger, normal) & has(passenger, risk_profile, threat_level) → **prob.** Output(pax_scan)|perform(clear, security_check, passenger) v **otherwise** output(pax_scan)|perform(alarm, security_check, passenger)

perform_scan(security_check, pax_scan, passenger) & has(passenger, threat) & has(passenger, risk_profile, threat_level) → **prob.** Output(pax_scan)|perform(alarm, security_check, passenger) v **otherwise** output(pax_scan)|perform(clear, security_check, passenger)

For every threat level an operational probability of detection of true positives and false positives is identified, which use the same representation as the detection rule above. The passenger will be identified as threat source if either the passenger scan, hand luggage scan or baggage scan will give an alarm. After this identification of the passenger the airport security system can arrest the passenger and thus take the passenger out of the environment or implement a second opinion check just like the example of the normal model explained before.