Quantifying Vulnerabilities in an Airport Checkpoint

A study on the role of employee behaviour in the emergence of vulnerabilities

A.J. van den Berg

Technische Universiteit Delft

TU Delft

Quantifying Vulnerabilities in an Airport Checkpoint

A study on the role of employee behaviour in the emergence of vulnerabilities

by

A.J. van den Berg

to obtain the degree of Master of Science
at the Delft University of Technology,
to be defended publicly on March 15, 2018

Student number:	4019016	
Project duration:	September 9, 2016 – Februari, 2018	
Thesis committee:	Prof. dr. R. Curran,	TU Delft, chair
	Dr. O. A. Sharpanskykh,	TU Delft, ATO, supervisor
	Dr. D. Zarouchas,	TU Delft, ASM, external examiner
	S.A.M. Janssen Msc,	TU Delft, ATO, examiner

TU Delft

Abstract

Ever since the attacks on the World Trade Center, airport security has been a topic of interest. The United States was caught by surprise and the attacks triggered a renewed interest in aviation security. It was well recognized that airport security was one step behind on intelligent attackers and this created the need to developed better risk assessment methods [38, 61, 67, 72].

Unfortunately, none of the risk assessment methods developed has the possibility to quantify the vulnerabilities in an airport checkpoint. One of the main challenges in developing a method which can do this, is to find a technique that can account for the complexity of the airport environment from which the vulnerabilities emerge. Furthermore empirical research has shown that security operators do not necessarily follow protocol, but behave as autonomous agents which regularly bend or break the rules [39, 41, 41, 42].

A method which can potentially identify vulnerabilities in such a complex environment is agent based modeling. This modeling technique has proven to be very powerful in modeling complex systems that emerge from the behaviour of autonomous agents. Some work has been done in this area [1, 37, 48], but until now this technique has not been used to quantify vulnerabilities in an airport checkpoint. Therefore, the aim of this project is to develop an agent based model of an airport checkpoint, quantify the vulnerabilities emerging from this checkpoint and analyze the effect of employee behaviour on these vulnerabilities. To do this, the behaviour of the security operators is modeled using models that are rooted in behavioural psychology and have strong empirical backing. The employees decision making is modeled using Decision Field Theory [17] and the employee performance is modeled using the Functional State Model [13, 14].

With the model developed, a set of experiments is performed to calibrate the model and analyze the vulnerabilities. These experiments result in the quantification of vulnerabilities for a predefined set of threat scenarios.

The analysis of these threat scenarios shows that employee behaviour mainly impact threats scenarios in which a weapon is hidden in the carry-on baggage. The reason that security operators have a large influence on the outcome of this screening process is that it is the process in which employees have to perform multiple activities and make multiple decisions. It is found that the vulnerabilities in this screening process are mainly dependent on the speed/accuracy trade-off as made by the employees. The perceived risk of the detected prohibited items plays a limited role, since most prohibited items are only seen as a small risk. The performance of the employees played a less important role on the outcome of the screening process and differences in performance are mainly caused by the personality type of the agents. The personality type that put more effort into a task, outperformed the other agents. The skill level of the operators however, did not significantly effect the outcome the simulation. This suggests that the effort an operator puts in is more important than the skill level of the operator.

Finally it is found that it is beneficial to minimize the number of steps in the screening process. This benefits overall performance, since adding steps to the screening process means adding opportunities to make mistakes.

Contents

1 Introduction

Ever since the attacks on the World Trade Center, airport security has been a topic of interest. The United States was caught by surprise and the attacks triggered a renewed interest in aviation security. It was well recognized that airport security was one step behind on intelligent attackers and this created the need to develop better risk assessment methods [38, 61, 67, 72]. A crucial step in each risk assessment method is quantifying the vulnerabilities in the system. These vulnerabilities are often quantified for a predefined set of threat scenarios. In this case vulnerability is defined as the probability of successfully bypassing airport security for a specific threat scenario.

Quantifying those vulnerabilities is a challenging task, since these values emerge from a socio-technical system in which security operators behave as autonomous agents. Empirical research has shown that security operators do not necessarily stick to protocol, but regularly bend and break the rules [39–42]. It is common to ignore threats and alarms are generally processed as false. Furthermore, the work at a checkpoint is repetitive which demotivates the employees and may lead to poor performance [50, 52, 59].

The aim of this work is to analyze the role of the security operators in the vulnerabilities that emerge for the different threat scenarios. The scope will be limited to the checkpoint, since this is the most important layer of defense [38]. To model airport security, use will be made of agent-based modeling. This technique allows for modeling complex environments which emerge from the interactions between agents by modeling all the agents as autonomous entities.

The main result of this work will be a model of an airport checkpoint that will be used to:

- quantify vulnerabilities for a predefined set of threat scenarios
- identify the contribution of security operators in the emergence of those vulnerabilities
- identify employee characteristics that are most influential on the emergence of vulnerabilities

To achieve this result, Chapter 2 introduces the different processes at an airport checkpoint and provides an overview of different methods to estimate vulnerabilities. Based on this background information a research objective and methodology is established in Chapter 3. After that a conceptual model of an airport checkpoint is developed in Chapter 4 and formalized in Chapter 5. With the airport checkpoint modeled, several experiments are performed to calibrate the model and analyze the relation between agent characteristics and vulnerability. This is the topic of Chapter 6. The conclusions on this project are drawn in Chapter 7 and the report ends with some recommendations for future work in Chapter 8.

2

Background

In this chapter a literature study is performed which serves as the basis for this work. The Chapter starts with introducing the different screening processes at an airport checkpoint in Section 2.1. After that, the role of security operators in these processes is discussed in Section 2.2. Section 2.3 then assesses several methods with may be suitable to quantify vulnerabilities at an airport checkpoint. Based on this assessment, the most promising method is selected.

2.1. Screening Processes at an Airport Checkpoint

The screening process at an airport security checkpoint are mostly developed as a reaction of past terrorist plots targeting aviation. After each attempt regulations and procedures are updated to deal with the new threat. To understand the processes at the checkpoint it is important to look at the equipment involved in screening, the tasks of the security operators and the role distribution between operators. All of these aspects will be discussed in detail in this section.

Subsection 2.1.1 will discuss the security regulations and the history behind those regulations. Subsection 2.1.2 then continues with discussing the equipment used in the screening process. After that Subsection 2.1.3 concludes with an overview of different tasks the security operators perform.

2.1.1. Background

Airports in Europa and the USA are obliged by law to perform security checks and the regulation around those checks have become more extensive over the years. In the USA the regulations are created and implemented by the Transportation Security Administration (TSA). In Europe the rules are set by the European Union and the checks are performed by private security companies hired by the airport.

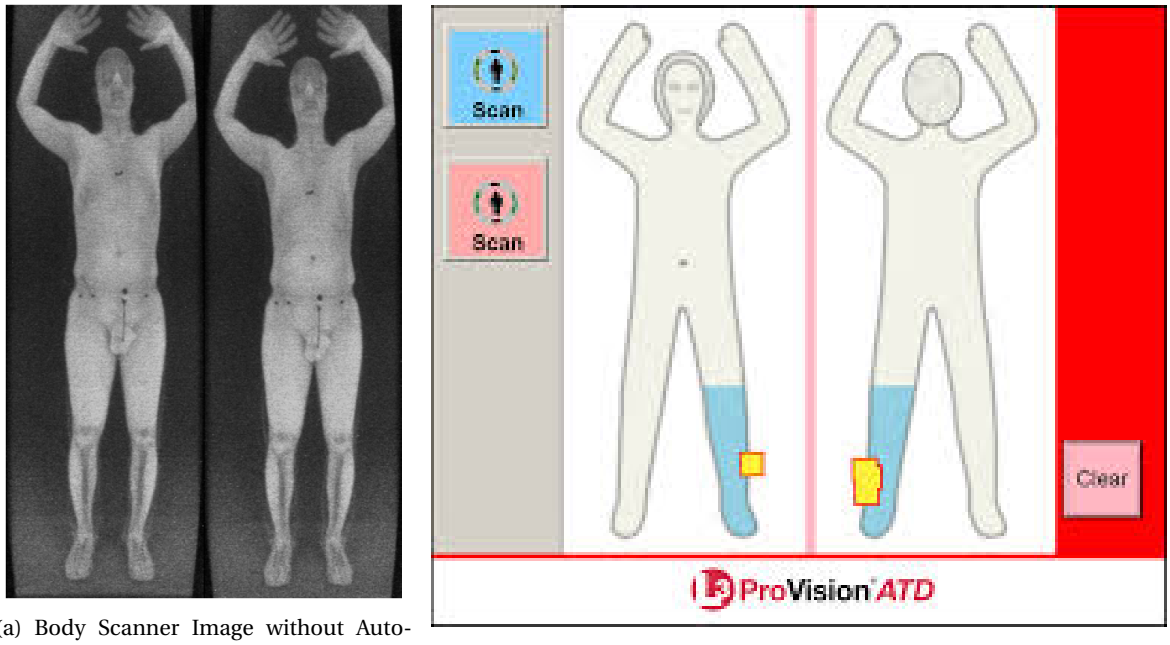
The security regulations in both continents are quite similar and are shaped by the events on 9/11 and other terrorist plots. As a direct consequence of 9/11, it became prohibited to bring knives and scissors into an aircraft. Later in 2001, a man tried to detonate an explosive hidden in his shoes [18]. Since this event, passengers in the USA are obliged to take off their shoes and put them in the X-Ray Machine. In Europe this is not required, but passengers shoes are checked frequently.

In 2006 a plot was discovered to blow up aircraft using liquid explosives[23, 51]. This led to a permanent ban on all fluids in quantities of more than 100 ml. This ban is enforced in both Europe and the USA [21, 70].

In 2009 a man tried to detonate a bomb hidden in his underwear [26]. This incident accelerated the replacement of metal detectors by body scanners [24]. However, security experts are not convinced that these body-scanners would have been able to detect the underwear-bomb [56, 57].

As can be seen from the above examples, the main threat to aviation after 9/11 are explosives. Therefore explosive trace detection equipment has been introduced at both US and European airports.

Despite all those security measures, airport security still has its vulnerabilities. In 2010 two bombs were intercepted between two flight legs [16]. These bombs were hidden in a card-ridge and undetectable in an X-Ray machine [28]. Furthermore ETD tests showed up negative on both bombs. The only reason these bombs were intercepted, was due to the work of the intelligence agencies.



(a) Body Scanner Image without Automatic Target Recognition

(b) Body Scanner Image with Automatic Target Recognition

Figure 2.1: Body Scanner images with and without automatic target recognition

2.1.2. Equipment

Equipment is a vital asset in detecting potential threats. In this section the possible choices of equipment at a security checkpoint are discussed. The following four pieces of equipment are addressed subsequently:

- Walk Through Metal Detector
- Body Scanner
- X-Ray Machine
- ETD Machine

Walk Through Metal Detector

There are two common methods to clear passengers that are entering the secured area of an airport. The first method is by scanning them with a walk through metal detector (WTMD), while the other method is by using a body scanner. In this section the WTMD will be discussed and the body scanner is the topic of the next section.

A walk through metal detector is a device which is used to scan a passenger for metals. The device is calibrated using standardized test pieces and is tested every day [69].

The WTMD is quite sensitive and even gives an alarm when a passenger forgets to take off his belt or has some coins in his pocket. When the machine gives an alarm, the passenger in question receives a pat down.

A major weakness of the WTMD is that it only detects metals. This leaves the airport vulnerable to all kind of weapons which do not contain any metal. This weakness has been exploited before [26] and this event accelerated the replacement of WTMDs by Body Scanners.

Body Scanner

Body scanners are used to scan passengers for forbidden objects. The machines have been quite controversial and were considered an invasion of privacy since the operators were able to see naked images of the person in the scanner comparable to the image in figure 2.1a.

Nowadays this is no longer the case. Both the European Committee and the US Government require the use of automated target recognition. The operators now sees a cartoon-like image of a person and the software automatically indicates areas of interest. An example of this is shown in figure 2.1b.

There are two types of body scanners:

- Back-scatter Scanners
- Millimeter Wave Scanners

These scanners work differently and will be discussed subsequently.

Back-scatter Back-Scatter Machines use X-Rays to create a 2D image of the body. These X-Rays penetrate low density materials like clothing, but not the body and from the reflections a 2D image of the body is made. On this image metals and other dense materials can be clearly distinguished against the human skin. The scanning process requires 30 seconds per passenger and the false positive rate is reported to be 5%.

The back-scatter machine has its weaknesses however. Researchers have been able to hide knives, guns and plastic explosives while passing through the machine [49]. This was done by minimizing the contrast between the body and the contraband.

Furthermore there are some health concerns about the usage of X-Rays. This caused the European Commission to ban the usage of back-scatter machines in all its member states [20].

Also, the back-scatter machines in use by the TSA have been removed as of the first of June, 2013 [68]. The reason for removal was a new requirement that all body scanners used automated target recognition. The supplier of the machines failed to make the deadline which resulted in the removal of all back-scatter machines on US airports.

The machines all have been replaced by Millimeter Wave Scanners. This type of body scanner will be the topic of the next section.

Millimeter Wave All body scanners at airports in the USA and the European Union are Millimeter Wave Scanners. Based on those millimeter waves a 3D image of the body is made. On this image dense objects are clearly distinguishable from the human skin.

A problem with this type of body scanners however, is the number of false positives. Reports have mentioned numbers up to 54 percent. One of the contributing factors was layered clothing. A study performed by the Pacific Northwest National Laboratory showed false positives of 38.5% in the absence of layered clothing. By reducing the sensitivity of the automated Detection Software the number of false positives was reduced to 17%. However, over the last few years the number of false positives seems to have dropped. A survey among travelers in the USA came up with a false positive percentage of 11%. It is unknown whether this reduction in false positives also means that the performance is reduced [31].

Furthermore, the performance of the body-scanners has been questioned by security experts. An old research shows that operators can easily identify guns, but have trouble identifying explosives. Bulk Explosives are detected only 56% of the time [30]. Detection will become even harder when the explosives are molded around the body or take the form of liquid and powder. Therefore it is doubted that the underwear bomb would have been detected by body-scanner [57]. Another security expert claimed in front of the Canadian Parliament that he can smuggle enough explosives through a body-scanner to bring down a Boeing 747 [56].

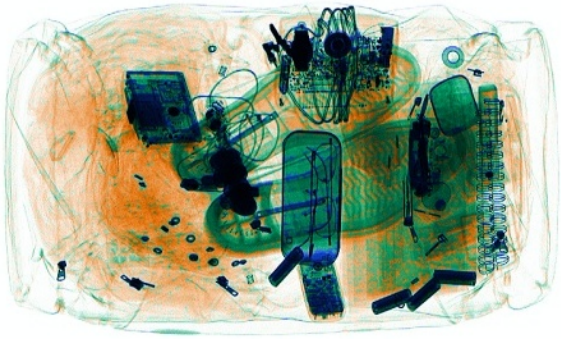
X-Ray Machine

At every airport in Europa and the USA carry-on baggage is screened with an X-Ray Machine. This machine generates an X-Ray image which has to be reviewed by an X-Ray Operator. If the Operator detects a potentially prohibited item on the X-Ray image, the bag will be inspected by another security employee.

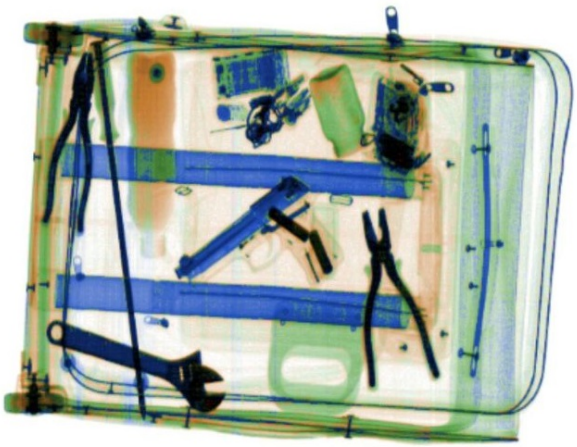
Two examples of X-Ray images shown in figure 2.2. In these images three colors can be seen and each color relates to different materials.

- **Blue** Materials which light up in blue on the X-Ray are metals, hard plastics and plastic explosives. Metal guns will be shown on the image as dark blue while plastic explosives will be light blue.
- **Green** This color generally refer to plastics and alloys which are not dense enough to turn blue. An example of a prohibited item turning up blue is a ceramic knife.
- **Orange** All Organic items will turn up orange in the X-Ray machine. All explosives (except plastic explosives) will turn up in orange and so will most drugs.

Despite this coloring, detecting a prohibited items remains a challenging task. The chances of detecting these items are dependent on both the qualities of the X-Ray Officer and the complexity of the image. Both will be discussed subsequently.



(a) Performance Quality vs. Task Level



(b) Performance Effort vs. Task Level

Figure 2.2: Two Examples of an X-Ray Image

Table 2.1: Detection probabilities for the scenarios specified in 2.2 [71]

	Case 1	**Case 2**	**Case 3**	**Case 4**	**Case 5**	**Case 6**	**Case 7**	**Case 8**
Guns	*0.97*	*0.96*	*0.90*	*0.92*	*0.82*	*0.81*	*0.82*	*0.80*
Knives	*0.92*	*0.86*	*0.79*	*0.72*	*0.62*	*0.5*	*0.54*	*0.44*
IEDS	*0.81*	*0.74*	*0.67*	*0.64*	*0.78*	*0.72*	*0.80*	*0.71*
Other	*0.75*	*0.77*	*0.71*	*0.68*	*0.57*	*0.58*	*0.56*	*0.54*

X-Ray officers must be able to consistently identify prohibited items in a short period of time. This requires adequate training and the continuous focus of the screener. Both criteria are challenging since the work is repetitive and boring which leads to a lowered attention span and high turn-over rates [25].

The second aspect which influences the operators performance is the detectability of the item. This is dependent on the type of item and the difficulty of the image. Three aspects have been identified which contribute to the difficulty of the image [63]:

- **Bag Complexity** The amount of noise and clutter in the bag.
- **Superposition** The extend to which the item is invisible due to other items in the bag.
- **View Difficulty** The difficulty to recognize the item due to the rotation of the target.

The performance of screeners is repeatedly tested and is considered lacking. Both European and American screeners fail to detect the most basic test items more than 20% of the time [12, 25]. This number rapidly increases when the tests become more realistic. Agents from both the U.S. Government Accountability Office and the Department of Homeland Security have been able to consistently bypass the X-Ray machine at all mayor U.S Airports [44, 60].

In this report the detection probabilities as shown in Figure 2.1 will be used. The cases in this table are related to different image complexities and are specified in Table 2.2. This data is obtained by measuring the performance of 67 screeners from mayor European airports to a data-set of 2048 images [71].

From these tables it becomes apparent that detection rates drop when the complexity of the image increases. This is especially true for guns and knives. The detection rate for guns drops from 97% to 80% while

Table 2.2: Scenarios in X-Ray screening [71]

	Case 1	**Case 2**	**Case 3**	**Case 4**	**Case 5**	**Case 6**	**Case 7**	**Case 8**
Bag Complexity	*Low*	*High*	*High*	*Low*	*Low*	*Low*	*High*	*High*
Superposition	*Low*	*Low*	*High*	*High*	*High*	*Low*	*Low*	*High*
View Difficulty	*Low*	*Low*	*Low*	*Low*	*High*	*High*	*High*	*High*

the detection rate for knives drop 92% to 44% when the complexity of the image increases. For Improvised Explosive Devices (IEDs) the story is a bit different. The base detection rate for IEDs is 82% and this drops to 71% for the most difficult images. However, apparently IEDs are hardest to detect when they are in a difficult superposition, but with a low bag complexity and view difficulty. The detection rate then is 65%. The paper does not offer an explanation for this counter-intuitive finding.

ETD Machine

After 9/11 the main threat to aviation are bombing attempts. There have been several attempts to blow up aircraft and the attackers have been very successful in smuggling explosives through security [16, 18, 26, 51]. The go to explosive for terrorists is PETN, a powerful plastic explosive which is almost vaporless which makes it hard to detect for bomb sniffing dogs and other explosive sniffers.

To deal with this threat, all airports in the US and the European Union have Explosive Trace Detectors at the checkpoint. Since sniffing is not a reliable technique for PETN, these machines rely on security employees which actively swap passengers for explosives.

If a passenger is selected for an ETD test, an officer will swap his hands, belt and luggage. This swap is then inserted into the ETD machine which scans it for both explosives and narcotics. The machine itself is extremely reliable provided that the swap contains enough explosive traces.

However, ETD technology has two downsides. First of all, this technique is labor intensive. To deal with this problem, not all passengers are tested. In the USA 60 percent of the passengers is tested for explosives and in the EU this is only 10 percent. At Rotterdam Airport this 10 percent is selected randomly by the WTMD.

The second downside of the ETD machines are the false positives. The machines detect compounds which can be used to build bombs, but many of those compounds are also part of everyday products. A prime example of this is glycerine. This substance can be used to produce dynamite, but is also used in hand sanitizers and cosmetics. An ETD does not know the origin of the compound and will test positive if the threshold value is reached.

Apart from those downsides the technique has one mayor limitation. The machine can only detect explosive traces if the the swap contains enough of those traces. Terrorist can remove those traces by sealing the explosives and cleaning the surface with solvents [16]. This makes the explosive undetectable for an ETD machine.

2.1.3. Tasks at the Checkpoint

In this section the different tasks of security employees at the checkpoint will be discussed. An airport checkpoint is staffed by four security operators and a supervisor. The operators consist of two males and two females. The reason for this is to ensure that pat down are always performed by an officer of the same sex as the passenger.

The four operators will rotate over the following three tasks:

- **Monitoring X-Ray** The task of this employee is to monitor the X-Ray machine and alert the employee checking bags if the bag contains a potentially prohibited item.
- **Checking Bags** The officer assigned to this task is responsible for checking the bags which are flagged by the employee monitoring the X-Ray.
- **Monitoring WTMD/Body Scanner** Two officers are assigned to monitor the WTMD or body scanner: one male and one female. This ensures a pat down is always performed by someone of the same gender.

Apart from the four operators at the checkpoint, there are additional employees which are responsible for performing the ETD check. If a person get (randomly) selected for an ETD test, one of these employees will perform this check. These employees are not attached to a checkpoint.

2.1.4. Conclusion

Airport security has been evolving rapidly after 9/11 under continued terrorist threats. After each terrorist plot, airport security has taken countermeasures to deal with the exploited vulnerabilities.

Both in the US and the European Union carry-on luggage is screened using X-Ray technology. The reliability of this technology depends on the type of weapon and the complexity of the bags. An operator is less likely to detect potentially prohibited items as complexity increases. If an operator detects a potentially prohibited item, the bag is passed on to a second employee which searches the bag.

Passengers themselves have to pass through a metal detector or body scanner. The first machine is only capable of detecting metals. Body scanners are a bit more advanced, but still have limitations in what they can detected. If one of these machines goes of, the passenger is subjected to a pat down.

Most of the threats after 9/11 involved explosives. To deal with this threat, explosive trace detection has become a part of the screening process. The process is time consuming though, which means that only a part of the passengers is screened.

2.2. Modeling the Behaviour of Security Operators

To keep the airport secure, procedures are developed to systematically counter security threats. In those procedures employees play an important role and thus the outcome of each screening procedure is dependent on employee behaviour.

Research has shown that it is common for security employees to bend and break the rules and employee performance can be improved. Therefore this section will address both employee decision making and performance. First the decisions of security operators is discussed in Subsection 4.2.2. After that, the employee performance is addressed in Subsection 4.2.3.

2.2.1. Analyzing the Decision Making Process

Empirical research has shown that employees cannot be expected to follow protocols but have the tendency to systematically bend and break the rules [6, 40, 41]. Therefore it is important to understand what decisions security operators at a checkpoint have to make and why operators sometimes break protocol. To do this, first all the the possible decision points at the security checkpoint are identified. After that several decision factors are discussed, which may cause the employee to bend or break the rules.

Decision Points

In the previous Section three screening procedures are discussed. In those screening procedures, seven different decisions are identified:

- If an X-Ray image is presented to the security operator, the operator must decide to evaluate the image.
- If the security operator evaluates a X-Ray image, the operator must decide whether the corresponding bag should be searched.
- If a security operator receives a bag, he must decide about searching the bag.
- If a passenger passes a WTMD or body scanner, the security operator must decide about performing a pat down.
- If a (potentially) prohibited item is found during a search, the security operator must decide about confiscating it.
- If a passenger wants to enter the secured area, the security operator must decide about performing an ETD test.
- If a prohibited item is confiscated, the security operator has to decide if additional screening is needed.

Since the list is quite extensive, it will be hard to include all those decision points into the model. Therefore simplifying assumptions must be made to reduce the number of decision points. This will be done during the conceptualization and formalization of the model.

Factors which Influence Decision Making

With all the decision points identified, it is important to understand which factors influence the decision process of security operators. These factors are identified from the work of Kirschenbaum [39–42]. These papers focus on airport security and provide an insight in the security culture at an airport. From this papers the following decision making factors are identified:

- **Time Pressure** The pressure to make decisions in less time than needed to increase the throughput at a checkpoint.

- **Group Decision** An event in which the agents collectively select an action from the set of possible actions
- **Negotiation** Bargaining process between a passenger and the security agents
- **Perception** The subjective ideas of the security agent about the characteristics of an attacker agent
- **Characteristics** A typical feature or quality of the security agent which influences the decisions making process

With the definitions of the decision factors established, some context will be given to each of those factors.

Time Pressure Security is under enormous pressure from airlines to make sure flights do not get delayed. Passengers should be processed in 20 to 30s and research has shown that decisions can significantly defer when there is limited decision time [6] This leads to security employees bending or even ignoring protocols [40, 41].

Group Decision Many security decisions are group decisions [33]. Instead of following protocol, security decisions tend to be informal in nature and are made as a group [40, 41]

Negotiation Passengers can not be seen as passive participant in the screening process. It is common that passengers negotiate with security employees and actually influence the decision process [39].

Perception There are many examples of security breaking protocols or ignoring threats [41] and almost all alarms are processed as being false [39] One of the factors contributing to this is the employees perception of what a terrorist is supposed to looks like [41].

Characteristics The employees characteristics play a big role in decision making [42] Some employees have the tendency to follow protocols, others might be more adaptive or social in the decision making process.

2.2.2. Performance of Security Operators

The tasks security operators perform at a security checkpoint are repetitive and can become boring. The nature of this work makes it hard for a security operator to stay focused and motivated [50, 53]. This section first discusses the activities at a security checkpoint which are effected by employee performance. After that, the factors which influence performance are identified.

Performance Dependent Activities

At the checkpoint, four activities are identified which are influenced by the performance of the agent. These activities are discussed subsequently

- Analyzing X-Ray images
  - Once the security operator is presented an X-Ray image, he must process process it for prohibited items. The percentage of false positives and negatives is dependent on the agents performance.
- Searching a bag
  - If the security operator decides to search a bag, the changes of finding a prohibited item, will depend on the performance of the operator.
- Performing a pat down
  - The changes of a security operator finding a prohibited item during a pat down will depend on how well the pat down is performed.
- Performing a ETD Check
  - The outcome of an ETD Check depends on how thorough the security operator swaps for traces.
- Decision Making

  - The consistency of a decision is dependent on the effort a security operator spends on the decision making process [17, 43]

With the activities which are influenced by the performance of the security operator identified, now the factors influencing performance will be identified.

Factors which Influence Performance

From literature, four factors are identified that influence human performance:

- Cognitive demand
  - The cognitive workload of an activity, is a factor that influences the stress levels of a human and effects the performance. [4]
- Stress
  - Stress is caused by high cognitive demands and effects the agents level of fatigue and performance [32, 34, 43].
- Fatigue
  - Fatigue or exhaustion is caused by high workloads, stress or shift work and effects the attention and performance [4, 47].
- Personality
  - Everyone has different cognitive abilities, susceptibilities for stress or exhaustion. This causes humans to respond differently to the same input [29].

2.2.3. Conclusion

The outcome of a screening procedure is dependent on both employee decision making and performance. In this section seven decision points have been identified as well as five factors which may cause an employee to break protocol. Furthermore, five activities in the screening procedures have been identified which are dependent on employee performance.

The number of activities and decisions points makes it clear that the outcome of each screening process is dependent on the behaviour of security operators. This raises the question what the effect is of employee behaviour on the vulnerabilities emerging from the checkpoint. The next section will discuss possible techniques to quantify vulnerabilities and identify the contribution of employee behaviour in the emergence of those vulnerabilities.

2.3. Methods to Quantify Vulnerabilities at an Airport Checkpoint

In the years after the attacks on the World Trade Center several new risk assessment methods have been developed to identify and quantify the risks in airport terminals. An important step in each of those risk assessment methods is the quantification of vulnerabilities for each threat scenario.

The aim of this section is to identify the method which is most suitable for quantifying vulnerabilities at an airport checkpoint. This model must be able to:

- **Account for the complexity of the system**
  - An airport checkpoint is a complex socio-technical environment in which vulnerabilities emerge from interactions between security operators, passengers and technology [7]. Security Experts have identified over 200 elements that influence airport security [19]. The resulting vulnerability emerges from inter-dependencies between all those elements which means that a method is required which is able to capture those non-linear relations.
- **Account for employees as autonomous agents**

  - Empirical research has shown that security operators behave as autonomous agents which do not necessarily stick to protocol, but regularly bend and break the rules [39–42]. It is common to ignore threats and alarms are generally processed as false. Furthermore, the work at a checkpoint is repetitive which demotivates the employees and may lead to poor performance [50, 52, 59]. These human factors effect the performance of the checkpoint as a whole and additional vulnerabilities may emerge from their behaviour. Therefore any method which aims to quantify the vulnerabilities in an airport checkpoint must account for employee behaviour.

- **Identify the factors which cause the vulnerabilities**

  - To make the vulnerability assessment useful, it is important to be able to identify the main factors from which each vulnerability emerges. Identifying these factors makes it possible to address them by changing policies and thus minimize a vulnerability.

In this chapter it is investigated what methods are currently used to quantify vulnerabilities how vulnerabilities in an airport terminal are identified

To do this, Section 2.3.1 assess the most common methods to identify and quantify vulnerabilities in a system. Then, all risk assessment methods applicable to airport terminals will be discussed in Section 2.3.2. All these methods will be assessed based on the criteria as defined above and the most promising method is selected.

2.3.1. Generic Vulnerability Assessment Methods

There are several generic methods to assess the vulnerability of a system which will be discussed subsequently:

- Expert Elicitation
- Vulnerability Logic Diagrams
- Event Trees
- Penetration Testing

The first tree methods are advocated in RAMCAP [72], the American standard method for risk assessments. The last method, penetration testing is practiced by both the TSA and DHS. It is important to note that most of those methods are not mutually exclusive, but can be combined to obtain a better result. These methods will be discussed with a focus on their usability in assessing vulnerabilities at an airport checkpoint.

Direct Expert Elicitation

The most common method to estimate vulnerabilities is to consult security experts involved in the field. These experts have inside knowledge of the equipment, procedures and performance of the employees. Therefore their reasoning could be a good basis to estimate the performance of the checkpoint and identify possible vulnerabilities.

Unfortunately expert elicitation has proven to perform poorly in parameter estimation when there are dependencies in the system [22]. In a complex environment as an airport these dependencies inevitably exist [19]. Thus expert elicitation is of limited value since it cannot deal with the complexity of the system and identifying possible failure modes.

The poor performance of experts in complex environments also implies that expert elicitation is not a suitable method to assess the role of employees or identifying the main factors contributing to the emergence of a threat scenario

Failure Trees

A failure tree models events in the form of an event tree [8, 36]. The nodes of the tree are events and the branches of each node specify the possible outcomes of the event. Each outcome of an event has a probability assigned to it. The probability for each specific series of events and the corresponding outcome is the product of the conditional probabilities for each event.

While this is a more structured approach to estimate the vulnerability to a specific threat scenario, the method still relies on a lot of assumptions. For each event in the tree the likelihood of the different outcomes

Table 2.3: The suitability of vulnerability quantification methods for assessing an airport checkpoint based on predefined criteria

	Expert Elicitation	Vulnerability Diagram	Failure Tree	Penetration Tests
Complexity of the System	*Maybe*	*Maybe*	*No*	*Yes*
Behaviour of the Agents	*Maybe*	*No*	*No*	*Yes*
Identifying underlying Factors	*Maybe*	*Maybe*	*No*	*No*

must be estimated. The reliability of this methods hinges on the accuracy of those estimates which are not always accurate [66].

Furthermore, it is questionable whether a failure tree is sufficient to model a complex socio-technical environment like an airport checkpoint. An oversimplification of the system will lead to loss of accuracy or failure to capture all vulnerabilities. Next to that failure trees depend on employees sticking to procedures which is not necessarily true.

Since a failure tree is quite a simple model, it is easy to identify the events in the tree which contribute most to the emergence of a vulnerability, but since the model is quite simple it is questionable whether these results correspond with reality.

Vulnerability Logic Diagrams

A vulnerability logic diagram shows all the steps an attacker has to take to reach their goal [62]. At each step the effectiveness of the countermeasures are estimated as low, medium or high. Based on those estimates, the vulnerability is categorized using a predefined scale.

The benefit of this method over the failure tree is that it does not require an exact number for the likelihood of each outcome. This saves time, lots of discussion and the results do not give a false sense of precision. The downside is the same as for the failure tree: the accuracy of the estimates may be low.

Apart from that, it must be realized that the attacker has to take only one step to pass the checkpoint. He joins the line and complies with the security operators until he is cleared. The chances of successfully doing so depend on the skill level of the employee, visibility of the weapon, beliefs about the weapon, equipment etcetera. This huge amount of parameters makes it extremely hard to predict the effectiveness of the countermeasures at the checkpoint. This prediction completely hinges on expert judgment, which is known to perform poorly in this kind of situations. Therefore this method is not suitable for assessing vulnerabilities in airport terminal either.

Penetration Testing

The easiest method to test vulnerability of airport defenses is physically testing them. This has been done by both the US Transportation Security Administration [65] and the US Department of Homeland Security [27]. The results from those tests can be used to give better vulnerability estimates and develop better protocols.

The big advantage of penetration testing is that it does not require any assumptions about the complexity of the system nor the behaviour of the security operators. This guarantees that the vulnerabilities found during these tests coincide with reality. However, a problem with penetration testing that it is labour intensive and thus expensive. The DHS performed 6000 penetration over the last years, while the number of public airports in the USA is over 5000 [3, 9]. This means that an airport is not even tested once a year.

Furthermore, this low number of tests makes it hard to identify the main factors from which these vulnerabilities emerge. This is important, since identifying these factors is the key to mitigating the vulnerability.

Conclusion

There are four common methods to estimate vulnerabilities which may be used for an airport checkpoint. This Section discussed them subsequently and the results are found in Table 2.3. The first approach is expert elicitation, but this method performs poorly in complex environments like an airport checkpoint. This means that expert elicitation on its own will perform poorly in estimating vulnerabilities and quantifying the effect of the underlying factors.

The vulnerability logic diagram performs poorly for the same reason. This diagram shows all the steps an attacker has to take and estimates the chances of success at every step. However, passing the security checkpoint is a single step in which the attacker has to comply with the security operators in order to bypass the checkpoint. Since passing the checkpoint is a single step, this basically comes back to expert elicitation.

A more suitable method to assess the vulnerabilities is a failure tree. This breaks the checkpoint processes down in a series of events with possible outcomes. The likelihood of each outcome for each event has to be

estimated. The reliability of this method depends on the accuracy of the underlying estimates and the validity of the failure tree. This method offers the possibility to break down each checkpoint process into subsequent activities and decisions and thus is capable to trace back vulnerabilities to decision points and activities. The main objection to this method is that it reduces the screening process to a series of steps. Given the dynamic nature of the checkpoint, this linear reasoning is probably not sufficient as a representation of the checkpoint. Furthermore it does not include the possibilities to analyze the effect of employee behaviour on the outcome of the screening process.

The method best suitable to identify vulnerabilities in an airport checkpoint is penetration testing. However, the method is labour intensive and cannot identify the main factors from which the vulnerabilities emerge. This makes it hard to address the root of the problem and minimize the identified vulnerability.

Given the limitations of these vulnerability identification methods, it is no surprise terrorist have been able to outsmart airport security over and over again. This problem is well recognized within the scientific community and several attempts have been made to develop a risk assessment method to identify and minimize the risk in airport terminals. These methods will be the topic of the next section.

2.3.2. Risk Assessment Methods for Airport Terminals

In light of the current terrorist threat against aviation, several risk assessment methods have been developed for airport terminals. The goals of these methods vary from identifying the most dangerous threat scenarios to optimizing the strategy of airport security, but in order to attain any of these goals, the vulnerabilities in airport security have to be identified properly.

This section will discuss those risk assessment methods and how they estimated vulnerability. First the Scenario Based Approach will be discussed in Subsection 2.3.2. After that a Game Theoretic Approach is examined in Subsection 2.3.2. Finally, an Agent-Based Method is reviewed in Subsection 2.3.2.

A Scenario Based Approach

The scenario based approach is an approach which tries to identify threat scenarios to which airport security is most vulnerable [19]. The designers of the method realize that airport security is a complex environment which cannot be described by a small set of variables and that its security cannot be assessed with a small number of threat scenarios. Therefore this method starts with identifying all security and threat elements which together describe the airport environment. This results in a list of 210 elements which are grouped in 15 categories. For each category the relation with other categories is defined. For example: an element from the category "weapon" allows "use of weapon". By reducing the relations between these categories, the number of scenarios is limited to approximately 220.000. For each of those scenarios, the counter-measures are identified as well. This makes it possible to identify scenarios in which a limited number of counter-measures is available.

This approach has three mayor limitations. First of all, the airport environment is reduced to a linear set of relations between threat elements and counter measures. Despite the large number of elements used in this method, the linear relations between them can never capture the dynamic nature of the airport environment. Since vulnerabilities emerge from the dynamics of the system, it is highly likely some vulnerabilities will be missed.

Second, this method aims to identify the threat scenarios to which the system is most vulnerable, but only identifies the number of counter measures related to each threat scenario. It would be better if the scenarios to which the counter measures are least effective could be identified. Unfortunately this is not possible, since the effectiveness of each counter measure in each threat scenario is undefined.

A Game Theoretical Approach

A potential method to assess airport security is the use of game theory[10]. This method has gained popularity since it accounts for intelligent attackers who exploit weaknesses in the system. The problem of game-theoretic models is that they are difficult to develop. The models generally require lots of assumptions which are hard to validate. One of the biggest problems is that game-theoretic models tend to over-rationalize things. This does not always correspond with reality [64]

A game theoretic approach which has gained some ground in airport security is the Bayesian Stackelberg game. In this game the defender acts first and the attacker gets to observe the defenses and act in response. The purpose of this game is to find the optimal policy for the defender. The method has been proven to be successful in finding this optimal policy [54, 55] and is currently under evaluation by the Transportation Security Administration. If these tests are successful this method could be deployed at 400 US airports. [5]

Table 2.4: The suitability of vulnerability identification methods for assessing an airport checkpoint based on predefined criteria

	Game Theoretic Approach	Scenario Based Approach	Agent Based Approach
Complexity of the System	*No*	*Maybe*	*Yes*
Behaviour of the Agents	*No*	*No*	*Yes*
Identifying underlying Factors	*No*	*Maybe*	*Yes*

To set up and solve a Bayesian Stackelberg game, the vulnerabilities in the system must be quantified for each possible strategy of the defender. The paper fails to mention how the airport is modeled and how the vulnerabilities are estimated or calculated. This is a pity, since identifying all vulnerabilities and quantifying the, is a crucial step in optimizing the airport defense strategy. Failure to do so, will inevitably lead to a sub-optimal strategy for the airport defenses. Therefore, a good vulnerability analysis is pivotal to the success of this game theoretic approach.

An Agent Based Approach

Over the last few years agent-based modeling has gained interest as an approach to assess airport security. An agent based model allows for modeling complex environments which emerge from the interactions between autonomous agents.

Some work has been done in this area already. First of all, a model of an airport terminal has been developed which aims to optimize resource allocation [48]. This model is very limited and contains minimal decision logic for the agents.

Furthermore, the technique is proposed as risk assessment method for airport terminals [37]. In line with this work, a model of an airport terminal is developed which can serve as a basis to study security, efficiency and resilience of operations in the terminal [1]. The model is still under development and contains limited logic for the security operators.

This approach seems very promising, since it is suitable for modeling complex environment and provides a good framework to model the behaviour of the individual agents. If an airport checkpoint is modeled using this technique, it becomes possible to identify the vulnerabilities and relate those to the underlying parameters.

Conclusion

The need of developing better risk assessment methods for airport terminals is fully recognized within the scientific community and several attempts have been made to do this. Unfortunately none of these methods properly modeled the airport checkpoint and quantified the vulnerabilities in an airport checkpoint. One of the modeling technique however seems quite promising. The performance of the modeling techniques with regards to the predefined criteria, is found in Table 2.4

The game theoretic approach aims to optimize the resource allocation of airport security, but does not provide a model of the airport terminal nor an insight how vulnerabilities are identified and estimated. These steps are crucial to optimize resource allocation, since poor estimates of vulnerabilities, will lead to sub-optimal resource allocation. This means the game theoretic approach actually needs a vulnerability assessment method to define the input.

The scenario based approach recognizes the complexity of the airport environment and expresses airport security as a set of linear relations between threat elements and counter measures. This results in a large number of threat scenarios which are filtered on the number of countermeasures. In the end only the threat scenarios with a limited number of countermeasures are analyzed. This method recognizes the complexity of the airport terminal, but defining linear relations between threat elements and counter measures does not capture the interdependencies between those elements. Furthermore, this method is able to identify threat scenarios for which the number of counter measures is limited, but is not able to quantify vulnerabilities or identify the role of employee behaviour in the emergence of those vulnerabilities.

The agent based approach recognizes the complex nature of the airport environment and models the environment as a set of agents interacting with each other. Currently some work has been done in this area, but so far it has not been used to quantify vulnerabilities in an airport checkpoint. However, the modeling technique itself seems to meet all the criteria as formulated in the introduction of this section. The technique is suitable for modeling complex environments which emerge from the interactions between autonomous agents. The vulnerabilities which emerge from this environment can be analyzed and traced back to the

underlying parameters. Furthermore, since security operators are modeled as autonomous agents, the effect of their behaviour on the vulnerabilities emerging from the checkpoint can be measured and analyzed.

2.4. Conclusion

The airport checkpoint is the most important layer in airport security. At the checkpoint passengers and carry-on luggage are screened for prohibited items and explosive traces. To do this, three different screening processes take place. First the baggage is scanned using x-ray technology. At the same time the passenger is scanned using either a WTMD or Body Scanner. Finally, some passengers are selected for a random explosive test.

To carry out those processes, a checkpoint is generally staffed with five employees. These employees play an important role in each of these processes by performing activities and making decisions. However, research has shown that employees decide to not always follow protocol and that the nature of the job makes it hard to stay motivated to perform well. This employee behaviour inevitably has consequences on the outcome of the screening processes and raises the question how vulnerabilities emerging from the checkpoint are effected by employee behaviour

There are several common techniques to identify vulnerabilities, but none of these approaches are suitable to assess the role of employee behaviour on the emergence of vulnerabilities in a complex environment like an airport checkpoint. The best technique is penetration testing, since this method does not require any assumptions about the system or the role of employees. Unfortunately this approach is not suitable to identify the main factors from which the exposed vulnerabilities emerge.

The problem of airport security is also widely recognized within the scientific community and several attempts have been made to develop a method to optimize airport security. Despite these efforts, none of those models included a method to quantify vulnerabilities at an airport checkpoint. Nevertheless, the agent based modeling approach seems a promising technique for a vulnerability analysis, since it has the potential to model the socio-technical environment from which these vulnerabilities emerge. In an agent-based model employees are modeled as autonomous agents which makes it possible to assess the effect of agent characteristics on vulnerability. Therefore, agent based modeling is proposed as a method to identify vulnerabilities at an airport checkpoint.

3

Research Objective & Methodology

Over the last two decades terrorist repeatedly outsmarted airport security by identifying and exploiting new vulnerabilities. It is only after each attack that procedures get changed to address the vulnerability that has been exploited. This reactive approach keeps airport security on the back-foot against innovating attackers. This problem is widely recognized by both security experts and the scientific community and some attempts have been made to develop new risk assessment methods.

A crucial step in each risk assessment method is the identification of vulnerabilities, but until now no method has been developed which can quantify vulnerabilities in an airport checkpoint. The main challenge to be faced in developing such a vulnerability identification method, is the complexity of the environment from which the vulnerabilities emerge. The airport terminal is a complex socio-technical system in which the employees operate as autonomous agents which do not necessarily pay attention or follow protocol.

The aim of this work is to develop a vulnerability identification method which takes into account employee behaviour. To do this, use will be made of agent-based modeling. This technique allows for modeling complex environments which emerge from the interactions between agents by modeling all the agents as autonomous entities.

The scope of this work will be limited to the airport checkpoint, since this is the main layer of defense. Within this scope the focus will be on the role of employee behaviour, since empirical research has shown that employees regularly bend and break protocol. Furthermore employee performance can be sub-optimal due to the boring and repetitive nature of the job. This employee behaviour inevitably has an impact on the emergence of vulnerabilities and the aim of this work is to find out how employee behaviour is related to the vulnerabilities which emerge at the checkpoint.

3.1. Research Questions

The research question is defined as:

> *Can the role of employee characteristics in the emergence of vulnerabilities at an airport checkpoint be identified and quantified using Agent-Based Modeling?*

To answer this question, the following sub-questions are defined:

- *How can the security operators be modeled by using an agent based approach?*
- *How is the outcome of employee activities and decisions influenced by their characteristics?*
- *How is the outcome of each screening process influenced by the characteristics of the employees?*
- *What is the vulnerability for each threat scenario and what is the role of the employees in each of these scenarios?*

How can the security operators be modeled using an agent based approach?

The first step in finding an answer to the research question, is the development of an agent based model of an airport checkpoint. With the airport screening processes analyzed and the role of the security operators identified, the next objective is to translate this knowledge into an agent based model.

How is the outcome of employee activities and decisions influenced by their characteristics?

Each of the employees in the model have activities to execute and decisions to make. The aim of this question is to quantify the effect of employee characteristics on each of those tasks and decisions.

How is the outcome of each screening process influenced by the characteristics of the employees?

With the effect of employee characteristics on individual activities and decisions analyzed, the next goal is to identify the employee characteristics which are most influential for the outcome of the screening process.

What is the vulnerability for each threat scenario and what is the role of the employees in each of these scenarios?

With the effect of the characteristics of security operators on each screening procedure identified, the last objective is to quantify the vulnerability for each threat scenario and analyze the contribution of the security operator to that number.

3.2. Research Methodology

To obtain an answer to the research question, a methodology is developed to answer each of the sub-questions. These will subsequently be discussed.

Modeling the security operators

The first research objective is to translate the knowledge of an airport checkpoint as discussed in 2 into an agent based model. To do this, the following steps will be taken:

- Identifying all employee activities and decisions.
- Selecting a modeling framework
- Selecting suitable behavioural models
- Developing a formal model
- Calibrating this model

The first step is to identify all the employee activities and decisions in the screening process and how these are related to each other. To do this, all the different screening processes are broken down into steps and schematized. This will be done for two different checkpoint configurations. By schematizing the processes, the employee activities, decisions and relations between them can readily be identified for each configuration.

The next step is to develop an architectural model of the security operators. This will provide the framework to implement the behavioural models related to the agents performance and decision making. The result of this step will be an overview of all the modules in the model of the security operator.

With the architectural framework established, the behavioural models for the agents decision making and performance will be selected. The most important criteria for those models is that they must be rooted in behavioural science and backed up with empirical support. This is crucial for the validity of the agent-based model as a whole.

Now that the whole model of the security operator is conceptualized and the roles of the security operators have been broken down into subsequent activities and decisions, the following step is to develop a formal model of the airport checkpoint.

When the model is formalized, the final step is the calibration of the model. To do this, first the underlying behavioural models are analyzed. Based on the results from this analysis and the findings in Chapter 2, the model will then be calibrated. At this point the agent-based model is finished and thus the first research objective is reached. The results from the model can be readily obtained by running a Monte-Carlo simulation.

Quantifying the effect of employee characteristics on each activity and decision

The next objective to identify the relation between employee characteristics and the outcome of tasks and decisions. To do this, first the employee characteristics will be identified which are related to decision making or performance. This will be done based on the relations in the formal model.

The next step is to analyze the effect of those characteristics on the outcome of all the individual tasks and decisions. It will be investigated if a change in this characteristic has a significant influence on the outcome of the activity or decision. The different characteristics are then compared to each other to see which characteristics are most influential for the outcome of a specific decision or activity. Finally, the main results from these analyses are discussed and will be explained based on the underlying behavioural models.

Quantifying the effect of employee characteristics on the outcome of each screening process

With the effect on employee characteristics on individual activities and decisions identified, the next step is to analyze the effect of employee characteristics on the outcome of the screening process in which the operator is involved.

The main objective is to find out which employee characteristics have a statistically significant impact on the outcome of the screening process. In doing so, the employee characteristics which have the largest influence on vulnerabilities are identified.

Identifying the role of employees in the vulnerability for each of the threat scenarios

The vulnerability for each of the threat scenarios is the result of interactions between employees, equipment and the prohibited item. The objective of this research question is to find out which part of the vulnerabilities can be attributed to employees.

4

Conceptual Model

The aim of this chapter is to conceptualize the checkpoint processes and the behaviour of the agents. To do this, first the screening processes will be schematized in Section 4.1. This will be done for two different checkpoint configurations. After that the behaviour of security operator is conceptualized in Section 4.2.

4.1. Screening Processes at an Airport Checkpoint

In this section the screening processes in two different checkpoint lay-outs will be conceptualized. The conceptual models of these checkpoints will serve as a basis for the experiments performed in this report. The processes at both airports are schematized in Figures 4.1 and 4.2. In those figures activities of the employees are colored green and decision points are yellow. The input and output of the processes are marked blue. Based on these figures, both checkpoint configurations are discussed.

4.1.1. Regional Airport

In this subsection the checkpoint lay-out of a regional airport is discussed. The content of this subsection is based on information which is provided by the airport and subsequently the following processes are discussed:

- Scanning Carry-On Luggage
- Scanning Passengers
- Testing for Explosives

Scanning Carry-On Luggage The screening process of carry-on luggage is depicted in figure 4.1a Carry-on luggage is screened using the X-Ray machine which is manned by an X-Ray Operator. This employee has the task to identify potentially prohibited items and decide whether the bag should be searched. If the X-Ray operator decides that the bag requires a search, the bag is passed on to a second employee which searches the bag.

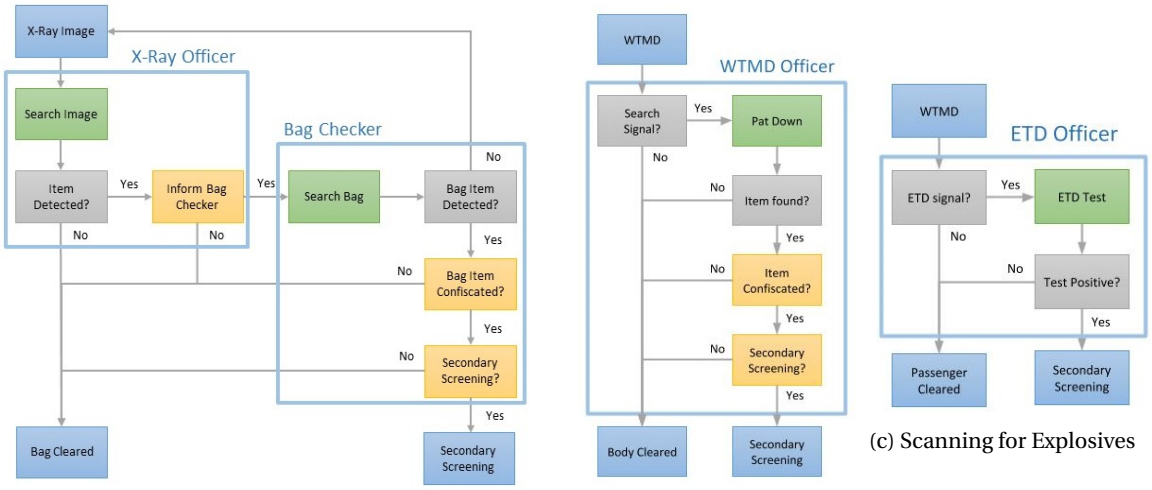
If the item is found, the bag searcher must decide whether it must be confiscated and if additional screening is needed for the owner of the item.

If the bag searcher cannot find the item he is looking for, the bag will be rescanned by the X-Ray Operator. This requires some level of coordination and communication between those employees.

Scanning Passengers In this checkpoint configuration all passengers have to go through a Walk Through Metal Detector when entering the restricted area. If the metal detectors goes off, a pat down is performed on the passenger. An overview of this process is shown in figure 4.1b

If an item are found during the pat down, the employee has to decide whether the item should be confiscated and if additional screening is needed. Otherwise the passenger is cleared.

In practice it happens that passengers forgot to get their wallets out of their pockets. In that case the passenger can avoid a pat down by going through the metal detector again. This procedure will not be included in the agent based model.



(a) Scanning Carry-On Luggage

(b) Scanning Passengers

(c) Scanning for Explosives

Figure 4.1: Screening Processes at a Regional Airport

Testing for Explosives Some passengers are randomly selected for an ETD test. This selection is based on a signal from the metal detector which goes off with a probability of 10%.

An overview of the ETD checking process is given in figure 4.1c If a passenger is selected for an ETD test, it is assumed this test is always performed If the passenger tests positive for explosive traces, he will automatically be subjected to additional screening. Otherwise the passenger is cleared.

4.1.2. Internal Airport

In this subsection the configuration at an International Airport is described. This description is based on publicly accessible information and personal experience. Subsequently, the following processes are discussed:

- Scanning Carry-On Luggage
- Scanning Passengers
- Testing for Explosives

Scanning Carry-On Luggage Similarly to the regional airport Carry-On Luggage is scanned by an X-Ray machine. The screening procedure is slightly different in this configuration and shown in figure 4.2a. The X-Ray Operator has the task to scan the images for prohibited items and decides whether a bag is cleared or not.

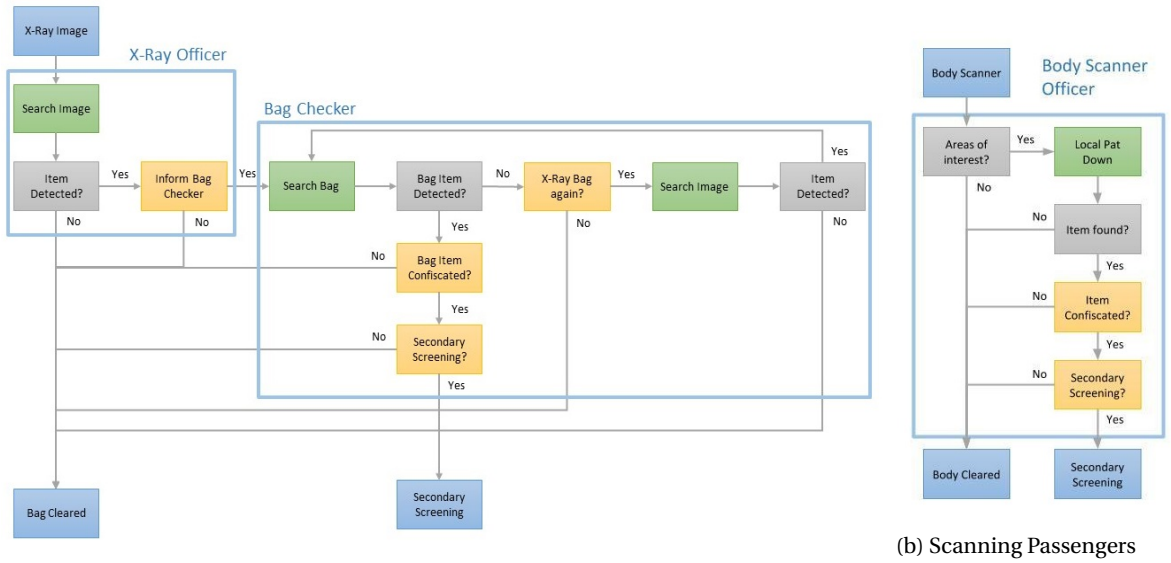
Contrary to the regional airport there is no direct communication between the X-Ray Officer and the employee checking the bags. The Bag Checker just receives the bags which are not cleared by the X-Ray Operator along with the corresponding X-Ray Image. This means the Bag Checker has to correctly identify the prohibited item on the X-Ray Image as well.

If the Bag Searcher cannot find the prohibited item, he can decide on rescanning the bag. This rescan is done by himself on a secondary X-Ray Machine.

If the item is found, the bag searcher must decide whether it must be confiscated and if additional screening is needed for the owner of the item.

Scanning Passengers In this configuration all Passengers are scanned with a body-scanner. An overview of this process is given in figure 4.2b. If this machines goes off, it indicates which areas on the body triggered the alarm. An employee will search the passenger using a local pat-down near the indicated areas.

Testing for Explosives It is not known how passengers are selected for ETD tests at this Internal Airport, so it is assumed this is the same as the Regional Airport. This means that the Body Scanner will randomly select 10% of the passengers for an ETD test.



(a) Scanning Carry-On Luggage

(b) Scanning Passengers

Figure 4.2: Screening Processes at the International Airport

Conclusion

In this section two checkpoint configurations are discussed which will be used as a basis for the agent based model. In both configurations, the checks for baggage, passengers and explosives are separated.

At both airports Carry-On Luggage is checked using an X-Ray machine, but the configuration of the does not allow for any communication between the X-Ray Operator and Bag Checker.

Passengers at the Regional Airport have to go through a walk through metal detector and are pat down if the machine goes off. The International Airport uses a body-scanner which indicates suspicious areas on the passengers body. This allows for a local pat down instead of a full pat down.

Finally, at the Regional Airport 10% of the passengers are randomly selected for an ETD test. It is assumed this is the same at the International Airport.

4.2. Modeling the Behaviour of Security Operators

In the previous section the tasks and role distributions for the security operators have been discussed. The focus of this section will be on how they perform their tasks. Studies have shown that employee performance is lacking and that it is common for security employees to bend and break the rules. Therefore both employee performance and decision making will be addressed.

To model employee behaviour, first an architectural framework is introduced in Subsection 4.2.1 which will serve as the basis for the formalized agent based model. After that the decision making model of security operators is conceptualized in Subsection 4.2.2. Then employee performance is addressed and a method is introduced to model employee performance in Section 4.2.3.

4.2.1. Architectural Framework for Security Operators

A common method to model human agents, is to divide the functionalities of the agents into three hierarchical layers: a strategic layer, a tactical layer and an operational layer [11, 35, 37, 58]. These three layers will be used as an architectural framework to model the behaviour of the Security Operators. The layers in the model will be discussed subsequently based on Figure 4.3. This figure shows the hierarchical layers along with the different modules which will be implemented in the layer.

The strategic layer is responsible for the agent decision making and consists of three modules: a goal module, a decision module and a belief module. The decision module is the central module and responsible for selecting the next action of the agent. This module will be an implementation of Decision Field Theory and decisions will be based on the results from the current activity, the goals and the beliefs of the agent.

The tactical layer is responsible for executing activities and consists of two modules. The first module is the activity module which is responsible for executing the tasks of the agent. These tasks are started based

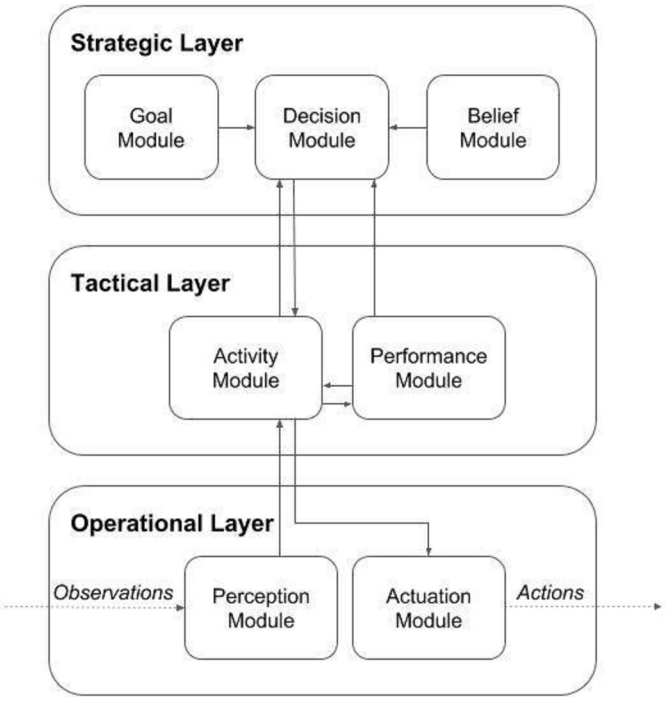


Figure 4.3: Conceptual Model of the Security Operator

on input from the environment or based on a decision of the agent. The second module in this layer is the performance module which determines both how well an agent performs on a task and how much effort is put into a decision. This performance module will be an implementation of the Functional State Model and updated based on the Task Complexity of the current task.

The operational layer is responsible for the interactions with the environment and has two modules: a perception module and an actuation module. The agent observes the environment through the perception module and acts on the environment using the actuation module.

4.2.2. Modeling the Decision Making Process

The decision making process of the security operators will be modeled based on with the work of Busemeyer and Townsend [17]. Their decision model, known as Decision Field Theory, has strong empirical backing and is famous for its ability to reproduce many known irrationalities in human decision making.

At the checkpoint the security operators have to decide between continuing the screening process or clearing a passenger. The decision making process behind this is an iterative process in which the operator constantly updates his preferences until the preference for one of the options exceeds a threshold value. This threshold value is one of the inputs of the model and its magnitude is related to the effort an agent spends on a decision. The higher the threshold value, the more time and energy the security operator needs to reach it.

During each iteration the agent focuses on one of his goals. The selection of this goal is a random process, but the likelihood of the agent focusing on a goal depends on how important the goal is to the agent. Once the attention of the agent is focused on one of his goals, the agents preferences are updated based on the agents beliefs about how each of the options helps him in achieving the goal he currently focuses on. The magnitude with which the preference for each of the goals is updated is known as valence. This valence will be defined for each combination of goals and options.

Finally, the decision making process is influenced by the agents initial beliefs. This initial belief is the preference the agent has for each outcome before the decision process starts.

4.2.3. Performance of Security Operators

The tasks security operators perform at a security checkpoint are repetitive and can become boring. The nature of this work makes it hard for a security operator to stay focused and motivated [50, 53].

To model the performance of security operators, the Functional State Model is selected [13]. To the best of the authors knowledge, this is the only performance model which takes into account all the factors de-

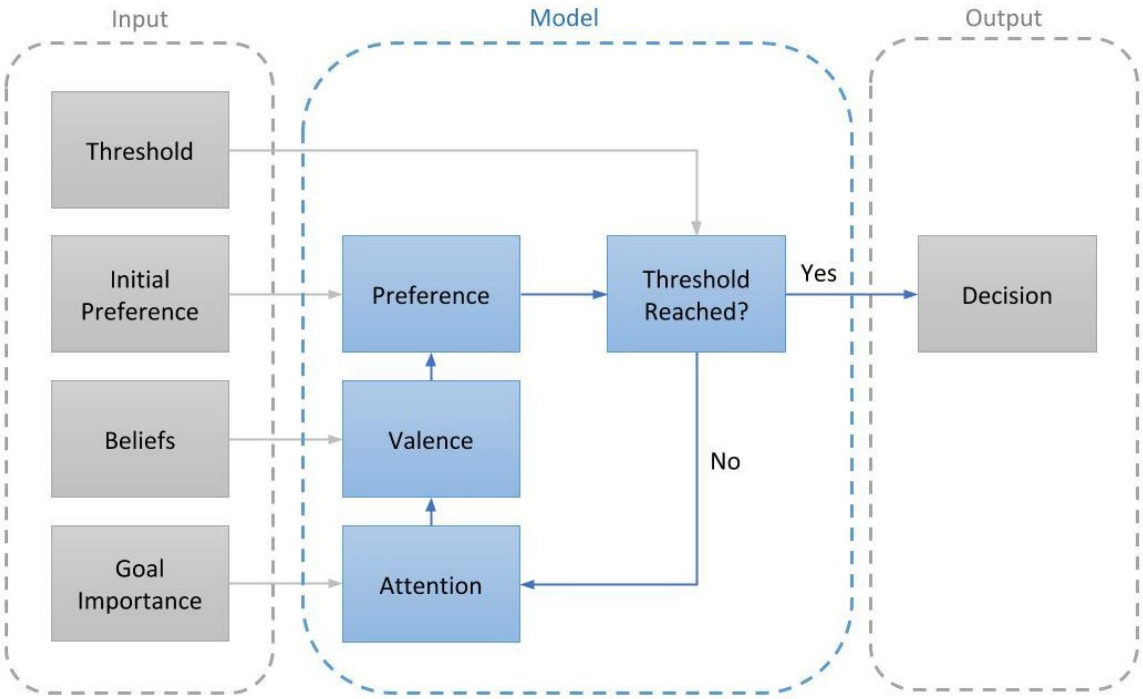


Figure 4.4: Decision Field Model

scribed. The Functional State Model is a dynamic performance model which describes performance based on task complexity, the state of the agent and its characteristics. The model incorporates factors like stress, exhaustion and situational awareness.

Figure 4.5 shows an overview of the Functional State Model. the input for the model is the Level of a task, which is dependent on the Skill Level of the Agents and Task Complexity. The output is the agents Performance Quality, which indicates how well an agent is performing.

The model contains a critical point. This is the point where the agent can reach its maximum performance without getting more exhausted.

If task levels get low, the agent will under-perform since he will not be triggered to generate enough effort. If the task levels get high, performance will drop since the task will become too difficult compared to agents skill level.

The authors of the functional state model have extensively verified the model to fully understand its internal behaviour. Furthermore the model has been validated by calibrating it with empirical data [14]. Based on this empirical study two example personality types are developed: Type I and II. Type II personalities are more sensitive to stress which negatively impacts their peak performance.

The model itself is quite complicated, since it has 37 parameters. However, since two example personalities are added, it is possible to set all the internal parameters of the model. In that case only the task level of the operator has to be defined.

4.3. Conclusion

The screening at an airport checkpoint can be divided into three processes: screening hand-luggage, screening passengers and performing ETD-tests. The hand-luggage is scanned using an X-Ray machine and if something suspicious is detected by the security operator manning the X-Ray, another operator searches the bag. Meanwhile, the passenger moves though a WTMD or body scanner and is subjected to a pat down if the machine gives an alarm. Finally, some passengers are randomly selected for an ETD test.

In each of those processes, employee performance and decision making plays an important role. To model this, a suitable performance model and decision model have been selected. The Functional State Model will be used to model the agents performance based on the complexity of the task he performs and Decision Field Theory will model the agents decision making. Furthermore, a layered model is used as an

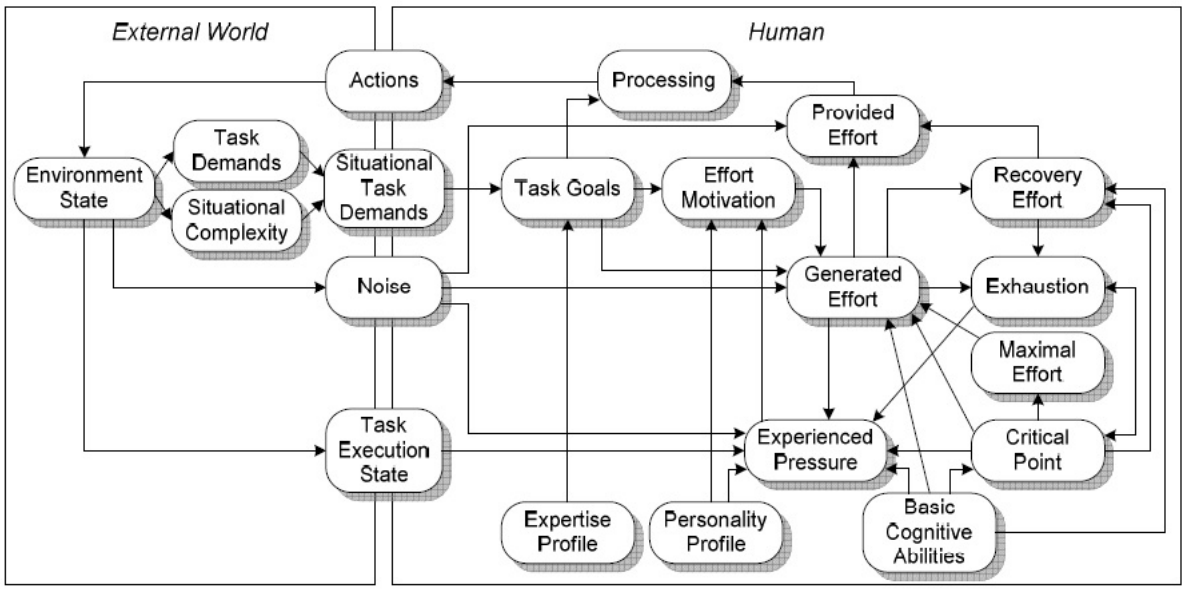


Figure 4.5: Functional State Model

architectural framework in which all the functionalities of the agents will be implemented. The highest level in this model is responsible for the decision making, the middle level for executing activities and the lowest level for interactions with the environment.

5

Agent Based Model

In this chapter an Agent-Based Threat Identification Model of an Airport Checkpoint is presented. This model is a derivation of the AATOM Model, an Agent-Based Model of an Airport Terminal which can be used to study operations in the airport terminal and will also be known as the baseline model for this work [1].

The model as presented in this chapter is an extension of the AATOM Model. In the AATOM Model the security operators have very limited cognitive abilities and this extension focuses on modeling that behaviour. The most significant changes with respect to the baseline model are the implementation of a performance model and decision making model for the operators. This chapter will discuss the most important aspects of the agent based model, as well as all the changes made to the AATOM model.

The model as used in this report is limited to the checkpoint and the rest of the terminal is not modeled. Passengers only pass the checkpoint and when the screening process is finished, the passengers are removed from the simulation.

To model the security checkpoint, first a few simplifying assumptions will be made in Section 5.1. After that, some basic functions to build up the model are introduced in Section 5.2. Next, the changes in environment with respect to the baseline model are described in Section 5.3. Then the agents are discussed in Section 5.4. With both the environment and agents are modeled, the interactions are described in Section 5.5. Finally, Section 5.6 provides an overview of all the input parameters of the model.

5.1. Assumptions

In Chapter 4 the processes at the checkpoint have been discussed as well as the activities and decision points of the security operators. The aim of this chapter is to model these processes, but this cannot be done without making some simplifying assumptions. These assumptions are discussed here. First the assumptions regarding the environment are discussed. After that the assumptions about passengers and the security operators are discussed subsequently.

5.1.1. Environment

To model the environment, the following assumptions are made:

- Complexity is an inherent property of baggage
  - Not every piece of baggage is the same and the complexity of the baggage can have influence on the search time, workload of the operator or detection probability of a weapon hidden in it. In this work baggage can be of low (0) or high (1) complexity.
- If the baggage contains or contained an explosive, the baggage always contains explosive traces.
  - As discussed in 2.1.2, it is possible to erase explosive traces using a solvent, but for now this beyond the scope of the simulation.
- The perceived risk of a prohibited item is the same for every operator
  - This is a simplifying assumption. The risk of a weapon as perceived by the security operator will be very subjective in reality.

- Sensors are always working.
- Sensors have no recovery time.
- X-Ray images have a complexity which is equal to the baggage scanned
  - Not every X-Ray image is the same and the complexity of the image varies based on the baggage scanned. Therefore the complexity of the image is assumed to be the same as the baggage scanned.
- X-Ray images show all the weapons in the bag.
  - In reality not all weapons will be visible. It is easy to make a weapon less visible or invisible using rotation or superposition as discussed in 2.1.2.
- The ETD sensor always detects explosive traces.
  - The ETD technology is extremely reliable and thus this assumption is close to reality.

5.1.2. Passenger

In the agent based model, the following assumptions about passengers are made:

- A passenger will only carry one prohibited item at the time, either in his bag or on his body
- If the passenger has or had an explosive on his body, the passenger always contains explosive traces.
  - As discussed in 2.1.2, it is possible to erase explosive traces using a solvent, but for now this beyond the scope of the simulation.

5.1.3. Security Operators

In this subsection the assumptions regarding the model of the security operators will be presented. First some general assumptions will be introduced and after that the assumptions regarding decision making and activities will be discussed.

- The skill level of the security operator is a fixed property of the operator and independent of the activity.
  - In real life the skill level of the operator may vary per task and increase over time.
- Security operators have a minimum task level.
  - If security operators are not performing an activity, they will not be completely idle. A human is not a computer, which goes to standby if it not used. Even when the security operator will be doing something unrelated to his job, this activity still requires some level of attention. Therefore a minimum task level will be defined for the operators.

Decision Making

- Risk as perceived by the agent is only based on the property 'risk' of the potentially prohibited item that is identified.
  - This is a simplifying assumption, since in reality the agents perception of the passenger may play an important role in the decision making process.
- Baggage is only selected for a search when a potentially prohibited item is identified
  - This is a simplifying assumption, since baggage could be selected for a search for more than one reason. It may be that the X-Ray image is very cluttered due to the superposition of various items or that some items could not be identified.
- If a prohibited item is detected during a pat-down or baggage search, it is confiscated 100% of the time.
  - This assumption probably holds most of the time, but there might be some room for negotiation or items which are in a grey area. However, this is beyond the scope of this model.

- If a security operator is requested to search a bag, this happens 100% of the time.
  - This assumption simplifies the model by removing one of the decision points as specified in 2.2.1
- If a bag is cleared by the X-Ray Operator, this bag is searched 0% of the time.
  - This assumption simplifies the model by removing one of the decision points as specified in 2.2.1
- If an ETD Check is required, this check is performed 100% of the time
  - This assumption simplifies the model by removing one of the decision points as specified in 2.2.1
- If no ETD Check is required, this checked is performed 0% of the time.
  - This assumption simplifies the model by removing one of the decision points as specified in 2.2.1
- If nothing is found during a pat-down, the passenger is always cleared.
  - This assumption simplifies the model by removing one of the decision points as specified in 2.2.1
- If a security officer finds and recognizes guns or explosives during a pat down or baggage search, this will always lead to secondary screening
  - This assumption simplifies the model by removing one of the decision points as specified in 2.2.1
- The beliefs of the security operator are static
- The importance of goals of the security operator are static
- There are three decision criteria involved in each decision the agent makes which are: accuracy, speed and risk

Activities

- Tasks have a fixed complexity

  This is a simplifying assumption. In reality the complexity of a task is something which only exists in our perception and represents our beliefs about how hard a task is.
- Tasks have a fixed duration time
  - In reality the duration time of a task may be dependent on the operator, the complexity or size of a bag etc. Furthermore a task may stop when the operator finds the object he was looking for.
- Average detection probabilities of weapons on X-Ray images are dependent on the baggage complexity, but independent of superposition and rotation of the weapon.
  - As discussed in 2.1.2 the detectability of a prohibited item is dependent on the complexity of the bag, superposition and rotation of the weapon.
- The average detection probability of weapons during a pat down is a constant value. (independent of the passenger, the location on the body and the type and size of weapon)
- The average detection probability during a baggage search is a constant value. (independent of the baggage complexity, size of the baggage and size of the weapon)

5.2. Function Definitions

In this section the basic functions to build up the agent based model are introduced. First some functions are introduced to access properties of objects and. After that, two functions dealing with stochastic processes are introduced. The section ends with two generic functions which are used throughout the model as well.

5.2.1. Basic functions in the model
The most basic function in the model is the function to read the properties of objects:

- $property(\boldsymbol{object})$
  - Returns the *value* of the *property* of the specified *object*.

Apart from this generic function, any object can contain its own functions. These functions can only be used for the object in which they are defined.

5.2.2. Stochastic Processes
Some of the processes which are described in the model, have a stochastic component. In these stochastic progresses a number will be drawn from a random distribution. Based on this draw, a particular action is chosen.

- $draw\_from(\boldsymbol{distribution})$
  - Returns a number draw from the distribution which is given as input. In this report the distribution *uniform_distribution* is used, which is represented by $U(0,1)$

5.2.3. Other functions
In this subsection two additional functions are introduced which will be used repeatedly in the model.

- $empty(\boldsymbol{value})$
  - Returns a Boolean which is true if *value* is not set and false otherwise.
- $pos(\boldsymbol{value})$
  - Returns *value* if it is bigger than 0 and 0 otherwise.

5.3. Environment
The environment in this model is specified to be a checkpoint within an airport terminal. This environment is derived from the AATOM Model and this Section describes the changes with respect to this baseline model.

The environment in the baseline model consist of three base components which are: $Area$, $Flight$ and $Physical\ Object$. In this model many areas specified in this model are not used, since it is specifically focused at the checkpoint. Furthermore, the flight a passenger takes is not relevant either. The base component physical object remains untouched, but some of it sub-components have changed, which are the $Baggage$ and $Sensor$. Furthermore two sub-components are added which are known as $Weapon$ and $X-Ray\ Image$.

In this section first the changes in $Baggage$ are discussed in Subsection 5.3.1. After that, the new sub-component $Weapon$ is introduced in Subsection 5.3.2. Then the new sub-component $X-Ray\ Image$ is introduced in subsection 5.3.3. Finally, the changes in sub-component $Sensor$ are discussed in Subsection 5.3.4.

5.3.1. Baggage
Baggage is a transparent and non-blocking object that is described by the following property vector.

$$\text{Property Vector Baggage} \begin{pmatrix} \text{Complexity} & c \\ \text{Explosive Traces} & e \end{pmatrix}$$

The property vector contains three properties:

- *Complexity (c)*
  - Property that indicates the complexity of the baggage. It can take the values *low* or *high*.
- *Explosive Traces (e)*
  - Boolean value which tells whether the baggage contains explosive traces.

Apart from the properties defined above, baggage is also defined by the following relations.

- $is\_owned\_by(\boldsymbol{baggage}, \boldsymbol{passenger})$
  - The baggage is owned by a passenger and has one relation of this type.
- $contains(\boldsymbol{baggage}, \boldsymbol{weapon})$
  - This relation specifies the weapon the baggage contains. A bag can have one suck relation. The inverse relation is $is\_located\_at(\boldsymbol{weapon}, \boldsymbol{object})$

Finally, the following functions are defined:

- $number\_of\_searches(\boldsymbol{baggage})$
  - Integer value which represents the number of times the baggage is searched.
- $weapon\_in(\boldsymbol{baggage})$
  - This function returns the type of weapon related to the bag.

5.3.2. Weapon

A Weapon is a transparent and non-blocking object that is described by the following property vector.

$$\text{Property Vector Weapon} \begin{pmatrix} \text{Name} & n \\ \text{Explosive Traces} & e \\ \text{Perceived Threat} & p \end{pmatrix}$$

The property vector contains three properties:

- *Name (n)*
  - Property that describes the weapon.
- *Explosive Traces (e)*
  - Boolean value which tells whether the baggage contains explosive traces.
- *Perceived Risk (p)*
  - Value which indicates the perceived risk of the weapon. It is a real value between 0 and 1.

Apart from the properties defined above, weapons are also defined by the following relation:

- $is\_located\_at(\boldsymbol{weapon}, \boldsymbol{object})$
  - The weapon is located at either the *body* of the passenger or in the passengers *baggage*.

Finally, the following function is defined for a weapon:

- $is\_confiscated(\boldsymbol{weapon})$
  - Function which indicates whether the weapon is confiscated. This function contains a Boolean value which is false by default.

5.3.3. X-Ray Image

An X-Ray image is a transparent and non-blocking object that is described by the following property vector:

$$\text{Property Vector X-Ray Image}\big(\text{Bag Complexity} \quad b\big)$$

The property vector contains one property:

- $BagComplexity\,(b)$
  - Positive numerical value which expresses the complexity of the image.

Furthermore one function is defined for an X-Ray image:

- $weapon\_on(\boldsymbol{xray})$
  - Function which contains the weapon type captured on the image. If the image does not contain a weapon, the type is not set.

5.3.4. Sensor

Four types of sensors are defined: the WTMD sensor, Body Scan sensor, X-Ray sensor and ETD sensor. Each of the sensors are non-blocking and transparent. For each sensor, the following standard functions are defined:

- $sensed(object)$
  - Sensor observing an object. This object could either be a passenger or baggage. The sensor is a Boolean which takes the value true if something is observed.
- $detection\_probability\_of(weapon, sensor)$
  - The chances of detecting a weapon are dependent on the interaction between the sensor and the weapon. This function contains a value between 0 and 1 which reflects that probability.

WTMD Sensor

The Walk Through Metal Detector is a sensor that detects metal. The observation of the WTMD is represented by a Boolean value. The value is true if metal is observed and else the observation is false.

$$\begin{aligned} & sensed\big(\boldsymbol{passenger}\big) \quad \twoheadrightarrow_{[0,0,1,1]} \quad draw\_from\big(\boldsymbol{uniform\_distribution}\big) \\ \leq \quad & detection\_probability\_of\big(weapon\_on\big(\boldsymbol{passenger}\big), \boldsymbol{wtmd\_sensor}\big) \quad \wedge \quad \boldsymbol{wtmd\_observation} \end{aligned}$$

Body Scan Sensor

A Body Scanner is a sensor that detects suspicious areas on the human body. The observation of the sensor is represented as a Boolean value, with false meaning nothing is detected and true meaning at least one suspicious area is detected.

$$\begin{aligned} & sensed\big(\boldsymbol{passenger}\big) \quad \twoheadrightarrow_{[0,0,1,1]} \quad draw\_from\big(\boldsymbol{uniform\_distribution}\big) \\ \leq \quad & detection\_probability\_of\big(weapon\_on\big(\boldsymbol{passenger}\big), \boldsymbol{body\_scanner\_sensor}\big) \\ & \wedge \quad \boldsymbol{body\_scanner\_observation} \end{aligned}$$

X-Ray Sensor

The X-Ray sensor observes two properties of the baggage: the complexity and the weapons in the baggage. This output of this observation is an X-Ray image.

$$sensed(\boldsymbol{baggage}) \twoheadrightarrow_{[0,0,1,1]} \quad complexity(\boldsymbol{x\_ray\_image}, complexity(\boldsymbol{baggage})) \\ \wedge \quad weapon\_on(\boldsymbol{x\_ray\_image}, weapon\_in(\boldsymbol{baggage}))$$

ETD Sensor

The Explosive Trace Detector (ETD) is a sensor that is used to detect the presence of explosive traces. The observation of the ETD sensor is represented by a Boolean value. If explosive traces are detected, the observation is *true*, else the observation is *false*

$$\boldsymbol{etd\_observation} = has\_explosive\_traces(\boldsymbol{baggage}) \quad \vee \quad has\_explosive\_traces(\boldsymbol{passenger})$$

5.4. Agents

The model consists of three types of agents: passengers, operators and security operators. This section will focus on the description of the security operator. The description of the passengers and operators will be limited to the changes compared to the baseline model.

5.4.1. Characteristics

In this subsection the characteristics of the agents are described. This is done for the passenger agent first, and then for the security operator.

Passenger

Passengers are agents for which no characteristics are defined, but the passenger is defined by one relation:

- $contains(\boldsymbol{passenger}, \boldsymbol{weapon})$
  - This relation specifies the weapons the baggage contains. In theory this could be more than one. The inverse relation is $is\_located\_at(\boldsymbol{weapon}, \boldsymbol{object})$

Furthermore, two functions are defined:

- $has\_explosive\_traces(\boldsymbol{passenger})$
  - Boolean value which describes whether the passenger contains explosives traces. This value is set to true when the passenger has a weapon which contains explosive traces. When the weapon is confiscated, this value remains true.
- $has\_secondary\_screening(\boldsymbol{passenger})$
  - Boolean value which describes whether the passenger is selected for additional screening. This value is false by default and can be set to true by the security operators.

Security Operator

A security operator is an agent that is responsible for the execution of security policies at the security checkpoint. The security operator is defined by the following feature vector:

$$\text{Feature Vector Security Operator} \begin{pmatrix} \text{Assignment} & s \\ \text{Personality Type} & p \\ \text{Skill Level} & sl \\ \text{Goals Importance} & g \end{pmatrix}$$

The following fixed properties of a security operator are defined:

- *Assignment (s)*
  - The task the employee is supposed to do. The possible assignments are: $xray\_officer$, $baggage\_checking$, $wtmd\_officer$, $body\_Scanner\_officer$.
- *Personality Type (p)*
  - An integer value which is either 1 and 2. The personality of an agents sets the underlying parameters of the Functional State Model which is described in 5.4.3. The values of these underlying parameters are specified in A.
- *Skill Level (sl)*
  - Value between 0 and 1 which reflects the employees ability to perform his task at the checkpoint. It is assumed that his skill level is the same for all tasks. Employees with a high skill level will consider the level of task to be lower compared to employees with a low skill level.
- *Goal Importance (g)*
  - Set of values between 0 and 1 which describe the importance of each of the agents goals. These goals are described in Subsection 5.4.4.

Next to that, a function is defined for operators:

- $task\_complexity\_of(\boldsymbol{security\_operator})$
  - Positive numerical value which represents the complexity of the activity an employee is currently performing. These activities are discussed in Subsection 5.4.3

5.4.2. Operational Layer

The operational layer is the lowest layer in the model and responsible for the interactions with other agents and the environment. The layer consists of a perception module to observe and an actuation module which allows the agent to act. Both modules will be discussed subsequently.

Perception Module

The perception module is responsible for the observation of agents. All observations are described using the following function:

$$obs(\boldsymbol{observation\_type})$$

In this Subsection the observations of the security operators will be discussed, because these differ slightly from the baseline model. For the other agents the AATOM Model still holds.

- $obs(\boldsymbol{passenger})$
  - The security operators with the assignments $wtmd\_officer$, $body\_scanner\_officer$ and $baggage\_searching$, observe passengers at the corresponding area.
- $obs(\boldsymbol{baggage})$

  - The security operator with the assignment $baggage\_searching$, observes the baggage in the corresponding area.

- $obs(\boldsymbol{x\_ray\_image})$

  - The security operator with the assignment $xray\_officer$ observes X-Ray images.

- $obs(\boldsymbol{wtmd\_observation})$

  - The security operator with the assignment $wtmd\_officer$, observes the output of the WTMD which is a Boolean value.

- $obs(\boldsymbol{body\_scanner\_observation})$

  - The security operator with the assignment $body\_scanner\_officer$, observes the output of the body scanner which is a Boolean value

- $obs(\boldsymbol{search\_request})$

  - The security operator with the assignment $baggage\_searching$, can observe a search request communicated by the security operator manning the X-Ray. This request is always for a specific bag.

Actuation Module

The actuation module allows the agent to perform actions which influence the environment. A security operator can perform two actions:

- $search\_request(\boldsymbol{baggage})$

  - This action can be performed by the security operator with the assignment $xray\_officer$ and can be observed by the security operator with the assignment $baggage\_searching$

- $confiscate(\boldsymbol{weapon})$

  - This action removes the weapon from the baggage or body of the passenger and can be performed by the security operator with the assignments $wtmd\_officer$, $body\_scanner\_officer$ and $baggage\_searching$.

5.4.3. Tactical Layer

The tactical layer is responsible for executing activities. The performance on these activities is determined by the functional state of the agent.

The tactical layer as described in this subsection only holds for the security operators and consists of two modules. The first module is the performance module which contains the functional state of the agent. This state is updated continuously depending on the experienced task level. The second module in this layer the actuation module which is responsible for executing activities. Both modules are discussed in detail below.

Performance Module

The agents performance is modeled using the Functional State Model as introduced in 4.2.3. The following feature vector is defined for the functional state model:

$$\text{Feature Vector Performance Module} \begin{pmatrix} \text{Basic Cognitive Abilities} & BCA \\ \text{Current Contribution} & CC \\ \text{Critical Point} & CP \\ \text{Effort Motivation} & EM \\ \text{Exhaustion} & E \\ \text{Experienced Pressure} & EP \\ \text{Experienced Pressure Change} & EPC \\ \text{Experienced Pressure Influence} & EPI \\ \text{Exhaustion Sensitivity} & ES \\ \text{Generated Effort} & GE \\ \text{High Effort Sensitivity} & HES \\ \text{High Pressure Sensitivity} & HPS \\ \text{Lowest Critical Point} & LCP \\ \text{Low Effort Sensitivity} & LES \\ \text{Low Pressure Sensitivity} & LPS \\ \text{Maximum Effort} & ME \\ \text{Optimal Experienced Pressure} & OEP \\ \text{Performance Effort} & PE \\ \text{Performance Norm} & PN \\ \text{Performance Quality} & PQ \\ \text{Performance Sensitivity} & PS \\ \text{Recovery Effort} & RE \\ \text{Top Maximum Effort} & TME \end{pmatrix}$$

The following features define the agents performance:

- *Basic Cognitive Abilities* (*BCA*)
  - Positive numerical value which quantifies the agents cognitive abilities in absence of exhaustion.
- *Current Contribution* (*CP*)
  - Positive numerical value which quantifies how much effort an agent wants to generate.
- *Critical Point* (*CP*)
  - Positive numerical value which quantifies the current cognitive abilities of the agent.
- *Effort Motivation* (*EM*)
  - Positive numerical value which quantifies the current motivation of the agent to generate effort.
- *Exhaustion* (*E*)
  - Positive numerical value which quantifies the exhaustion as experienced by the agent.
- *Experienced Pressure* (*EP*)
  - Positive numerical value which quantifies the pressure as experienced by the agent
- *Experienced Pressure Change* (*EPC*)
  - Positive numerical value which quantifies the change in experienced pressure.
- *Experienced Pressure Influence* (*EPI*)
  - Positive numerical value which quantifies the influence of experienced pressure on the agents effort motivation
- *Exhaustion Sensitivity* (*ES*)

  - Positive numerical value which quantifies the agents sensitivity to exhaustion. A higher sensitivity leads to a higher experienced pressure change.

- *Generated Effort* (*GE*)
  - Positive numerical value which quantifies the effort generated by the agent.
- *High Effort Sensitivity* (*HES*)
  - Positive numerical value which quantifies the agents sensitivity to generated efforts above the critical point. A higher sensitivity leads to a higher experienced pressure change.
- *High Pressure Sensitivity* (*HPS*)
  - Positive numerical value which quantifies the sensitivity of the agent to pressures above the optimal experienced pressure. The higher this sensitivity, the lower the agents effort motivation.
- *Lowest Critical Point* (*LCP*)
  - Positive numerical value which quantifies the agents cognitive abilities in case of maximum exhaustion.
- *Low Effort Sensitivity* (*LES*)
  - Positive numerical value which quantifies the agents sensitivity to generated efforts below the critical point. A higher sensitivity leads to a higher experienced pressure change.
- *Low Pressure Sensitivity* (*LPS*)
  - Positive numerical value which quantifies the sensitivity of the agent to pressures below the optimal experienced pressure. The higher this sensitivity, the lower the agents effort motivation.
- *Maximum Effort* (*ME*)
  - Positive numerical value which quantifies the maximum effort an agent can generate at that moment.
- *Optimal Experienced Pressure* (*OEP*)
  - Positive numerical value which quantifies the pressure at which the effort motivation of the agent is maximized.
- *Performance Effort* (*PE*)
  - Positive numerical value which quantifies the effort the agent spends on performing its task
- *Performance Norm* (*PN*)
  - Positive numerical value which expresses the norm the agent has for his performance quality.
- *Performance Quality* (*PQ*)
  - Positive numerical value which quantifies the quality with which the agent performs its tasks.
- *Performance Sensitivity* (*PS*)
  - Positive numerical value which quantifies the agents sensitivity to performance quality. A higher sensitivity leads to a higher experienced pressure change.
- *Recovery Effort* (*RE*)
  - Positive numerical value which quantifies the effort the agents spends on recovering from exhaustion.
- *Top Maximum Effort* (*TME*)

– Positive numerical value which quantifies the maximum effort an agent can generate in absence of exhaustion.

Furthermore, the following function is defined for the performance module:

- $update(\boldsymbol{task\_level})$
  - This function is used after each time-step to updates the agents state.

$$EP(t+dt) = EP(t) + Pos(\mu_1 \cdot EPC \cdot (1-EP)) + Pos(\mu_2 \cdot EPC \cdot EP)) \cdot dt$$

Experienced Pressure (EP) is the pressure the agent experiences. This is a continuous function which is updated based on the Experienced Pressure Change (EPC). In this equation μ_1 and μ_2 are scaling factors. The function $Pos(x)$ means the maximum of either 0 or x. The parameter dt is the time interval between updates.

$$E(t+dt) = E(t) - \pi \cdot RE \cdot dt + Pos(\eta \cdot (GE - CP) \cdot dt)$$

Exhaustion (E) is effected by the Recovery Effort (RE) of the agent and the Generated Effort (GE). Recovery Effort will decrease the Exhaustion, where Generated Effort will cause an increase if it is above a Critical Point (CP). In this equation the parameters π and η are scaling factors.

$$CP = LCP + (1-E) \cdot (BCA - LCP)$$

The Critical Point represent the agents current cognitive abilities. It is linearly dependent on Exhaustion and is bounded by two parameters: the Lowest Critical Point (LCP) and the Agents Basic Cognitive Abilities (BCA). Both are characteristics of the agent.

$$ME = LCP + \zeta \cdot (CP - LCP)$$

The Maximum Effort (ME) is the maximum effort an agent can generate dependent on his exhaustion. The agent can generate scales linearly with the Critical Point and has its lower boundary set by the Lowest Critical Point. In this equation ζ is the scaling factor.

$$TME = LCP + \zeta \cdot (BCA - LCP)$$

The Top Maximum Effort (TME) is the Maximum Effort an agent can generate in absence of exhaustion. In that case the Critical Point is equal to the agents Basic Cognitive Abilities.

$$EPI = 1 - ((HPS \cdot Pos(EP - OEP)) + LPS \cdot Pos(OEP - EP)$$

The Influence of Experienced Pressure (EPI) is the influence of experienced pressure on the agents effort motivation. Its magnitude is dependent on the difference between Experienced Pressure and Optimal Experienced Pressure (OEP). If the Pressure deviates from the optimal point, the Influence of Experienced Pressure will be effected by the agents Sensitivity for High and Low Pressure (HPS and LPS).

$$EM = EPI \cdot \left(\frac{1 + \frac{1}{\gamma}}{1 + \gamma \cdot e^{-\phi \cdot TL}} - \frac{1}{\gamma} \right)$$

Effort Motivation (EM) is the motivation of an agent to ut effort into the task. Its magnitude depend on the Influence of Experienced Pressure and the Task Level. γ and ϕ are shape parameters of the function

$$CC = \epsilon \cdot \frac{ME}{TME} \cdot EM \cdot (w1 \cdot CP + w2 \cdot TL + w3 \cdot ME)$$

The Current Contribution to the Effort Generated (CC) is the effort an agents wants to put in at the current moment. Its value is dependent on Task Level, the Critical Point and Maximum Effort. The contribution of each of those parameters is weighted with the parameters $w1$, $w2$ and $w3$.
The outcome of this is scaled with the agents Effort Motivation and the ratio between Maximum Effort and Top Maximum Effort. In this equation ϵ is a scaling parameter.

$$GE(t+dt) = GE(t) + \beta \cdot (CC - GE(t)) \cdot dt$$

Generated Effort is the total effort generated by the agent. It is modeled as a continuous function which is updated based on the difference between Current Contribution and Generated Effort. The parameter β is a scaling factor.

$$RE = pos(\alpha \cdot (CP - GE)) \cdot GE \cdot ((BCA - CP)/BCA)$$

Recovery Effort (RE) is the effort an agent spend on recovering from Exhaustion. This can be done when the Generated Effort is below the critical point. Recovery Effort linearly increases when the Generated Effort moves away from the critical point. The recovery effort also linearly increases with the distance between the Critical Point and the Agents Basic Cognitive Abilities. The parameter α is a scaling factor.

$$PE = GE - RE - NE$$

Performance Effort (PE) is the effort an agent spends on performing his tasks. It is calculated by subtracting the Recovery Effort from the Generated Effort.

$$PQ = PE/TL$$

Performance Quality (PQ) quantifies the current performance of the agent on his tasks. This value depends on the relation between the Performance Effort and Task Level. If the Task Level increases the Performance Effort should increase as well to maintain the same Performance Quality

$$EPC = ES \cdot E - PS \cdot (PQ - PN) + HES \cdot \frac{Pos(GE - CP)}{BCA - LCP} - LES \cdot \frac{Pos(CP - GE)}{BCA - LCP}$$

The Experienced Pressure Change is the change in pressure the agent experienced due to several factors. these factors are: Exhaustion, Perceived Performance and the agents sensitivity to High and Low Efforts. Perceived Performance is the difference between the Performance Quality and the agents Performance Norm (PN). All contributing factors are scaled with the agents sensitivity for these factors (*S)

Activity Module

Security operators can perform four different activities. All of these activities have the feature vector:

$$\text{Feature Vector Activity} \begin{pmatrix} \text{Duration Time} & T \\ \text{Task Complexity} & TC \end{pmatrix}$$

- *Duration Time (T)*
  - The time an activity is going to take.
- *Task Complexity (TC)*
  - Positive numerical Value which represents the complexity of a task

Furthermore, there is one relation which defines an activity:

- $average\_detection\_probability(\boldsymbol{activity}, \boldsymbol{weapon})$

– Value between 0 and 1. The average detection probability of a weapon during an activity, relates the weapon and the activity.

Finally there are three functions defined for an activity:

- $state\_of(\boldsymbol{activity})$
  - The state of the activity. This can be either *not_started*, *in_progress* or *has_finished*.
- $result\_of(\boldsymbol{activity})$
  - The result of the activity. The possible results depend on the activity.
- $detection\_probability\_of(\boldsymbol{activity}, \boldsymbol{weapon})$
  - This function maps the average detection probability to the actual detection probability based on the agents current performance quality and returns this value. The probability is calculated as:

$$pos\left(1 - \frac{1 - average\_detection\_probability\_of(\boldsymbol{activity}, \boldsymbol{weapon})}{\boldsymbol{scaling\_factor} \cdot performance\_quality(\boldsymbol{security\_operator})}\right)$$

    In this function the detection probability increases when PQ increases. To make sure the expected value of the detection probability, E(detection probability) is equal to the average detection probability, a scaling factor is introduced. This factor has to be chosen such that E(Scaling Factor * PQ) = 1. This value will be determined during the Calibration of the model in Section.

    The resulting probability should be in the interval (0,1). To ensure that these boundaries are not violated the function *pos* is used. Without this function, the detection probability could theoretically drop below zero. For the upper bound no additional constrains are needed, since the function itself bounds the maximum detection probability to 1.

    6.2.1.

The activities a security operator can perform, are discussed in detail below.

X-Ray Handling X-Ray handling is the activity in which a security employee searches an X-Ray image for prohibited items. The activity is modeled as a waiting period and the outcome of the activity can either be $is\_cleared$ or $continue\_screening$.

The activity starts when an X-Ray image is observed by the security operator. In that case the activity is in progress and the task complexity is set to the complexity of the x-ray image.

$$obs(\boldsymbol{x\_ray\_image}) \rightarrow_{[0,0,1,get\_duration\_time(\boldsymbol{x\_ray\_activity})]} state\_of(\boldsymbol{x\_ray\_activity}, \boldsymbol{in\_progress}) \wedge task\_complexity\_of(\boldsymbol{security\_operator}, task\_complexity\_of(\boldsymbol{x\_ray\_image}))$$

When the $x\_ray\_activity$ has been in progress for the predefined duration time, the activity is finished.

$$state\_of(\boldsymbol{x\_ray\_activity}, \boldsymbol{in\_progress}) \rightarrow_{[0,0,get\_duration\_time(\boldsymbol{x\_ray\_activity}),1]} state\_of(\boldsymbol{x\_ray\_activity}, \boldsymbol{has\_finished})$$

The activity result is set when the activity is finished and is dependent on a stochastic process. A number is drawn from a uniform distribution between 0 and 1 and if this number is bigger than the probability of detection, nothing is detected and the passenger is cleared. Otherwise the screening process continues.

$$
\begin{aligned}
& state\_of(\textbf{x\_ray\_activity}, \textbf{has\_finished}) \quad \twoheadrightarrow_{[0,0,1,1]} \\
& \quad (draw\_from(\textbf{uniform\_distribution}) \\
\leq \quad & detection\_probability\_of(weapon\_on(\textbf{x\_ray\_image}), \textbf{x\_ray\_activity}) \\
& \quad \wedge \quad result\_of(\textbf{x\_ray\_activity}, \textbf{continue\_screening})) \\
& \quad \vee \quad \textbf{otherwise}\ result\_of(\textbf{x\_ray\_activity}, \textbf{is\_cleared})
\end{aligned}
$$

Baggage Checking Baggage Checking is an activity in which a security operator searches a bag for prohibited items. The activity is modeled as a waiting period and the outcome of the activity can be $nothing\_detected$ or $item\_confiscated$.

The activity starts when the security operator observes both a search request and the corresponding baggage. In that case the activity state is set to in progress and the task complexity of the operator is set to the task complexity for this task.

$$
\begin{aligned}
& obs(\textbf{search\_request}) \quad \wedge \quad obs(\textbf{baggage}) \quad \twoheadrightarrow_{[0,0,1,get\_duration\_time(\textbf{x\_ray\_activity})]} \\
& \quad state\_of(\textbf{bag\_search\_activity}, \textbf{in\_progress}) \\
\wedge \quad & task\_complexity\_of(\textbf{security\_operator}, get\_task\_complexity(\textbf{bag\_search\_activity}))
\end{aligned}
$$

In the case of the International Airport, the security operator assigned to checking bags rescans the bags himself. In that case a new baggage searching activity can be triggered by his own decision:

$$
\begin{aligned}
& result\_of(\textbf{bag\_search\_decision}, \textbf{search\_baggage}) \quad \twoheadrightarrow_{[0,0,1,get\_duration\_time(\textbf{x\_ray\_activity})]} \\
& \quad state\_of(\textbf{bag\_search\_activity}, \textbf{in\_progress}) \\
\wedge \quad & task\_complexity\_of(\textbf{security\_operator}, task\_complexity\_of(\textbf{bag\_search\_activity}))
\end{aligned}
$$

The activity is finished when the duration time of the activity reaches a predefined time limit. At that point the activity state is set to $has\_finished$

$$
\begin{aligned}
& state\_of(\textbf{bag\_search\_activity}, \textbf{in\_progress}) \\
\twoheadrightarrow_{[0,0,get\_duration\_time(\textbf{bag\_search\_activity},1)]} \quad & state\_of(\textbf{bag\_search\_activity}, \textbf{has\_finished})
\end{aligned}
$$

The activity result is set when the activity is finished and is dependent on whether a weapon is detected and confiscated during the search. If nothing is detected, the result is set to $nothing\_detected$, otherwise the activity result is set to $item\_confiscated$.

$$
\begin{aligned}
& state\_of(\textbf{bag\_searching\_activity}, \textbf{has\_finished}) \\
& \quad \twoheadrightarrow_{[0,0,1,1]} \quad (draw\_from(\textbf{uniform\_distribution}) \\
> \ & detection\_probability\_of(\textbf{bag\_searching\_activity}, \textbf{weapon}) \\
& \quad \wedge \quad result\_of(\textbf{bag\_searching\_activity}, \textbf{nothing\_detected})) \\
\vee \quad & \textbf{otherwise}\ result\_of(\textbf{bag\_searching\_activity}, \textbf{item\_confiscated})
\end{aligned}
$$

Physical Checking The Physical Checking activity is an activity in which a security operator pat downs a passenger.The activity is modeled as a waiting period and the result of the activity can be $is\_cleared$ or $item\_confiscated$

The Physical Checking activity is started when the security operator observes the alarm from the WTMD or Body Scanner and the passenger.

$$\begin{aligned} & obs(\textbf{wtmd\_observation}) \quad \wedge \quad obs(\textbf{passenger}) \\ \rightarrow\!\!\!\!\!\rightarrow_{[0,0,1,get\_duration\_time(\textbf{pat\_down\_activity})]} \quad & state\_of(\textbf{pat\_down\_activity}, \textbf{in\_progress}) \\ \wedge \quad task\_complexity\_of(\textbf{security\_operator}, task\_complexity(\textbf{pat\_down\_activity})) & \end{aligned}$$

$$\begin{aligned} & obs(\textbf{body\_scanner\_observation}) \quad \wedge \quad obs(\textbf{passenger}) \\ \rightarrow\!\!\!\!\!\rightarrow_{[0,0,1,get\_duration\_time(\textbf{pat\_down\_activity})]} \quad & state\_of(\textbf{pat\_down\_activity}, \textbf{in\_progress}) \\ \wedge \quad task\_complexity\_of(\textbf{security\_operator}, task\_complexity(\textbf{pat\_down\_activity})) & \end{aligned}$$

The physical checking activity is ended after a predefined duration time:

$$\begin{aligned} & state\_of(\textbf{pat\_down\_activity}, \textbf{in\_progress}) \\ \rightarrow\!\!\!\!\!\rightarrow_{[0,0,get\_duration\_time(\textbf{pat\_down\_activity}),1]} \quad & state\_of(\textbf{pat\_down\_activity}, \textbf{has\_finished}) \end{aligned}$$

The result of the pat down is determined when the activity is finished and depends on whether a prohibited item is found and confiscated. If nothing is found case, the result is set to $is\_cleared$, otherwise the result is set to $item\_confiscated$

$$\begin{aligned} & state\_of(\textbf{pat\_down\_activity}, \textbf{has\_finished}) \\ \rightarrow\!\!\!\!\!\rightarrow_{[0,0,1,1]} \quad & (draw\_from(\textbf{uniform\_distribution}) \\ > \; & detection\_probability\_of(\textbf{pat\_down\_activity}, \textbf{weapon}) \\ \wedge \quad & result\_of(\textbf{pat\_down\_activity}, \textbf{is\_cleared})) \\ \vee \quad \textbf{otherwise} \; & result\_of(\textbf{pat\_down\_activity}, \textbf{item\_confiscated}) \end{aligned}$$

ETD Checking The ETD Checking activity is an activity in which a passenger is scanned for explosive traces. The activity is modeled as an activity that happens instantly.

If a passenger is observed, which has not been checked yet, there is a change $etd\_check\_probability$ that the passenger is selected for an ETD Check. If this is the case, the activity is started. Else the activity is considered as finished.

$$\begin{aligned} & obs(\textbf{passenger}) \\ \rightarrow\!\!\!\!\!\rightarrow_{[0,0,1,1]} \quad & draw\_from(\textbf{uniform\_distribution}) < \textbf{etd\_check\_probability} \\ \wedge \quad & state\_of(\textbf{etd\_activity}, \textbf{in\_progress}) \end{aligned}$$

If the activity state is in progress, it is set to $is\_finished$. The result of the activity depends on whether the passenger or the baggage contains explosive traces.

$$\begin{aligned} & state\_of(\textbf{etd\_activity}) = \textbf{in\_progress} \\ \rightarrow\!\!\!\!\!\rightarrow_{[0,0,1,1]} \quad obs(\textbf{etd\_observation}) \quad \wedge \quad & result\_of(\textbf{etd\_activity}, \textbf{secondary\_screening}) \\ \vee \quad \textbf{otherwise} \; & result\_of(\textbf{etd\_activity}, \textbf{is\_cleared}) \end{aligned}$$

5.4.4. Strategic Layer

In the AATOM model, the strategic layer for passengers is developed. This model supplements the that model by adding a strategic layer for security operators. The strategic layer of security operators is responsible for agents decision making in the screening process. The outcome of these decisions determine the next step in the screening process.

The operators decisions are based on his goals which serve as decision criteria in the decision making process. These goals can be conflicting and are discussed in the Goal Module. Furthermore, in each decision the beliefs of the operator play an important role. These beliefs are discussed in the Beliefs Module. Based on the goals and beliefs of the operator, a decision is made. The reasoning process behind this decision is discussed in the Reasoning Module.

Goal Module

The goal module contains the goals of the security operator. These goals are criteria in the agents decision making and have one property:

- *Goal Importance (i)*
  - Value between 0 and 1 which expresses the importance of the goal to the agent.

There are three goals defined for the security operator. These will be discussed in detail below. For each of the goals, the importance is an input variable of the model. There may be lots of factors which influence this value, but this is beyond the scope of this model.

Accuracy The security operator wants to do his work as well and accurate possible. The importance of this goal may be dependent on pressure within the organizations or the agents own standards.

Speed The agents wants to do his job as fast as possible. The importance of this goal may be due to pressure within the organization to reach a certain throughput or the security operator wanting to minimize effort.

Perceived Risk It is the job of the security operator to minimize the risk of an attack. Perceived risk represents the beliefs an agent has about the potential consequences of the observed prohibited item. The importance of this goal may be dependent on the agents beliefs about the likelihood of an attack and his risk aversion.

Belief Module

The belief module is the module that contains the beliefs of the security operators. It is assumed that these beliefs are fixed and thus will not be updated based on new observations.

There are two types of beliefs which are defined in this module: initial beliefs and goal related beliefs. Both will be discussed in detail below

Initial Beliefs An initial belief is the preference an agent has for an outcome of a decision before thinking about it. This is known as a gut feeling based on past experiences.

An initial belief has the function:

- $initial\_preference\_for(\boldsymbol{outcome})$
  - Numerical Value which expresses the agents initial preference for a given outcome.

The Initial Preference is defined for each outcome

Goal Related Beliefs A Goal related belief expresses the belief of the agent about the relation between a goal and a possible outcome. The belief itself has no properties, but is defined as a relation between a decision outcome and a goal.

- $valence\_of(\boldsymbol{goal}, \boldsymbol{outcome})$
  - Numerical value which expresses the belief of the agent about to what extend the option helps in reaching the goal.

Reasoning Module

The reasoning module of the security operators is responsible for their decision making. The decision model used in this module is decision field theory which was introduced in 4.2.2. The decision making process is described by the feature vector:

$$\text{Feature Vector Decision Model} \begin{pmatrix} \text{Threshold} & t \\ \text{Outcomes} & o \\ \text{Choice} & c \end{pmatrix} \tag{5.1}$$

The features are described as follows:

- *Threshold (t)*
  - Positive numerical value which expresses the strength of the agents preference when a decision is made.
- *Outcome (o)*
  - Set of all possible outcomes of a decision. This set is dependent on the type of decision
- *Choice (c)*
  - The outcome which is chosen

Furthermore, three functions are defined:

- $state\_of(\boldsymbol{decision})$
  - The state of the decision. This can be either *not_started, in_progress* or *has_finished.*
- $preference\_for(\boldsymbol{decision}, \boldsymbol{outcome})$
  - Numerical value which expresses the strength of the agents preference for each outcome.
- $attention\_for(\boldsymbol{decision})$
  - Goal on which the agent is currently focused. An agent can be focused on one goal at the time. The goals are: *speed, accuracy, perceived_risk*

Finally, one method is defined in the decision module. This method updates the agents preference for a certain outcome:

- $update\_preference\_for(\boldsymbol{decision}, \boldsymbol{outcome}, \boldsymbol{valence})$
  - This method updates the agents preference for an outcome with:

$$preference\_for(\boldsymbol{decision}, \boldsymbol{outcome}) = preference\_for(\boldsymbol{decision}, \boldsymbol{outcome}) + valence$$

The trigger to initiate a decision making process depends on the type of decision. Once the decision making process is in progress, the preference for each outcome is set to the initial preference for that outcome and the threshold value is set based on the agents performance effort.

$$\begin{aligned} state\_of(\textbf{decision}, \textbf{in\_progress}) \quad \wedge \quad & empty(preference\_for(\textbf{decision}, \textbf{outcome})) \\ \twoheadrightarrow_{[0,0,1,1]} \quad & preference\_for(\textbf{decision}, \textbf{outcome}, initial\_preference\_for(\textbf{outcome})) \\ \wedge \quad & threshold(\textbf{decision}, performance\_effort\_of(\textbf{security\_operator})) \end{aligned}$$

If the preference for one of the outcomes is bigger than the threshold value, that outcome will be the result of the decision and the decision making process is finished.

$$\begin{aligned} state\_of(\textbf{decision}, \textbf{in\_progress}) \quad \wedge \quad & preference\_for(\textbf{decision}, \textbf{outcome}) \geq threshold(\textbf{decision}) \\ \twoheadrightarrow_{[0,0,1,1]} \quad & choice(\textbf{decision}, \textbf{outcome}) \quad \wedge \quad state\_of(\textbf{decision}, \textbf{has\_finished}) \end{aligned}$$

If none of the preferences reach the threshold value, the decision making process continues. In that case the agent attention is focused on one of his goals. This is determined by a stochastic process. A number is drawn from a uniform distribution on the interval 0 to 1 and based on the number drawn from this distribution and the importance of each of the goals, the attention of the security operator is set to one of the three goals as discussed in 5.4.4.

$$\begin{aligned} & state\_of(\textbf{decision}, \textbf{in\_progress}) \twoheadrightarrow_{[0,0,1,1]} \\ & draw\_from(\textbf{uniform\_distribution}) \leq importance\_of(\textbf{accuracy}) \\ & \wedge \quad attention\_for(\textbf{decision}, \textbf{accuracy}) \\ \vee \quad & importance\_of(\textbf{perceived\_risk}) < draw\_from(\textbf{uniform\_distribution}) \\ & \wedge \quad attention\_for(\textbf{decision}, \textbf{perceived\_risk}) \\ & \vee \quad \textbf{otherwise}\ attention\_for(\textbf{decision}, \textbf{speed}) \end{aligned}$$

If the decision making process is in progress and the preference is set, the preference for each outcome is updated based on the goal related beliefs of the agent.

$$\begin{aligned} state\_of(\textbf{decision}, \textbf{in\_progress}) \quad \wedge \quad & \neg empty(preference\_for(\textbf{decision}, \textbf{outcome})) \\ \twoheadrightarrow_{[0,0,1,1]} \quad & state\_of(\textbf{decision}, \textbf{in\_progress}) \\ \wedge \quad update\_preference\_for(\textbf{decision}, \textbf{outcome}, & valence\_of(attention\_of(\textbf{decision}), \textbf{outcome})) \end{aligned}$$

The security operator can perform three decision processes, depending on his assignment. Those three decision processes are discussed in detail below.

Bag Search Decision The decision to search a bag is made by the security operator assigned to the X-Ray machine (or by the officer checking bags at the International Airport).

The possible outcomes are *is_cleared* or *search_baggage*. In the first case, the baggage is cleared, otherwise the baggage is searched.

The decision making process is triggered when a potentially prohibited item is detected on the x-ray image:

$$\begin{aligned} & result\_of(\textbf{x\_ray\_activity}, \textbf{continue\_screening}) \\ \twoheadrightarrow_{[0,0,1,1]} \quad & state\_of(\textbf{bag\_search\_decision}, \textbf{in\_progress}) \end{aligned}$$

If the X-Ray officer decides the bag should be checked, the officer assigned to baggage checking is alerted.

$$result\_of(\textbf{bag\_search\_decision}, \textbf{search\_baggage}) \quad \twoheadrightarrow_{[0,0,1,1]} \quad search\_request(\textbf{baggage})$$

Rescan Decision This decision is made by the security operator assigned to searching the bag. The decision to rescan a bag is made when the baggage is searched and nothing is found.

$$\begin{aligned} & result\_of(\textbf{bag\_search\_activity}, \textbf{nothing\_detected}) \\ \wedge \quad & number\_of\_checks(\textbf{baggage}) \leq max\_number\_of\_checks \\ & \twoheadrightarrow_{[0,0,1,1]} \quad state\_of(\textbf{rescan\_decision}, \textbf{in\_progress}) \end{aligned}$$

The activity is finished when the operator makes a decision. The possible outcomes are $is\_cleared$ or $needs\_rescan$. In the first case, the baggage is cleared, else it is scanned by the x-ray again.

Secondary Screening Decision This decision is made by security operator with the assignments $wtmd\_officer$, $body\_scanner\_officer$ or $baggage\_searching$ and is initialized when a prohibited item is confiscated.

$$\begin{aligned} & result\_of(\textbf{bag\_search\_activity}, \textbf{item\_confiscated}) \\ \twoheadrightarrow_{[0,0,1,1]} \quad & state\_of(\textbf{secondary\_screening\_decision}, \textbf{in\_progress}) \end{aligned}$$

$$\begin{aligned} & result\_of(\textbf{pat\_down\_activity}, \textbf{item\_confiscated}) \\ \twoheadrightarrow_{[0,0,1,1]} \quad & state\_of(\textbf{secondary\_screening\_decision}, \textbf{in\_progress}) \end{aligned}$$

The decision is made when one of the preferences reaches the threshold value. The possible outcomes are $is\_cleared$ or $secondary\_screening$.

5.5. Interactions

Agents interact with each other and the environment. These interactions are described in Section REF of the AATOM Model. This section contains the changes and additional interactions with respect to that model.

5.5.1. Agent - Environment

There is one addition to the agent - environment interaction in the AATOM model:

- Security operator with the assignment $wtmd\_officer$, $body\_scanner\_officer$ or $baggage\_checking$ with weapon
  - The relation is modeled as follows:

$$activity\_result(\textbf{activity}, \textbf{item\_confiscated}) \quad \twoheadrightarrow_{[0,0,1,1]} \quad remove(\textbf{weapon})$$

5.5.2. Agent - Agent

There is one change with respect to the interactions in the AATOM model:

- Security operator $xray\_officer$ with security operator $baggage\_checking$
  - The relation is modeled as follows:

$$\begin{aligned} & choice\_of(\textbf{bag\_search\_decision}, \textbf{search\_baggage}) \\ & \twoheadrightarrow_{[0,0,1,1]} \quad search\_request(\textbf{baggage}) \end{aligned}$$

5.6. Input Parameters

To use the model, all input parameters have to be set. This section provides an overview of all the input parameters of the model.

5.6.1. Checkpoint Parameters

For a checkpoint, two parameters have to be set:

- $Maximum\ Number\ of\ Rescans$
- $ETD\ Check\ Probability$

5.6.2. Environment

There are three elements in the environment which require input parameters. These elements are: baggage, weapons and sensors. Each of those will be discussed subsequently.

Baggage

For each piece of baggage, one parameter has to be set:

- $Complexity$ (c)

Next to that, the baggage is connected to a $passenger$.

Weapon

Three weapon parameters are identified:

- $Name$ (n)
- $Explosive\ Traces$ (e)
- $Risk$ (r)

Furthermore the weapon location is set to be either in the $baggage$ or on the $passenger$.

Sensor

For each type of sensor, the detection probability is set for each type of $weapon$.

5.6.3. Security Operator

For each security operator, the following parameters are set:

- $Assignment$ (s)
- $Personality\ Type$ (p)
- $Skill\ Level$ (sl)

Apart from these parameters, some of the operators modules have input parameters as well. These will be listed by module below.

Activity Module

For each activity two parameters have to be set as input:

- $Duration\ Time$ (t)
- $Task\ Complexity$ (tc)

Furthermore, for each activity the $average\ detection\ probability$ is set for each type of $weapon$.

Goal Module

For each of the goals the following property is defined:

- $Goal\ Importance\ (i)$

Belief Module

For each of the outcomes for each decision the following property is set:

- $Initial\ Preference\ (i)$

Furthermore, for each combination of $outcome$ and $goal$ a valence is defined.

6

Analysis & Experiments with the Checkpoint Model

In this chapter the experiments performed with the model of Chapter 5 are discussed. Three sets of experiments have been performed with the following goals:

- Experiment 1: Understanding the dynamics of the behavioural models
- Experiment 2: Calibrating the behavioural models
- Experiment 3: Quantifying vulnerabilities for a pre-defined set of threat scenarios and analyze the role of employees in the emergence of these vulnerabilities.

The first set of experiments is discussed in Section 6.1 and is aimed at getting a better understanding of the behavioural models which are implemented. In those experiments, the dynamics of the models are studied based on varying input parameters and analyzing the output. These experiments form the basis for the calibration of the input variables. The second set of experiments is aimed at calibrating the performance and decision models for all tasks and decisions of the security operators. This is the topic of Section 6.2. The third and final experiment is used to quantify vulnerabilities for a pre-defined set of threat scenarios and analyze the role of employees in the emergence of these vulnerabilities. This experiment is discussed in Section 6.3.

6.1. Analyzing the Behavioural Models

The aim of this section is to get a better understanding of the behavioural models that are implemented in the agent based model of the security operators. This analysis will be the basis to calibrate those models in the next section.

In this section first the relation between input and output of the functional state model is analyzed in Subsection 6.1.1, after that the Decision Making Model is analyzed in Subsection 6.1.2.

6.1.1. Functional State Model

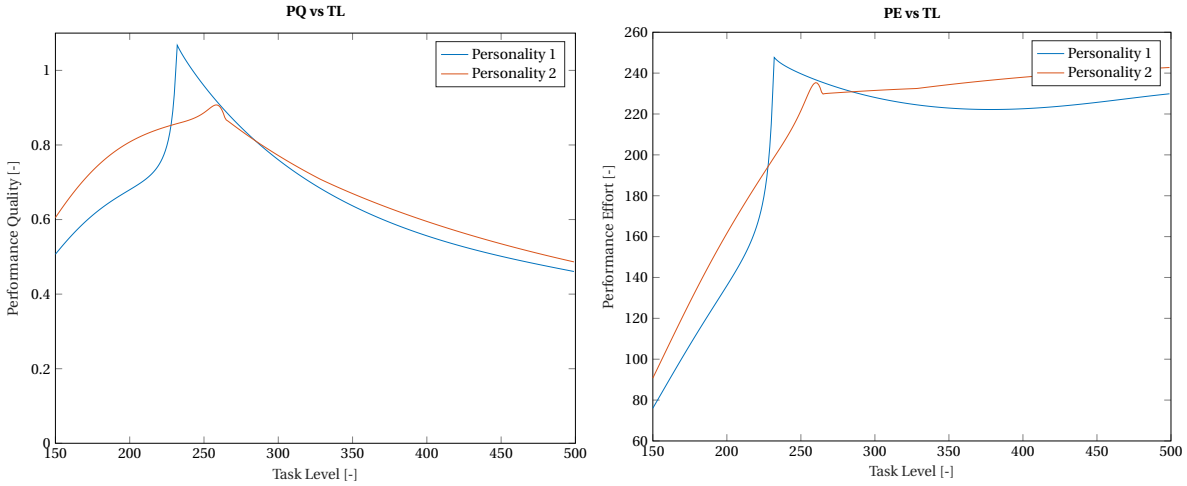
The functional state model is used to model the performance of the security operator. This model is introduced in 4.2.3 and the mathematical description can be found in Section 5.4.3.

Setup

The only input of the model is the Task Level (TL). This input is calculated by dividing the Task Complexity (TC) by the Skill Level (SL) of the agent:

$$TL = \frac{TC}{SL} \tag{6.1}$$

The output parameters of the model are the Performance Effort (PE) and Performance Quality (PQ). Performance Effort is the effort an agent puts into its task and is also used as the threshold value in his decision



(a) Performance Quality vs. Task Level

(b) Performance Effort vs. Task Level

Figure 6.1: Input Output relations of the Functional State Model

making. Performance Quality is an abstract value which is translated to detection probabilities as discussed in 5.4.3.

The analysis of the FSM will be limited to the input and output of the model. An extensive verification of the model has already been performed by the authors [14]. From this study two example personality types are defined which are Personality Type (PT) I and II. These types will be used in this report as well. The main difference between PT I and PT II is that PT II experiences more stress. The parameters corresponding with these PTs can be found in Appendix A.

Results

Figure 6.1a shows the relation between input and output of the FSM for both PTs after the TL is kept constant for 20 seconds. At this point in time the PQ is converged to an equilibrium value for any value of TL. From the figure it is clear that both PT I and II have a small range in which PQ is optimal . For both personalities this is the range around a task level of 250. The peak performance of PT I is at TL = 230, at this point it outperforms PT II by 24%.

At task levels which are below 225 the PQ of both personalities rapidly drop. This is mainly due to a lack of PE as can be seen in figure 6.1b. In this range PT II outperforms Type I by 20%.

At task levels above 275 the performance of both personalities exponentially decreases. The performance effort of both agents stays approximately levelled around a PE of 230, which means that the agent cannot generate more effort. The TL keeps increasing, which leads to a drop in performance quality.

6.1.2. Decision Model

Decision field theory was introduced in 4.2.2 and the formal description is given in 5.4.4. To better understand the dynamics of this model a set of experiments is performed. This is done based on two scenarios which are:

- **Scenario 1: Prohibited item detected and perceived as threat**
  - In this scenario, one of the security employees detects a prohibited item and considers this as a threat.
- **Scenario 2: Prohibited item detected but not perceived as threat**
  - In this scenario the security employee also detects a prohibited item, but does not consider the item to be a threat.

In both scenarios the employee has to decide between following protocol or breaking the rules. For both scenarios, all the parameters which effect the outcome of the decision making process are studied separately. The aim of this is to develop an understanding of how the outcome is effected by the input parameters. To do this, the following case studies will be performed:

Table 6.1: Scenario 1 - DFM Parameters: prohibited item detected, and perceived as threat

	Initial Preference	**Valences**		
Option 1: Continue Screening	*0*	*30*	*-30*	*30*
Option 2: Clear Passenger	*0*	*-30*	*30*	*-30*

Threshold	**Attention Weight**		
U(70, 250)	*0.333*	*0.333*	*0.334*
	Accuracy	Speed	Risk

- **Number of Iterations as function of Valence**
  - The purpose of this case study is to investigate how the number of iterations changes with valence. An increase in iterations corresponds with an increase in decision time
- **Choice as function of Valence**
  - The choice of an option depends on the magnitude of the valences. When the valences increases, the decision threshold will be reached faster, which means that the agent did spend less time on its decision and the choice will be less thought through.
- **Choice as function of Attention Weight**
  - By shifting the attention weight of the security operators, some decision criteria become more or less important. The aim of this case study is to investigate how that influences the choice.
- **Choice as function of Initial Preference**
  - The agents initial preference for an option biases the agent toward choosing that option. This case study aims to get a better insight into the relation between initial preference and the option chosen by the agent.

In order to analyze the effect of single input a parameter on the outcome, it is important that all other parameters are kept constant, therefore the default input for all the case studies is specified in Table 6.1 for scenario 1 and in Table 6.2 for scenario 2. This input will be used in each case study, except for the input parameter which is investigated. For both scenarios the threshold value varies between 70 and 250, since this is the range of the performance effort which is used as threshold value. The goals accuracy and risk contribute to the preference for continuing the screening process, where the goal speed increases the preference for clearing the passenger. The scaling factor of 30 is a trade-off between decision time and stability of the decision. Increasing this number will cause the operator to make faster decisions, but results in choosing the best option less often. Decreasing this number will exponentially increase decision time, but the best option will be chosen more often. The value of 30 guarantees that a relatively stable decision is made in an acceptable amount of iterations. The initial preference is set to zero for both cases, since the effect of this parameter will be investigated later in this section.

Iterations vs Valence

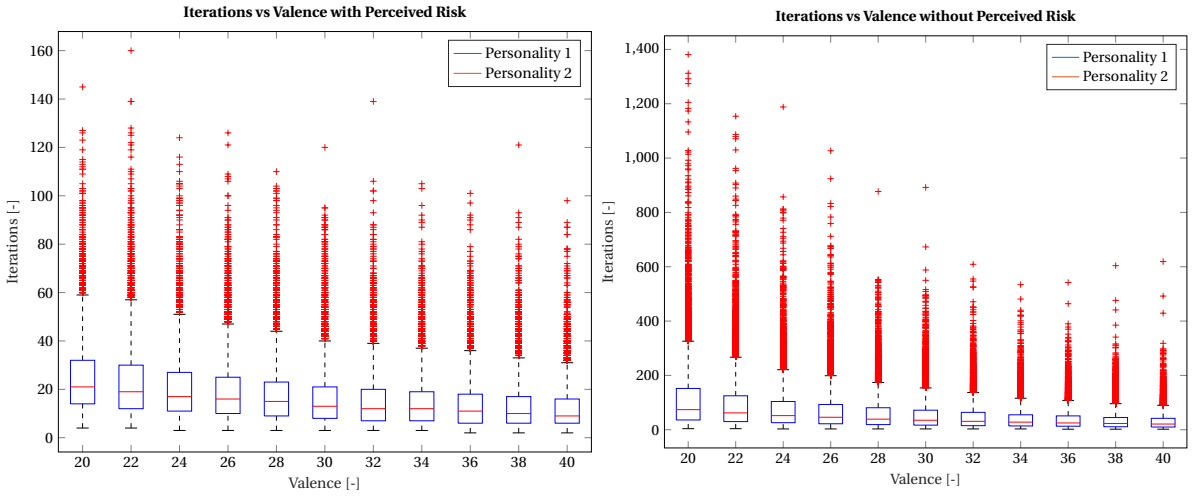
In this case study the number of iterations as a function of valence is investigated for both scenarios. The input as specified for the scenarios is used, except for the valence matrix which will be varied. It is assumed that the valences for all decision criteria are of equal magnitude, except for the valence of risk in scenario 2 which stays 0.

Increasing valences means that the decision threshold can be reached faster, therefore it is expected that the number of iterations decreases when valence increases. Furthermore scenario I is expected to require fewer iterations in order to reach the decision threshold. This is because scenario 1 has a dominant option, whereas in scenario 2 both options are equally good. It is easier to choose an option when one is clearly better,

Table 6.2: Scenario 2 - DFM Parameters: prohibited item detected, but not perceived as threat

	Initial Preference	**Valences**		
Option 1: Continue Screening	*0*	*30*	*-30*	*0*
Option 2: Clear Passenger	*0*	*-30*	*30*	*0*

Threshold	**Attention Weight**		
	Accuracy	Speed	Risk
U(70, 250)	*0.333*	*0.333*	*0.334*



(a) Scenario 1: Prohibited item detected and perceived as threat

(b) Scenario 2: Prohibited item detected but not perceived as threat

Figure 6.2: Number of Iterations as function of Valence

compared to two equally valid options. The range which is investigated are valences of 20-40. The results for scenario 1 and 2 are found in Figure 6.2. Each datapoint in those graphs is the result of 1000 simulations.

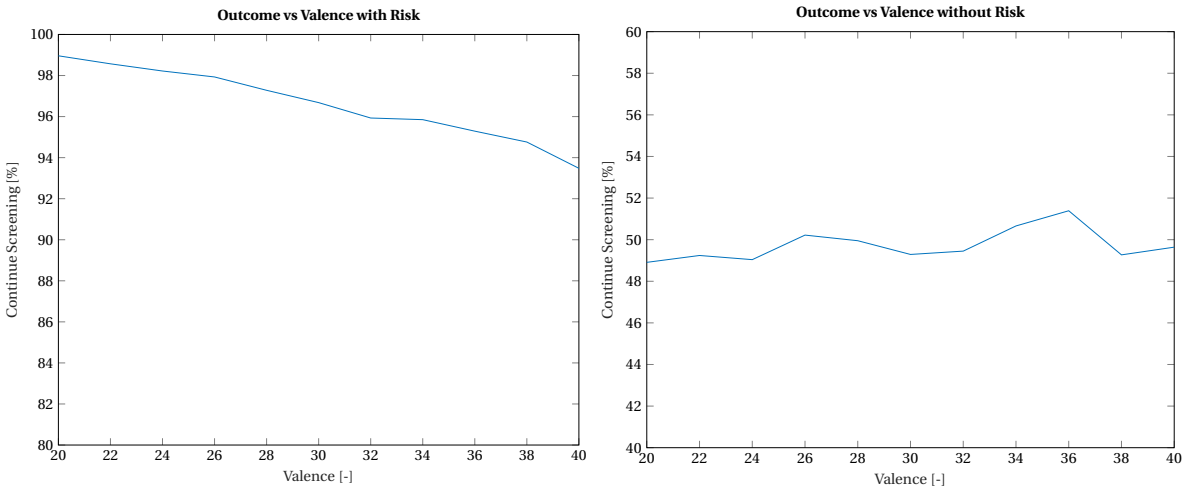
From the figures it follows that the number of iterations indeed decreases when valence increases. Furthermore the number of iterations in scenario 2 are indeed much larger than in scenario 1.

Finally the graphs show a large spread in the number of iterations and numerous outliers. Especially in scenario 2 at low valences the number of iterations gets particularly high. This number of iterations is way too high for decisions which only take seconds. It can be assumed that an iteration takes 300 ms [2], which corresponds to 10 iterations per 3 seconds. In the second scenario, the 75 percentile of valence = 20 is 326. This corresponds with a decision time of 98 seconds, which is way more time than the officers can invest in a decision.

It is clear that the number of iterations must be brought back. this can be done in three ways. First, the valence can be increased to reduce the number of iterations. Second, the initial preference could be increased in the direction of the dominant option. The third option would be to limit the number of iterations. This would mean that decisions could be made based on a time limit instead of reaching a threshold. These choices will be made during the implementation of each decision in 6.2.2.

Choice vs Valence

In this case study the choice as function of valence is investigated for both scenarios. Again, valence is the parameter which is varied. It is expected that the dominant option is chosen more often when the valence decreases. This is because a smaller valence corresponds with a larger number of iterations and when the iterations increase, the chances of choosing the inferior option decreases. The range which is investigated



(a) Scenario 1: Prohibited item detected and perceived as threat

(b) Scenario 2: Prohibited item detected but not perceived as threat

Figure 6.3: Decision Making as function of Valence

are valences of 20-40. The results for scenario 1 and 2 are found in Figure 6.3. Each datapoint in those graphs is the result of 1000 simulations.

From the figure it follows that the option to continue screening is chosen less often in scenario 1 when valence increases. This corresponds with what was expected, since the option to continue screening is the dominant option in this scenario. By increasing the valence, less steps are required to reach the threshold value which makes the decisions making process less stable. Therefore the dominant option to continue screening will be chosen less often.

In Figure 6.3b this trend is not visible. In this figure both options are chosen around 50% of the time over the whole interval. This is because both options are equally good in this scenario, which means that the valence has no effect on the agents choice.

Choice vs Attention Weight

In this case study the choice as function of attention weight is investigated. It is assumed that for each of the three decision criteria the agent can have an attention weight of low (0.333), average (0.5) or high (0.667). After these weights are contributed to each criteria, these are normalized such that the sum of the three weights is 1.

It is expected that increased attention weights for accuracy and risk will lead to an increased preference for continuing the screening process, where an increased attention weight for speed will increase the preference to clear the passenger.

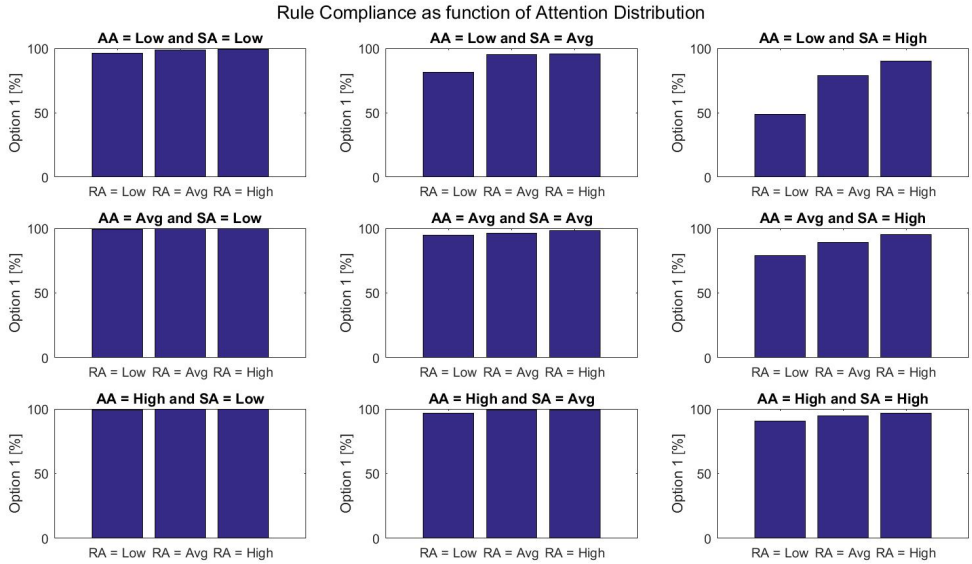
Since there are 3 decision criteria, with three possible attention weights there are 27 possible combinations. Figure 6.4 shows how often the security operators choose to continue screening for each of those combinations. From the figure it follows that screening is indeed continued more often when the attention weight for accuracy and risk are high. Furthermore an increase in attention weight, leads to the screening being discontinued more often. Each datapoint in those graphs is the result of 1000 simulations.

In scenario 1, there is one combination of attention weight in which the screening process is continued in only 50% of the cases. In this scenario the attention weight for speed is high, where the goal importance for both accuracy and risk are low.

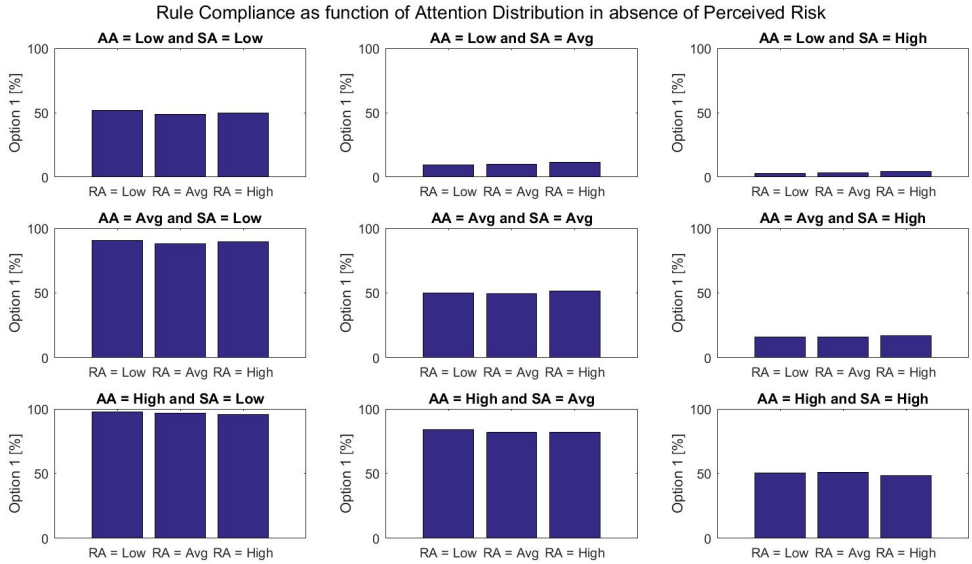
In scenario 2, the goal importance for risk does not play a role. This is because the valence for risk is 0. In this scenario the dominant option is determined by the attention weight for speed and accuracy. If both have the same value, there is no dominant option. Otherwise, the criteria with the highest attention weight is dominant.

Choice vs Initial Preference

In this case study the outcome as function of initial preference is investigated. It is assumed that the initial preference of the agent is a preference to follow protocol and thus continue screening.

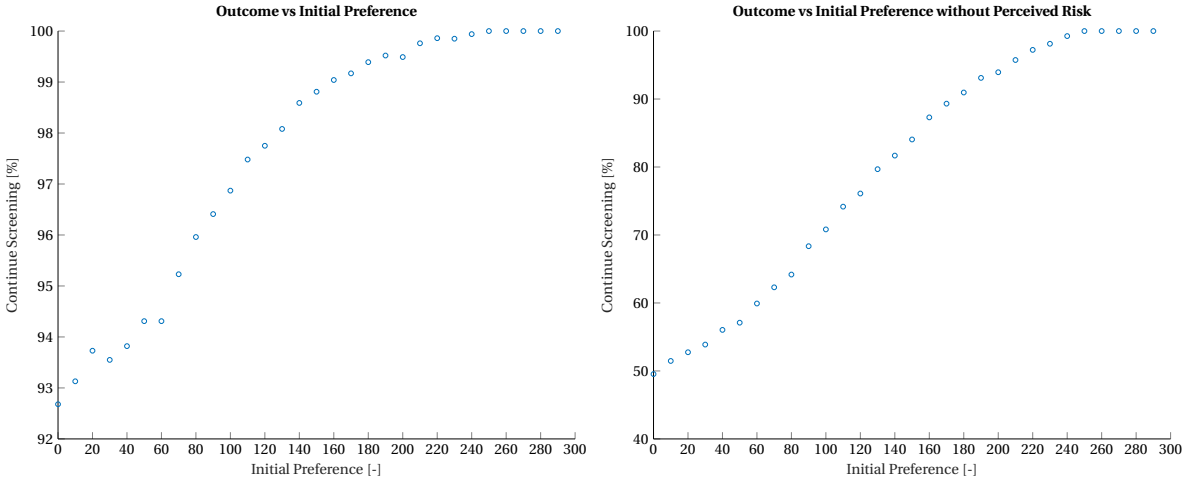


(a) Scenario 1: Prohibited item detected and perceived as threat



(b) Scenario 2: Prohibited item detected but not perceived as threat

Figure 6.4: The effect of the agents attention distribution on rule compliance. In this figure AA = Attention for Accuracy, SA = Attention for Speed and RA = Attention for Perceived Risk



(a) Scenario 1: Prohibited item detected and perceived as threat

(b) Scenario 2: Prohibited item detected but not perceived as threat

Figure 6.5: Decision making as function of Initial Preference

It is expected that an increase in initial preference to continue screening, will result in an increase in the number of times the agents opts to continue screening chosen. The results for both scenarios are found in Figure 6.5. Each datapoint in those graphs is the result of 1000 simulations.

From the figure it follows that both graphs have the same general shape. The choice to continue screening indeed increases from a baseline value to 100% when the initial preference becomes 250. After 250 the operator chooses to continue screening 100% of the time. This is because the initial preference already exceeds the threshold value.

It must be noted that the range of values for both scenarios is different. In Scenario 1, screening is continued 93% of the time without any initial preference. In scenario 2 this is only 50%. This is because scenario 1 has a dominant option, where in scenario 2 both options are equal.

Conclusion

In this section the behaviour of the defender model was investigated. First the Functional State Model was investigated. The developers of this model have defined two example personalities types (PT)in their paper. These PTs will be used as the personalities for the employees in this report. The biggest difference between the two personalities, is that PT I is less prone to stress than PT II.

By analyzing the input and output from the Functional State Model, it was found that there is a small range of Task Levels (TL) in which Performance Quality (PQ) is optimal. This is the range from a TL of 230 to 260. If the TL gets below this range, the tasks are too easy for the agent and the agent will not be able to motivate himself leading to a loss of PQ. If TL gets above this range, the task becomes too hard for the agent and PQ will drop due to the high TL. Furthermore it is found that stress limits peak performance, but increases performance when the task is too easy or hard for the agent.

The second part of this Section analyzed the Decision Field Model. It was found that the number of iterations required to make a decision was dependent on valence and the presence or absence of a dominant option. If valence increased or one option was dominant, the number of iterations decreased. Furthermore it was found that an increase in valence lead to less stable decisions.

The attention weight of the agent also has large influences on the outcome of the decision. A shift in attention weight can even cause a shift in dominant options. Finally, the Initial Preference increases the likelihood an option is chosen.

The results of this Section will be used in implementing the tasks and decisions made by the agents. This will be the topic of the next section.

6.2. Calibration of the model

In this section the agents performance and decision making is calibrated based on the experiments performed in Section 6.1. First the agents performance is set for each task in Subsection 6.2.1. After that, the

decision making process of the agents is implemented in Subsection 6.2.2

6.2.1. Performance

To run the agents based simulation, a task complexity (TC) must be set for any of the tasks a security operator has to perform. These task complexities must be set in such a way that the resulting performance quality (PQ) of the employee matches with the predefined detection probabilities. If the PQ of an employee is too high or too low, the percentage of weapons detected during an activity will not match the average detection probability.

The following parameters are assumed:

- $TL_{idle} = 150$
- $SL = 0.8, 0.9, 1.0$

The Task Level (TL) when an officer is idle is set to 150. While the officer is not performing any work related tasks, it is not a machine which you can switch off, meaning that a task level of 0 is unrealistic. According to Table 6.1a, a Task Level of 150 will result in a PQ which is around 50% of the officers peak performance. This will be taken as a baseline value for all of the security operators at the checkpoint, regardless of their Skill Level (SL).

Furthermore, the SL indicates the officers level of training. In this report three discrete Skill Levels will be assumed. The Skill Level of different officers at the checkpoint is unrelated.

In this subsection the performance of the agents is calibrated for the following tasks:

- Scanning X-Ray images
- Searching Baggage
- Pat Downs

The calibration of the first tasks will be based on data which relates the complexity of x-ray images to performance. For the other tasks more assumptions are needed. Crucial for that is that tasks are ranked in level of difficulty.

In this report is it assumed that Scanning X-Ray images is the most difficult task on a checkpoint. The officer has one second to identify potentially prohibited items in a bag and research has shown that false negatives increase when the images become harder [71].

Bag searching is assumed to be easier than scanning an X-Ray image. The officer already knows what he is looking for and has more time to perform his task.

The easiest task is assumed to be a pat down. The reason for this is that this is considered to be a routine task, since all persons have approximately the same shape. Contrary to that, searching a bag in a systematic way is more challenging since all bags are different.

X-Ray Performance

In this section the performance of security employees on analyzing X-Ray images is calibrated. This is done based on the detection probabilities as described in Table 2.1 and Table 2.2. From these tables it follows that the number of false negatives is related to bag complexity. For each of the weapon categories the increase in false negatives is:

- **Gun:** 8.33%
- **Knife:** 9.68%
- **IED:** 3.85%
- **Other:** 0,00%

In this report the assumption is made that the change in detection rate is only dependent on bag complexity and not on the type of weapon. Therefore the average change in false negatives (FN) over the four categories are taken. When averaging the increase in FN of the four categories of prohibited items we get 5.47%.

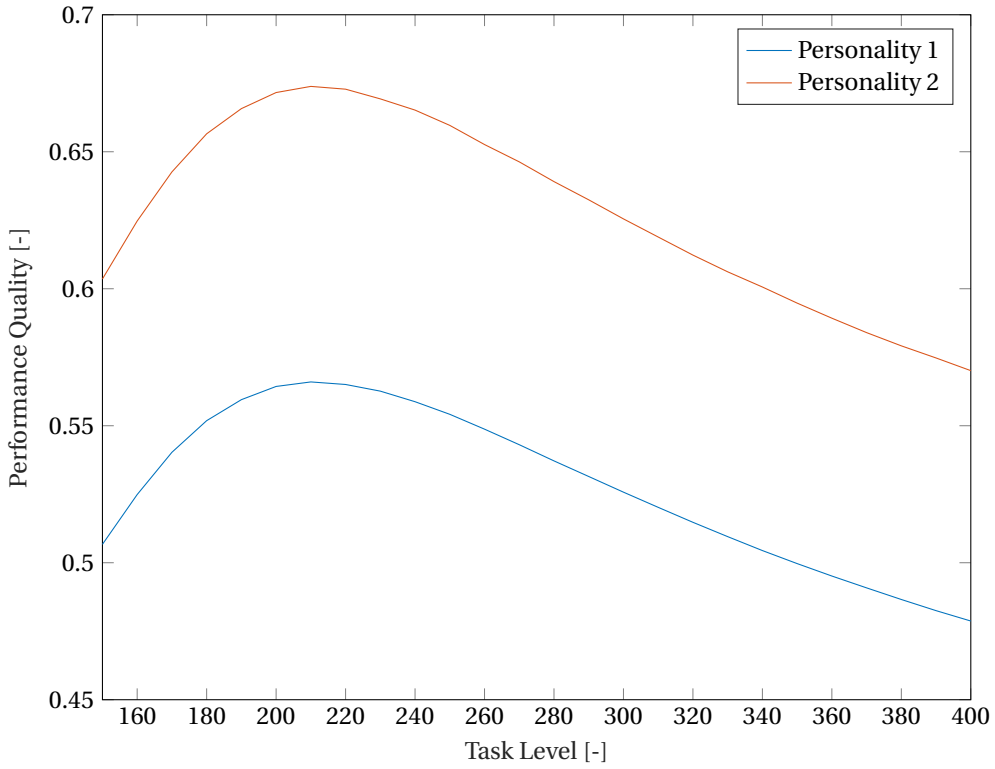


Figure 6.6: PQ as a function of TL for X-Ray images

The number of FN is directly related to PQ by the equation shown below:

$$P(FN) = \frac{P\left(FN\ Average\right)}{Scaling\ Factor \cdot PQ}$$

From this equation it follows that an increase in FN of 5.47% corresponds with a decrease in PQ of 5.18%. The Task Level (TL) is calculated using the equation:

$$TL = \frac{BTC_{XRay} + BC \cdot ITC}{SL} \tag{6.2}$$

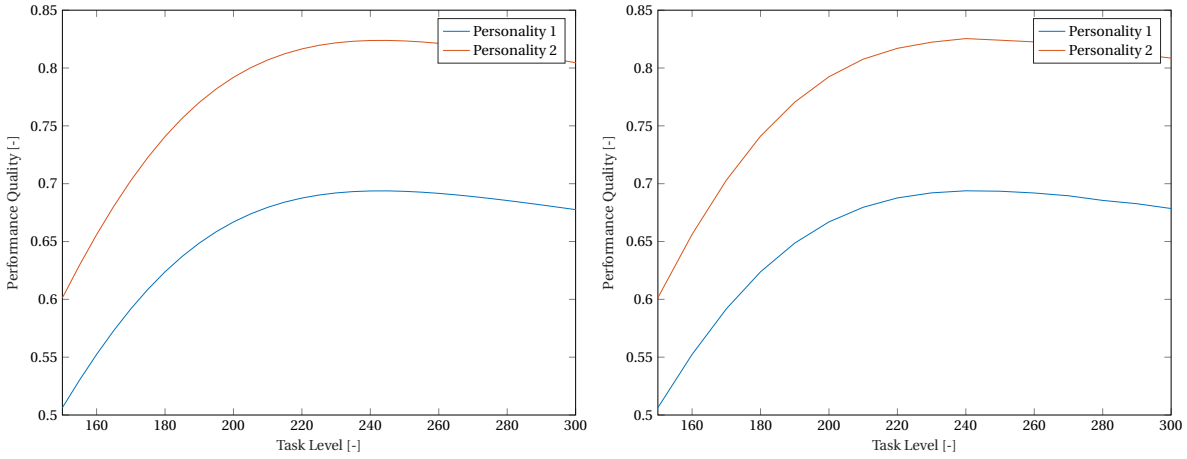
In this equation BTC is the Basic Task Complexity. This parameter is the task complexity of scanning the easiest X-Ray images. BC is the Bag Complexity which indicates the complexity of the X-Ray image. ITC is the Increase in Task Complexity due to the complexity of the image.

In this equation, BC can take the discrete values 0 and 1, in which 0 stands for a bag with low complexity and 1 for a bag with high complexity. Furthermore SL can take the values 1.0, 0.9 and 0.8. The values for BTC and ITC have to be calibrated. To do this, use will be made of the assumed change in detection rates and PQ when bag complexity increases. The relation between TL and PQ is given in figure 6.6.

Note that this figure of PQ vs TL differs from Figure 6.1a. That figure shows the relation between PQ and TL when TL is constant and PQ has reached its equilibrium value. This is not the case in figure 6.6. In this figure the Task Level just changed from the Baseline TL of 150 to the current PQ which are taken are taken 1 second after the change in TL.

Based on this figure, the TL of scanning X-Ray images is determined. In the region where TL is between 150 and 210, PQ increases if TL increases. This is due to a lack of generated effort by the agents as explained in section 6.1.1. From TL is 210 to 400, PQ decreases with TL. This is because the TL becomes so high that the agents can no longer deliver the same quality.

Since an increase in Bag Complexity is associated with a drop in PQ, the range of task levels must be on the right side of the figure. The BTL will be assumed to be 210. Now ITC can be calculated based on the fact that PQ decreases with 5.18% when the bag complexity becomes high instead of low. Based on this information ITC is found to be 53. This value is found by trying a range of values for each combination of SL and Personality Type.



(a) PQ as a function of TL for Checking Bags

(b) PQ as a function of TL for Pat Downs

Finally the Scaling Factor has to be determined such that the expected value $E(Scaling\ Factor \cdot PQ) = 1$. This ensures that the probability of detecting a weapon is indeed equal to the average detection probability. To determine the Scaling Factor the average PQ should be known, which can be calculated by taking all the combinations of Personality Types, SL and BC. This are 12 combinations (2·3·2) with an average PQ of 0.5943. Thus the Scaling Factor becomes 1.68.

Bag Search Performance

In this section the performance of employees performing a bag search is calibrated. It is assumed that this search takes 120 seconds on average. The likelihood of a false negative are given by the equation:

$$P(FN) = \frac{P(FN\ average)}{Scaling\ Factor \cdot PQ} \tag{6.3}$$

In this equation it is assumed that the Scaling Factor is the same as in the previous section. The PQ again is a function of Task Level only. The relation between PQ and TL is given in Figure 6.7a.

Comparing this figure to Figure 6.6, it becomes clear that the values for PQ are much higher during a bag search. The main reason for this is the difference in processing time between the tasks. X-Ray images are scanned in a second while searching a bag takes two minutes. This gives the employee some time to focus on the job and reach a higher PQ. During a bag search the PQ of the employee reaches an equilibrium value, which is not the case during the evaluation of an X-Ray image. Here the PQ is still rising when the evaluation ends

In this report it is assumed that performing a bag search has a task complexity of 200. This makes it slightly easier than searching an X-Ray image. Based on the graph it is expected that the PQ of the agent will be higher than on x-ray images.

Pat down performance

In this section the Pat down performance of agents is calibrated. It is assumed that the Task Complexity of this task is 175 which makes it easier than searching a bag. Furthermore it is assumed that a pat down takes 90 seconds and the PQ is taken at the end of this period.

The relation between TL and PQ for this task is shown in Figure 6.7b. Based on this graph it is expected that employees with a lower skill level will perform better on a pat down. This is comparable to the result found on the bag check performance.

6.2.2. Decision Making

In this section the decision making of agents is calibrated. This is done for three types of decisions which are introduced in 5.4.4:

- **Decision to search a bag**
  - This decision is made by the officer that detected a potentially prohibited item on an X-Ray image.

Table 6.3: Input Parameters Bag Check Decision

	Initial Preference	**Valences**		
Option 1: Check Baggage	*0.95 * PE*	*30*	*-30*	*30 * Perceived Risk*
Option 2: Clear Baggage	*0.0*	*-30*	*30*	*-30 * Perceived Risk*

- **Decision to rescan a bag**
  - This decision is made by the officer searching a bag, when the prohibited item cannot be found.
- **Decision to apply additional screening**
  - This decision is made when an officer confiscates a prohibited item. This could either be during the search of a bag or a pat down.

All decision of agents are based on three decision criteria:

- Accuracy
- Speed
- Perceived Risk

Apart from these decision criteria, a decision can also be influenced by the agents initial preference. In this report it is assumed that the agents initial preference coincides with the protocols as implemented on the checkpoint. The magnitude of this initial preference depends on the type of decision.

Furthermore, the agents valence for each criteria can take values between 0 and 1. These values are multiplied by a scaling factor of 30 to limit the number of iterations and thus the decision time.

Requesting a bag check

If the X-Ray operator detects a potentially prohibited weapon in a bag, he has to decide whether the bag should be checked. The parameters assumed for the decision criteria are listed in Table 6.3.

In this trade-off speed and accuracy have the same valence. Furthermore the valence for perceived threat varies between 0 and 1, depending on the type of weapon found in the bag.

Since the scaling factor is 30, it follows from figure 6.2b that making an autonomous decision in this case can take over 600 iterations if the perceived Risk is close to 0. This is equivalent to three minutes, while in reality a decision is made in a matter of seconds [71].

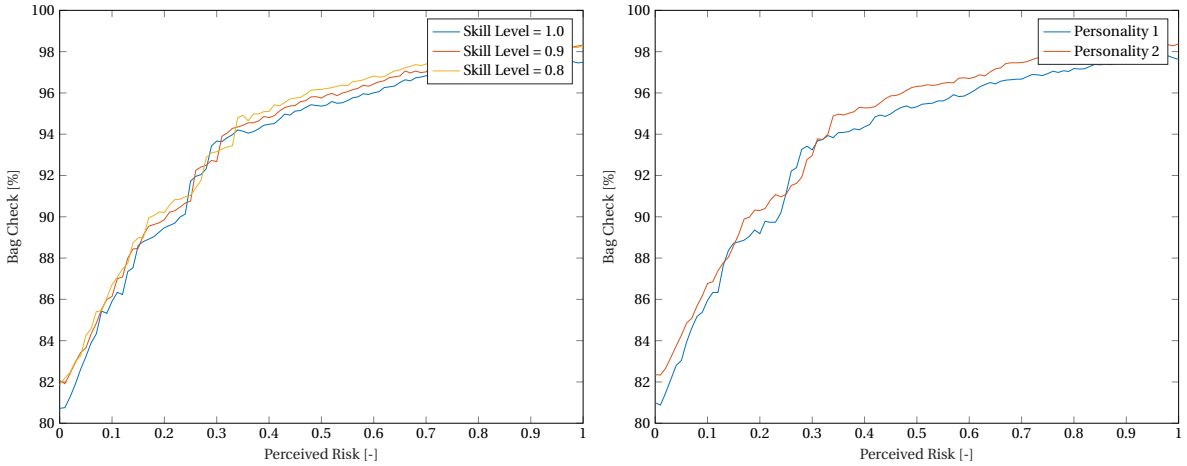
This means that the agent has no time to make a fully autonomous decision, but that his decision will largely be based on initial preference. Since it is his job to select bags which have to be searched, it is assumed that his initial preference will be to search the bags if a potentially prohibited object is detected. Based on this line of reasoning, the Initial Preference is assumed to be 95% of the decision threshold and in favour of option 1.

Figure 6.8 shows that the number of bags which are searched increases when the perceived risk of a prohibited object increases. When there is no perceived risk, the number of bags searched is 82%, which increases to 99% if the perceived risk is largest.

Furthermore there seem to be small differences in decision probabilities between agents of different skill level and personality. The agents with the lowest skill level seem to make the best decisions, as do the agents which experience stress.

The first result is interesting, since the agents with the highest skill level performed better on detecting prohibited items, but apparently the performance effort involved in that, was lower compared to lesser skilled employees. They performed better with less effort, just because the level of the task was lower for them. When it comes to decision making, it is performance effort that counts. The performance effort is related to the threshold value of the decision making process and putting more effort into a decision simply leads to the best option being chosen more often. In this case, lesser skilled employees put more effort in their tasks, and thus make better decisions.

Furthermore employees which experience stress outperform the other employees in making the best decision. This is not surprising since these employees also performed better in finding prohibited items, regardless of skill level. This means the increase in performance is fully caused by increased performance effort, and thus more effort will be put in their decisions as well.



(a) Percentage of Bag Checks for each skill level

(b) Percentage of Bag Checks for each personality type

Figure 6.8: Percentage of Bag checks as function of Perceived Risk

Table 6.4: Input Parameters for a Rescan Decision

	Initial Preference	**Valences**		
Option 1: Check Baggage	*0.0*	*30*	*-30*	*30 * perceived Risk*
Option 2: Clear Baggage	*0.0*	*-30*	*30*	*-30 * Perceived Risk*

Requesting an additional X-Ray scan

If the security operator that is assigned with searching baggage cannot find the item he is looking for, he has to decide whether an additional X-Ray scan is required. This decision is made based on the same criteria as the decision to search a bag. The input parameters are listed in Table 6.4

The difference between the decisions is in the Initial Preference. Searching the bag takes quite some time and this gives the agent the time to think about further actions. Next to that the agent is less inclined to request a rescan. Observations of a checkpoint at Rotterdam The Hague Airport showed that it is very uncommon for a bag to get rescanned, so it seems that there is not a lot of external pressure on the officer to ask for a rescan. Therefore it is assumed that the initial preference is 0% and thus the decision to request a rescan is fully autonomous.

Figure 6.9 shows the number of rescans as function of perceived risk. When there is no perceived risk, 50% of the bags are rescanned, which increases to 94% when the risk is perceived as maximum.

Furthermore there are small differences in decision probabilities between agents with different skill levels and personality types. Again the lesser skilled agents and the agents which are prone to stress outperform the other agents. This is an expected results, since these agents also performed better on identifying potentially prohibited items.

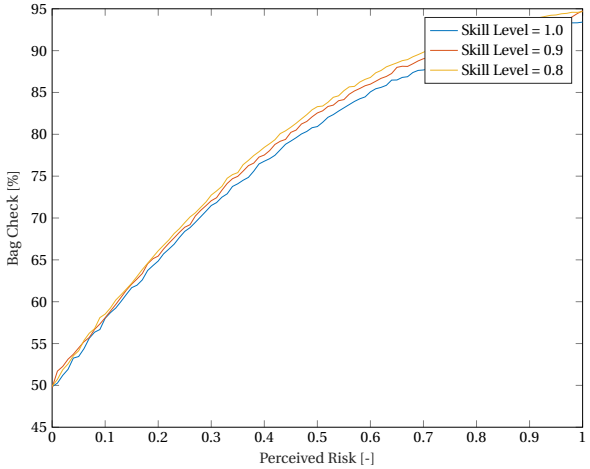
Requesting secondary screening

If a prohibited item is confiscated, the officer has to decide whether additional screening is needed for the passenger. This decision is made based on the criteria of accuracy and perceived threat. It is assumed that a secondary screening has no effect on the throughput of a checkpoint and thus speed is of no importance.

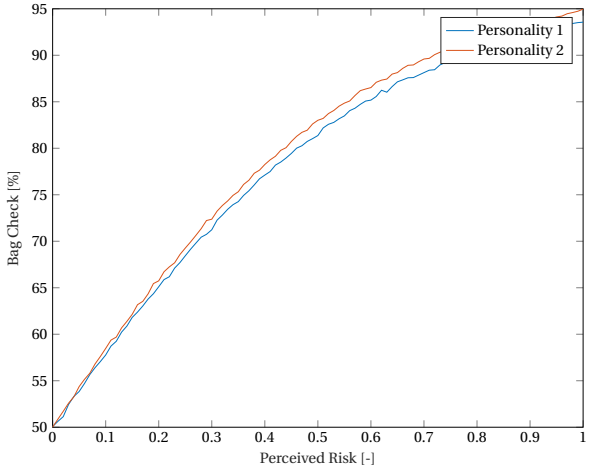
Furthermore the agents valence for the criteria accuracy is in favor of clearing the passenger, unless the weapon is recognized as a bomb or gun. In that case, the agents initial preference will be 100% of the threshold value in favor of secondary screening, so in practice this is not an autonomous decision.

If the weapon is not recognized as a gun or bomb, the initial preference is 0 for both options. The input parameters for this case are listed in Table 6.5.

Figure 6.10 shows the number of secondary screenings as function of perceived risks. The graph is cut of at a perceived risk of 0.4, since only guns and bombs have values above that and confiscation of these weapons immediately lead to secondary screening. In this interval the percentage of secondary screenings increases from 0% to 2% for security operators that are assigned to searching baggage and from 0% to 2.5% for agents



(a) Percentage of Rescans for each Skill Level

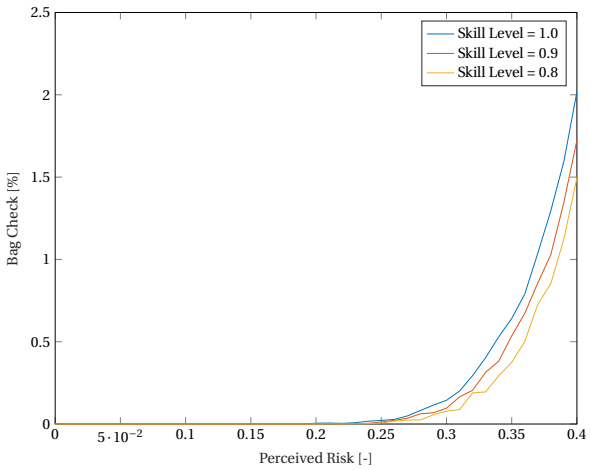


(b) Percentage of Rescans for each Personality Type

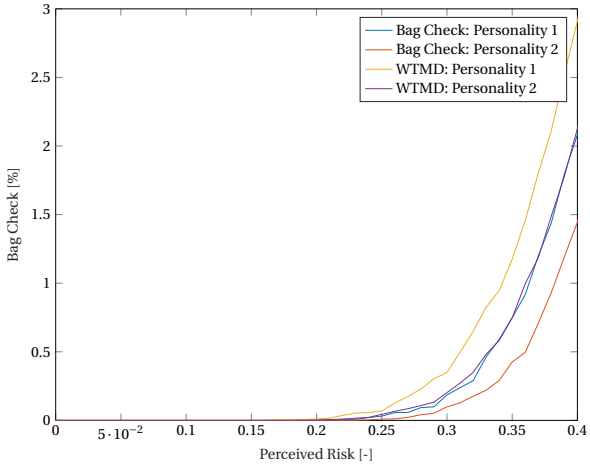
Figure 6.9: Input Output relations of the Functional State Model

Table 6.5: Input parameters for the secondary screening decision if the weapon is not recognized as a big threat

	Initial Preference	**Valences**		
Option 1: Secondary Screening	*0.0*	*-30*	*0*	*30 * Perceived Risk*
Option 2: Clear Passenger	*0.0*	*30*	*0*	*-30 * perceived Risk*



(a) Percentage of Secondary Screenings for each Skill Level



(b) Percentage of Secondary Screenings for each Personality Type

Figure 6.10: Percentage of secondary screenings as function of perceived risk

assigned to the walk through metal detector or body scanner. This difference in result is again explained by the difference in performance effort. Searching a bag is a more difficult task and thus the officers are motivated to put in more performance effort. This results is the officers choosing the dominant option more often. In this case the dominant option is to clear the passenger. Similarly, the agents which experience stress or have a lower skill level put more effort into their work again and thus choose the dominant option more often too.

6.2.3. Conclusion

In this section the task complexities and the agents decision making process was calibrated.

First the task complexities were set based on data of officers analyzing X-Ray images and assumptions about the relation between task complexities. It was assumed that analyzing X-Ray images was the hardest task and performing a pat down the easiest.

Based on this calibration it followed that lesser skilled employees outperformed the highest skilled employees on pat-downs and searching bags. The reason behind this is that these tasks are not challenging enough to highly skilled employees and they are not motivated to put in any effort resulting in poor performance.

After the task complexities are set, the decision making process is calibrated. The officers make their decisions based on the criteria of accuracy, speed and perceived risk. The higher the effort of the agents, the higher the chances the dominant option is chosen.

Some decisions are not fully autonomous though. The decision to search a bag is largely influenced by the agents initial preference in favor of searching the bag. Likewise, if an item gets confiscated which is recognized as a gun or a bomb, the agents decision about secondary screening is fully determined by his initial preference in favor of secondary screening.

With the task complexities set and the agents decision making calibrated, the parameters of the checkpoint model are all set. In the next section the performance of the checkpoint is analyzed.

6.3. Analyzing Checkpoint Performance

In this section the checkpoint performance is analyzed based on 15.000 simulation runs. During each run the following input parameters are varied:

- **Weapon** The weapon the attacker uses is one of the weapons as discussed in Section 5.3.2
- **Weapon Location** The attacker has the option to hide the weapons on his body or in his baggage.
- **Checkpoint Configuration** The checkpoint configuration is either the Regional or International Airport.
- **Skill Level** The skill level of the agents is either 0.8, 0.9 or 1.0. The skill level of each agent is set independent of the other agents.
- **Personality Type** The agents either have personality I or II as described in 6.1.1. The corresponding settings for the functional state model are found in appendix A.
- **Attention Weights** The attention weight for each criteria is set to 0.33, 0.5 or 0.67. The attention weights for each agents are set independent of each other.

Based on the data from the simulation runs, first the influence of input parameters on the PQ of the agents is analyzed in Subsection 6.3.2. After that the agents decisions are related to the attention weights in Subsection 6.3.3. Finally, Subsection 6.3.5 identifies the performance of checkpoints for each threat scenario.

6.3.1. Input Parameters

The input parameters as used for this experiment are discussed here. First the checkpoint parameters are discussed. After that the weapons included in the simulation are introduced. With the weapon introduced, the detection probabilities of the weapons will be set for the sensors and operator tasks subsequently. Finally, the input parameters of the security are introduced.

The following checkpoint parameters are used:

- Configuration = Regional or International

- Maximum number of rescans = 3
- Percentage of ETD Checks = 10%

The passenger can bring the following weapons:

- A fully functional improvised explosive device.
  - Name = Explosive Bulk
  - Contains explosive traces = true
  - Perceived Risk = 1.0
- Liquid explosives which are not recognized as a bomb. Since 2006 people are not allowed to bring liquids through airport security after a bomb plot was discovered involving liquid explosives [21, 51, 70]. The advantage of bringing liquid explosives is that they aren't directly recognizable as explosives.
  - Name = Explosive Liquid
  - Contains explosive traces = true
  - Perceived Risk = 0.1
- Explosives in powder form which are not recognized as a bomb. In 2009 a terrorist successfully smuggled a bomb into a flight from Schiphol to Detroit which contained PETN in the form of powder [26]. One of the problems of this type of explosive, is that it is not necessarily recognized as such.
  - Name = Explosive Powder
  - Contains explosive traces = true
  - Perceived Risk = 0.2
- A handgun.
  - Name = Gun
  - Contains explosive traces = false
  - Perceived Risk = 1.0
- A legal knife. A knife is quite a common item for people to carry and screeners quite frequently come across knives people accidentally carried into their hand luggage. These items are obviously confiscated, but as long as the knife is only prohibited but not illegal, not much will be thought of it.
  - Name = Knife
  - Contains explosive traces = false
  - Perceived Risk = 0.3
- A legal ceramic knife. This weapon ha the same properties as a knife, but does not contain any metal.
  - Name = Ceramic Knife
  - Contains explosive traces = false
  - Perceived Risk = 0.3

The perceived risks for these weapons are an estimate. Bombs and fire-arms are assumed to have the highest perceived risks. However, if a bomb is not recognized as such, the perceived risk is much lower. Especially liquids are probably not considered a big threat since the operators are continuously throwing away water bottles. Knifes are assumed to be a bigger threat, but this is still a very common item to have in your back, so the perceived risk will not be extremely high.

The corresponding detecting probabilities for each combination of weapon and sensor/activity are given in Table 6.6. The values for the sensors and the X-Ray activity are based on the values are discussed in 2.1.2.

Table 6.6: The average detection probability for each sensor and activity

	Explosive Bulk	Explosive Liquids	Explosive Powder	Gun	Knife	Ceramic Knife
WTMD	*0.00*	*0.00*	*0.00*	*1.00*	*1.00*	*0.00*
Body Scanner	*0.56*	*1.00*	*0.00*	*1.00*	*1.00*	*1.00*
X-Ray Activity	*0.735*	*0.645*	*0.645*	*0.875*	*0.675*	*0.675*
Bag Search Activity	*0.90*	*0.90*	*0.90*	*0.90*	*0.90*	*0.90*
Pat Down Activity	*0.90*	*0.90*	*0.90*	*0.90*	*0.90*	*0.90*

Table 6.7: PQ on scanning X-Ray images

	Average PQ [%]	95% Percent CI [%]
Skill Level 0.8	*0.582*	*0.579 - 0.586*
Skill Level 0.9	*0.601*	*0.598 - 0.605*
Skill Level 1.0	*0.612*	*0.608 - 0.616*
Personality I	*0.545*	*0.544 - 0.545*
Personality II	*0.652*	*0.651 - 0.652*

No data could be found on how security operators perform on searching bags and pat downs. Therefore these values are just assumed.

For each of the security operators the following parameters are set:

- Skill Level = 0.8 or 0.9 or 1.0
- Personality Type = 1 or 2
- Goal Importance = 0.33 or 0.5 or 0.67.

The parameter goal importance is set for each of the three goals. After all the three values are set, they are normalized such that they add up to one. After normalizing these values, they serve as the attention weight in the decision model.

During each run, all the input parameters which can take multiple values are randomly assigned. The outcome from all the runs will be analyzed and discussed in the next sections.

6.3.2. Outcome of each activity as function of the agents characteristics

In this Subsection the outcome of activities is investigated as function of the agents characteristics. The two characteristics which influence the Performance Quality of the agent are Skill Level and Personality Type.

Interestingly, time was not a factor in the PQ of the agents on any of the tasks, which means that the agents do not get exhausted by the tasks. This is in line with the nature of the tasks which are described as "boring, repetitive and do present really few challenges for the employee". [53]

In this Subsection, employee performance will subsequently be discussed for the tasks:

- Scanning an X-Ray image
- Searching a bag
- Performing a pat down

X-Ray Scanning

The performance of officers on scanning an X-Ray image can be found in Table 6.7. As can be seen, PQ significantly increases with Skill Level. The agents with the highest skill level outperform the agents with the lowest skill level with 5.2%.

Table 6.8: PQ on scanning X-Ray images continuously

	Average PQ [%]	**95% Percent CI [%]**
Skill Level 0.8	*0.694*	*0.688 - 0.701*
Skill Level 0.9	*0.731*	*0.725 - 0.738*
Skill Level 1.0	*0.758*	*0.751 - 0.764*
Personality I	*0.671*	*0.669 - 0.672*
Personality II	*0.781*	*0.779 - 0.782*

Table 6.9: PQ on a Bag Search

	Average PQ [%]	**95% Percent CI [%]**
Skill Level 0.8	*0.762*	*0.758 - 0.767*
Skill Level 0.9	*0.750*	*0.746 - 0.754*
Skill Level 1.0	*0.733*	*0.728 - 0.737*
Personality I	*0.683*	*0.683 - 0.684*
Personality II	*0.811*	*0.810 - 0.812*

Furthermore, agents which experience stress outperform agents without stress with 20%. This result may seem counter intuitive, but is caused by the fact that the agents are bored by their tasks and find it hard to motivate themselves to put in some effort. Stress apparently triggers the agents to put some extra effort in the task.

This result is in line with the results found earlier in the chapter. From Section 6.1.1 it becomes clear that agents without stress outperform agents with stress only in the region around the optimal task level. Section 6.2.1 shows that when the agents have been idle before, the agents with stress outperform the other agents over the whole range.

Finally, the PQ on scanning X-Ray images are relatively low, since the PQ of the agent is still rising when the task ends and thus the equilibrium value is not reached. The task is too short for the agent to reach maximum performance. Therefore an additional simulation of 5000 runs was done in which the agents had a continuous stream of bags. The results from this simulation are found in Table 6.8. Comparing the values in this table to the previously found values shows that PQ increases with 21.3% when the X-Ray officer is busy all the time.

Bag Searching

The Performance Quality of officers on searching a bag can be found in Table 6.9. Comparing this table to Table 6.7 shows that the PQ of officers on a bag search is 25% higher than the PQ values on scanning a X-Ray image. The reason for this is already discussed in the previous section.

Furthermore, the agents with the highest skill level get outperformed by the agents with the lowest skill level by 4.0%. This seems counter intuitive, but is in line with figure 6.7a. In this figure Performance Quality drops if the Task Level becomes too low. This is because the agent does not get motivated enough to generate effort. For lower skilled agents the tasks is more challenging and thus they are more motivated to put in some effort. This leads to the counter-intuitive result that the most skilled agents are not top performers on this tasks

Furthermore agents which experience stress again outperform agents without stress with 19%.

Pat Down

The performance of officers can be found in Table 6.10. Comparing this table to Table 6.9 shows that the PQ on Pat Downs is 6.6% lower than on searching a bag. The reason for this is that the task is easier, and thus the

Table 6.10: PQ on a Pat Down

	Average PQ [%]	95% Percent CI [%]
Skill Level 0.8	*0.748*	*0.744 - 0.751*
Skill Level 0.9	*0.734*	*0.731 - 0.737*
Skill Level 1.0	*0.665*	*0.662 - 0.668*
Personality I	*0.652*	*0.651 - 0.654*
Personality II	*0.774*	*0.772 - 0.776*

agents are less motivated.

For the same reason, the highest skilled agents are again outperformed by the lowest skilled agents by 12%. Furthermore, stress increases performance with 19%.

Conclusion

In this Subsection the Performance Quality of the agents was analyzed for each of the tasks at the checkpoint. During this analysis it was found that stress positively influences the agents PQ. Apparently stress helps to motivate the agents to generate some effort despite of the rather boring tasks. Furthermore an increase in Skill Level does not always lead to higher performance quality. Lesser skilled agents performed better on easy tasks like bag checking and a pat down. The reason for this is that highly skilled agents were not able to motivate themselves enough on easy tasks. Finally, the agents PQ was lowest on analyzing X-Ray images. The reason for this is that the agents barely had time to generate effort once they got the task, since the duration was only one second. If the agents behind the X-Ray would be kept busy all the time, PQ would increase with 21%.

6.3.3. Outcome of each decision as function of the agents Characteristics

In this Subsection the decision making of employees is investigated as function of the agents attention weights. The following decisions will be analyzed subsequently:

- Decision to request a Bag Search
- Decision to request a Rescan
- Decision to request a Secondary Screening

Bag Search Decision

When a potentially prohibited item is detected, bags are searched 93.7% of the time on average. This number varies based on the attention weights for each of his goals. The influence of the attention weight for each criteria is found in table 6.11

From the table it becomes apparent that the attention weight for speed is the most dominant parameter in this decision. Varying this parameter from low to high, leads to a 12% decrease in bag searches. The second most important parameter is the attention weight for accuracy. Increasing this parameter from low to high, causes a 11% increase in bag searches.

The attention weight for risk is less dominant. An increase from low attention to high, causes a 5.3% increase in bag searches. The reason that this parameter is less influential, is that most of the prohibited items have threat values of less than 1, which means that they are not perceived as a big security risk. Speed and Accuracy on the other hand always play a big role in the trade-off.

Rescan Decision

In this section the influence of attention weight on the rescan decision is analyzed. The correlations between attention weight and the agents decisions are found in Table 6.12

In this table, the attention weight for speed is again the most dominant parameter. Varying this parameter from low to high, causes a 54% decrease in rescans. If the attention weight for speed is high, only 45.1% of the bags are rescanned.

Table 6.11: Percentage of Bag Searches as function of Attention Weight

	Option 1		
	Average [%]	**95 Percent CI [%]**	**Runs [-]**
Accuracy Attention = Low	*88.4*	*86.9 - 90.0*	*1687*
Accuracy Attention = Med	*94.9*	*93.9 - 96.0*	*1767*
Accuracy Attention = High	*97.7*	*97.0 - 98.4*	*1808*
Speed Attention = Low	*98.8*	*98.4 - 99.4*	*1862*
Speed Attention = Med	*95.1*	*94.1 - 96.1*	*1688*
Speed Attention = High	*87.0*	*85.4 - 88.6*	*1712*
Risk Attention = Low	*91.1*	*89.8 - 92.5*	*1698*
Risk Attention = Med	*94.4*	*93.3 - 95.5*	*1804*
Risk Attention = High	*95.9*	*94.9 - 96.8*	*1760*

Table 6.12: Percentage of Rescans as function of Attention Weight

	Option 1		
	Average [%]	**95 Percent CI [%]**	**Runs [-]**
Accuracy Attention = Low	*61.5*	*49.7 - 73.4*	*65*
Accuracy Attention = Med	*76.2*	*65.6 - 86.7*	*63*
Accuracy Attention = High	*92.1*	*85.6 - 98.8*	*64*
Speed Attention = Low	*98.6*	*95.9 - 101*	*72*
Speed Attention = Med	*76.8*	*66.9 - 86.8*	*69*
Speed Attention = High	*45.1*	*31.4 - 58.8*	*51*
Risk Attention = Low	*76.7*	*66.0 - 87.4*	*60*
Risk Attention = Med	*72.9*	*61.5 - 84.2*	*59*
Risk Attention = High	*79.4*	*70.2 - 88.7*	*73*

The second most important parameter is the attention weight for accuracy. Increasing this parameter from low to high, leads to a 50% increase in rescans. If accuracy is important to the officer, 92.1% of the bags are rescanned.

The results for the attention weight for risk are not statistically significant. During the 15.000 runs, only 192 rescan decisions had to be taken. Since the attention weight for risk is not that influential, this number was not large enough to produce significant differences in the results between different attention weights.

Finally it must be noted that the influences of attention weight on rescan decisions is much larger than on search decisions. The reason is that this is a fully autonomous decision, while the bag search decision mainly relies on initial preference.

Secondary Screening

In this section the influence of attention weight on the secondary screening is discussed. It must be noted that in some cases the decision is completely based on initial preference. This is the case when either a gun or a bulk explosive is confiscated. These cases are filtered out of the results.

In the remaining cases the number of secondary screenings is marginal. In 3601 secondary screening decisions, only 5 passengers required additional screening. This was not enough to produce significant results.

Conclusion

In this Subsection it is found that the attention weight for speed is the most dominant parameter. This parameter was closely followed by the attention weight for accuracy. The attention weight for perceived risk is less important. This is because most of the prohibited items used in this simulation are not perceived as a big threat and thus the valences for perceived risk are lower than the valences for speed and accuracy.

6.3.4. Outcome of each screening process as function of the agents characteristics

With the effect of employee characteristics on each activity and decision analyzed, the next question is how these characteristics effect the outcome of the entire screening process. To answer this question the outcome of each screening process is analyzed in relation to each of the employee characteristics. This is subsequently done for the x-ray operator, bag searcher and WTMD officer.

It must be noted that not all characteristics will show a statistically significant contribution to the outcome. This is because of the limited number of iterations and may change if this number is increased. Nevertheless, this number of iterations is enough to identify the employee characteristics which have the largest impact on the outcome of each screening process.

Characteristics of the X-Ray Officer

Figure 6.11 shows the relation between the characteristics of the X-Ray officer and the outcome of the baggage screening process. From this figure the characteristics with a (statistically) significant impact on the outcome can readily be identified.

For both configurations the significant factors are the goal importance for accuracy, speed, perceived risk and the agents personality. With the current number of iterations the skill level of the operators shows no significant contribution to the outcome of the process.

The factors with the biggest influence are importance for accuracy and speed. An increase in importance for accuracy from low to high means an increase in weapons confiscated of 12.9% at the Regional Airport and 16.2% at the International airport. The same increase from low to high in importance of accuracy means a decrease in weapons confiscated of 14.5% at the Regional Airport and 11.0% at the International Airport. The effects of goal importance for perceived risk and personality type on the outcome of the screening process are less prominent. Varying the goal importance of perceived risk from low to high results in an increase in weapons confiscated of 6.4% at the Regional Airport and the results at the International Airport are statistically insignificant. Furthermore, the difference between personality type is an increase of 5.0% in weapons confiscated at the Regional Airport and 6.6% at the International Airport. In both cases, agents with PT II outperform agents with PT I.

From this analysis it is clear that the main contribution of the x-ray operator to the outcome of the baggage screening process is his trade-off between speed and accuracy. This is an interesting result, since the only decision this operator has to make is the decision to alert the bag checker. In the model the x-ray operators have a large initial preference for alerting the officer searching bags if a prohibited item gets detected, but despite this initial preference the speed/accuracy trade-off still has a large impact on the outcome of the operators decision.

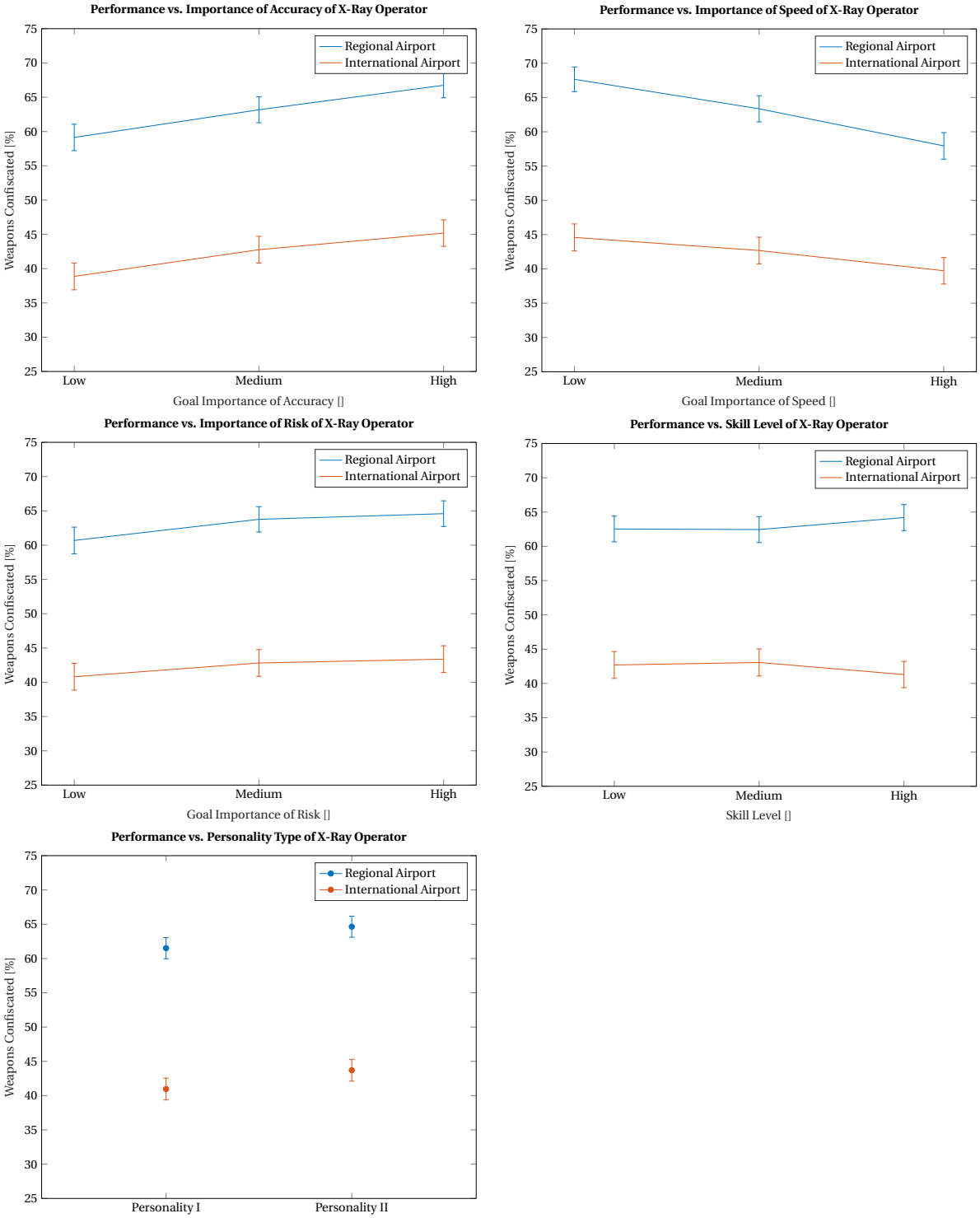


Figure 6.11: The effect of the characteristics of the X-Ray Officer on the outcome of the baggage screening process

Characteristics of the Bag Searching Officer

The relation between the outcome of the baggage screening process and the characteristics of the Bag Searching Officer are found in Figure 6.12. From this figure it can be found that in the Regional configuration there are no statically significant relations between the agents characteristics and the outcome of the screening process.

In the checkpoint configuration of the International Airport the factors with a clear influence on the outcome of the screening process are the goal importance of accuracy, speed and the personality type of the operator. An increase in the goal importance for speed from low to high results in an increase of 14% in items confiscated. The same increase in importance of speed results in a decrease of 15.2%. Finally PT II outperforms PT I again by 13.9%.

The reason the the characteristics of the officer checking bags only show a significant influence on the outcome of the screening process at the International Airport not at the Regional Airport can be explained from the difference in task distribution at the two checkpoints. At the International Airport the officer searching bags has to analyze the X-Ray image himself and also performs the rescans himself. This increase in activities and decisions for which the operator is responsible are the reason that his behaviour has a relatively large impact on the outcome of the screening process compared to the Regional checkpoint configuration.

Characteristics of the WTMD / Body Scanner Officer

The relation between the characteristics of the officer responsible for the WTMD or Body Scanner and the outcome of the process of screening passengers is shown in Figure 6.13. From this figure it is clear that in both configurations there are no significant correlations between the characteristics of the officer and the outcome of the screening process.

The main reason for this is that the screening process for passengers contains less activities and decision points compared to the process of screening bags. This makes the influence of employee behaviour on this process much smaller.

6.3.5. Quantifying Vulnerabilities in the Checkpoints

In this section the vulnerabilities in both checkpoint configurations are analyzed and the role of employee behaviour in each of these vulnerabilities is investigated. First the vulnerabilities are analyzed for both the Regional and International Airport. After that a comparison is made between the two configurations. Finally, the role of employee behaviour in these vulnerabilities is discussed.

Vulnerabilities at the Regional Airport

In this section the performance of the checkpoint at the Regional Airport is analyzed. The results from the simulation runs are found in Table 6.13.

From this Table it becomes clear that some weapons are never confiscated. The reason for this is that these weapons cannot be detected by the equipment used to scan the passengers. None of the explosives smuggled on your body get detected by the WTMD machine and the same is the case for ceramic knives. Explosives still get detected by a random ETD test though, leading to a secondary screening in 10.1% of the cases.

Furthermore knives can be taken through the checkpoint without much consequences. The worst case scenario is that the knife gets confiscated and the attacker has to try it again. The chances on a secondary screening are 0.0%, which means the attacker can keep trying until he finally succeeds in smuggling a knife through the checkpoint.

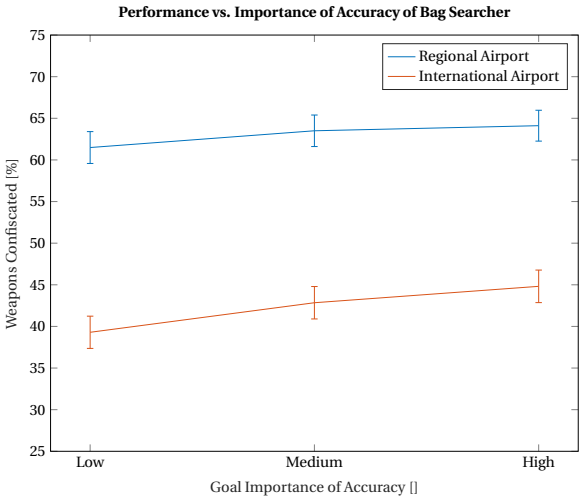
The checkpoint performs best on detecting guns both in the X-Ray and the WTMD. These weapons get confiscated 84.8% of the time when the attacker puts it in his baggage and immediately leads to a secondary screening. This number gets up to 90.7% when the attacker carries the weapon on his body.

International Airport

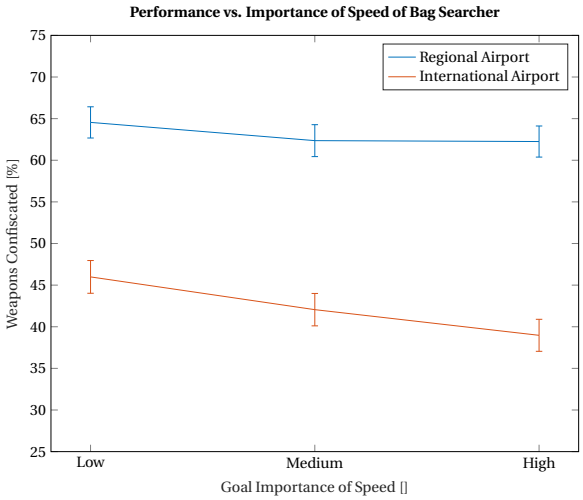
In this section the performance of the checkpoint model of the International Airport is analyzed. The results from the simulation runs are found in Table 6.14.

At the International Airport only one type of threat remains undetected. Smuggling explosive powder through a body scanner has a success rate of 88.6%. The only measure against it is a random ETD check.

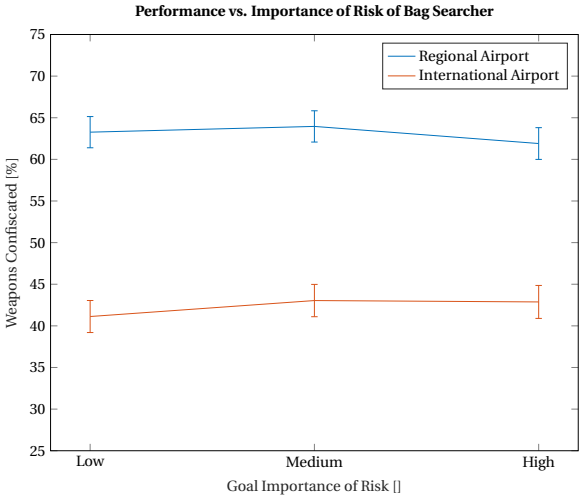
Furthermore liquid explosives and powders hidden in a bag are confiscated only 32-34% of the time. Even when these items are confiscated the security operator does not necessarily recognize these items as bomb parts and thus the attacker is free to walk away and try again until he succeeds or gets caught by a random



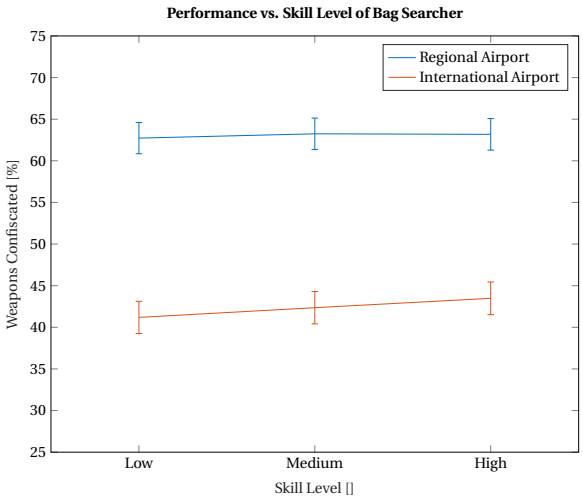
(a) Scenario 1: with Risk



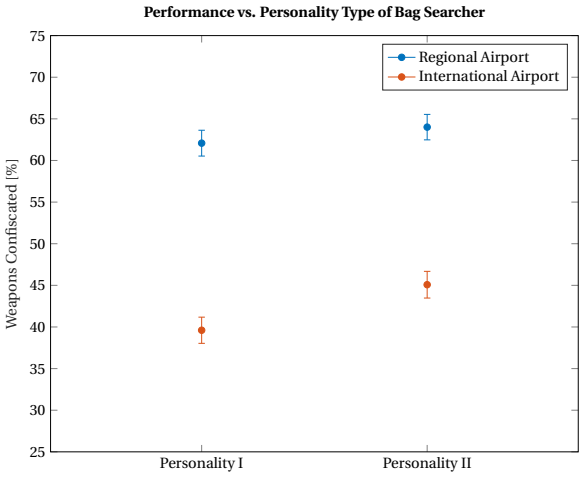
(b) Scenario 1: with Risk



(c) Scenario 1: with Risk

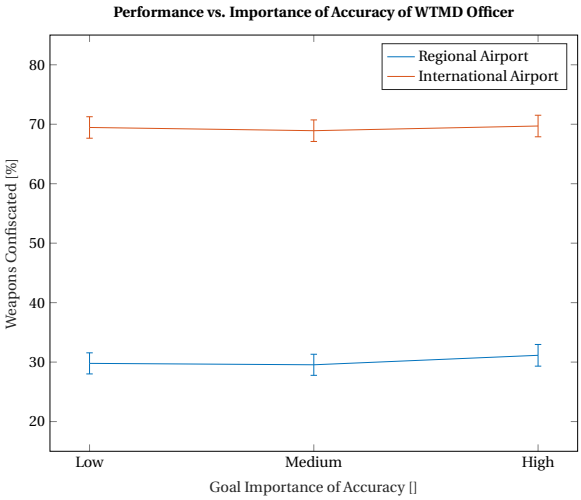


(d) Scenario 1: with Risk

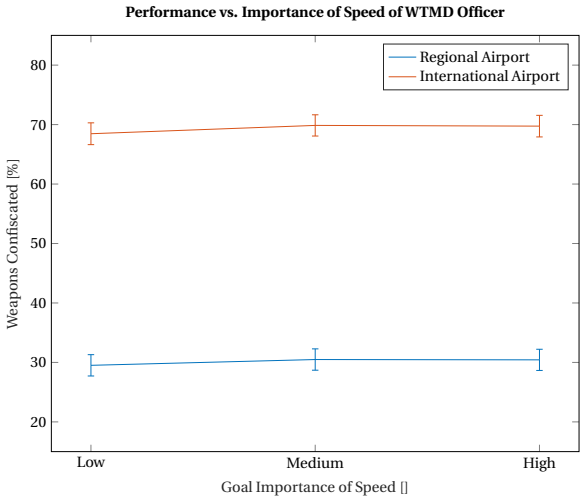


(e) Scenario 1: with Risk

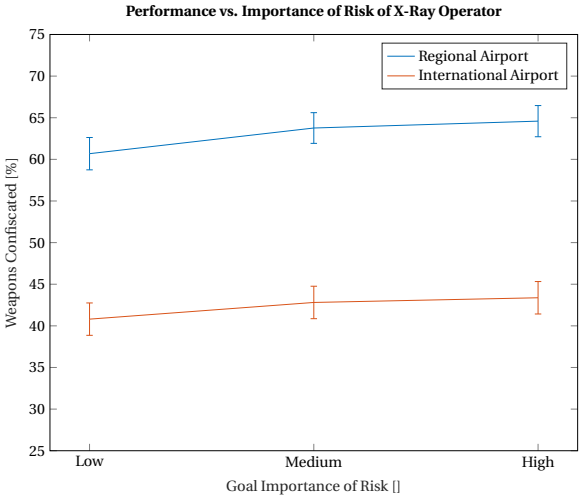
Figure 6.12: The effect of the characteristics of the Bag Searching Officer on the outcome of the baggage screening process



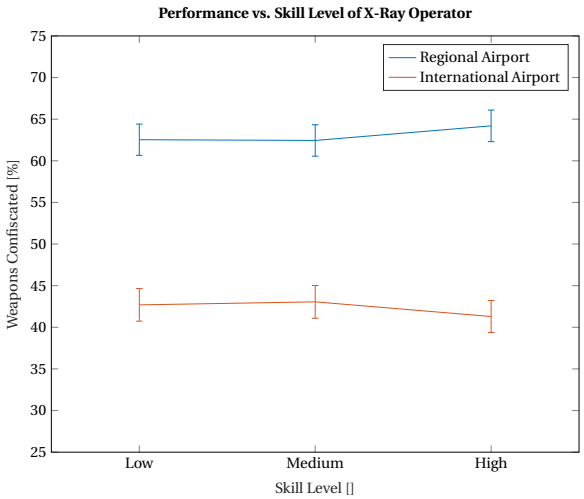
(a) Scenario 1: with Risk



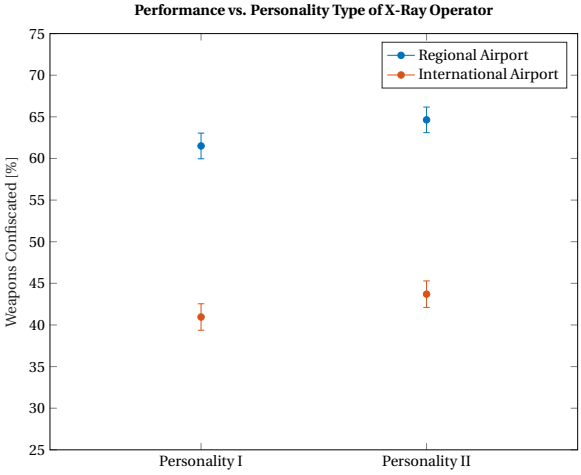
(b) Scenario 1: with Risk



(c) Scenario 1: with Risk



(d) Scenario 1: with Risk



(e) Scenario 1: with Risk

Figure 6.13: The effect of the characteristics of the WTMD/ Body Scanner Officer on the outcome of passenger screening

Table 6.13: Checkpoint Performance of the Regional Airport on different types of threats

			Confiscated		Secondary Screening	
Weapon	**Location**	**Sample size**	**Average [%]**	**95 Confidence [%]**	**Average [%]**	**95 Confidence [%]**
Explosive Bulk	Baggage	*625*	*68.6*	*65.0-72.3*	*72.3*	*68.8 - 75.8*
Explosive Bulk	Body	*636*	*0.0*	*0.0 - 0.0*	*9.11*	*6.88 - 11.4*
Explosive Liquid	Baggage	*645*	*53.8*	*50.0 - 57.6*	*9.14*	*6.92 - 11.5*
Explosive Liquid	Body	*654*	*0.0*	*0.0 - 0.0*	*9.78*	*7.51 - 12.1*
Explosive Powder	Baggage	*629*	*53.4*	*49.5 - 57.3*	*9.22*	*6.95 - 11.4*
Explosive Powder	Body	*580*	*0.0*	*0.0 - 0.0*	*11.4*	*8.79 - 14.0*
Gun	Baggage	*650*	*84.8*	*82.0 - 87.5*	*84.8*	*82.0 - 87.5*
Gun	Body	*656*	*90.7*	*88.5 - 92.9*	*90.7*	*88.5 - 92.9*
Knife	Baggage	*620*	*57.1*	*53.2 - 60.9*	*0.00*	*0.00 - .477*
Knife	Body	*616*	*91.7*	*89.5 - 93.9*	*0.00*	*0.00 - .480*
Ceramic Knife	Baggage	*635*	*57.4*	*53.6 - 61.3*	*0.00*	*0.00 - .466*
Ceramic Knife	Body	*652*	*0.0*	*0.00 - 0.00*	*0.00*	*0.00 - 0.00*

Table 6.14: Checkpoint Performance of the International Airport on different types of threats

			Confiscated		Secondary Screening	
Weapon	**Location**	**Sample size**	**Average [%]**	**95 Confidence [%]**	**Average [%]**	**95 Confidence [%]**
Explosive Bulk	Baggage	*607*	*49.4*	*45.4 - 53.4*	*53.9*	*49.9 - 57.8*
Explosive Bulk	Body	*614*	*55.4*	*51.4 - 59.3*	*61.1*	*57.2 - 64.9*
Explosive Liquid	Baggage	*637*	*31.7*	*28.1 - 35.3*	*9.73*	*7.43 - 12.0*
Explosive Liquid	Body	*592*	*89.9*	*87.4 - 92.3*	*8.78*	*6.50 - 11.1*
Explosive Powder	Baggage	*605*	*33.9*	*30.1 - 37.7*	*10.4*	*7.98 - 12.8*
Explosive Powder	Body	*653*	*0.00*	*0.00 - 0.00*	*12.4*	*9.89 - 14.9*
Gun	Baggage	*606*	*70.0*	*66.3 - 73.6*	*70.0*	*66.3 - 73.6*
Gun	Body	*582*	*90.7*	*88.3 - 93.1*	*90.7*	*88.3 - 93.1*
Knife	Baggage	*604*	*35.4*	*31.6 - 39.2*	*0.00*	*0.00 - 0.00*
Knife	Body	*600*	*94.2*	*92.3 - 96.0*	*0.00*	*0.00 - .795*
Ceramic Knife	Baggage	*674*	*36.4*	*32.7 - 40.0*	*0.00*	*0.00 - 0.00*
Ceramic Knife	Body	*628*	*93.0*	*91.0 - 95.0*	*0.00*	*0.00 - .471*

ETD check. Bulk Explosives on the other hand are detected in 50% of the cases and are also recognized as a bomb leading to immediate secondary screening.

An attacker bringing a gun is still very unsuccessful. The best method would be to hide it in the baggage, but this only has a success rate of 30%. When the weapon gets detected it also gets immediately confiscated. Knives can best be brought hidden in the baggage as well. In that case they are only confiscated 36% of the time, but the attacker is free to try it again, since the chances of additional screening is minimal

Comparing configurations

There are two differences between the configurations at the Regional and International Airport. The first is the equipment to scan passengers. The Regional Airport uses a WTMD whereas the International Airport uses a Body Scanner. This choice of equipment impacts the detection rates of weapons hidden on the attackers body. The second difference is the communication between the officer operating the X-Ray and the officer searching the Bag. At the Regional Airport there is the possibility to communicate directly, but at the International Airport this is not possible. In this section the effect of those differences on the overall performance are discussed.

When comparing the detection rates for weapons hidden on the attackers body, the International Airport outperforms the configuration of the Regional Airport by 127%. In the configuration of the Regional Airport 30.6% of the weapons hidden on the attackers body get detected, while the International Airport detects 69.5% of those weapons. The main reason for this difference, is the inability of a WTMD to detect 4 out of 6 of the weapons used in this simulation. The Body Scanner on the other hand flawlessly detected 4 out of 6 types of weapons and detects one weapon type with 56% certainty. Only explosive powders do not get picked up by this machine. So while body scanners seem to perform better, it must be noted that they still can be beaten by an attacker which is intelligent enough to bring the right kind of weapon.

Comparing the performance on checking bags, the configuration of the Regional Airport outperforms the International Airport. In this configuration 62.6% of the weapons in the baggage are confiscated, whereas in the configuration of the International Airport this is only 42.6%. The main reason for this is the lack of communication in the configuration of the International Airport. The officer behind the X-Ray flags a bag for a search, but the officer performing the search has to identify the threat on the X-Ray image himself. This extra step in the process apparently causes a loss in performance of 32% and is caused solely by the fact that two officers independently have to recognize a threat on an X-Ray image instead of just one.

The role of security operators in the emergence of Vulnerabilities

This work has discussed the influence of security operators on the outcome of each screening process and quantified vulnerabilities for a limited number of threat scenarios. The aim of this section is to discuss how each vulnerability is influenced by employee behaviour.

By analyzing the vulnerabilities in the two checkpoint configurations it has become clear that some weapons can only be detected by an ETD test or cannot be detected at all. This inability to detect some of the weapons used in this study is due to the equipment used at the checkpoint and not caused by the security operators.

Next to that some weapons are detected and confiscated, but no additional screening is required by the security operators. In this case the operator confiscates the item because it is prohibited, but does not perceive it as such a threat that secondary screening is required. This can be a problem, because it allows the attacker to try again until he succeeds. The main vulnerability in this category are liquid explosives. While liquids are forbidden, the operators encounter so many liquids that they will just confiscate the bottle without seeing it as a real threat.

Finally, the vulnerability for some threat scenarios is high due to employee performance and decision making. This is especially the case for prohibited items hidden in the baggage of a passenger. The main reason for the poor detection rates during the screening of baggage is the complexity of the process. It is the only process in this model which consists of multiple activities and decision points, which makes the process heavily dependent on employee performance and decision making. At the International Airport the vulnerabilities related to the baggage screening process are even higher, since they introduced additional steps into the screening process, which introduces more opportunities for the security operators to end the search before the item is confiscated.

6.3.6. Conclusion

In this section the performance of a checkpoint was analyzed by performing 15.000 independent runs. In this section the conclusions from this analysis are summarized.

The first relation which is investigated is the performance quality as a function of the agents characteristics. It appeared that agents with stress outperform other agents by 20%. This seems surprising, but is explained by the fact that stress motivates the agents to put in more effort. Furthermore, an increase in skill level does not always mean an increase in performance. It is found that searching a bag or performing a pat down is such an easy task, that the highest skilled agents could not motivate themselves to put in enough effort and got outperformed by their lesser skilled counterparts.

The second thing which is investigated is the relation between decisions and the agents characteristics. It is found that the most dominant factor is the attention weight for speed. This factor was closely followed by the attention weight for accuracy. The attention weight for perceived risk is less important. This is because most of the prohibited items used in this simulation are not perceived as a big threat and thus the valences for perceived risk are lower than the valences for speed and accuracy.

By analyzing the relation between employee characteristics and the outcome of each screening process it is found that the screening of baggage is the process that is most effected by employee behaviour. Based on this number of runs, this is the only process in which there are statistically significant relations between employee characteristics and the outcome of the process. The largest contribution of employee characteristics is the trade-off between speed and accuracy. Another factor is the personality, in which agents with stress outperform the other agents.

Finally, the checkpoint performance is analyzed as a whole. During this analysis two main weaknesses are identified. The first weakness is the checkpoints inability to detect some prohibited items. Especially the WTMD is vulnerable since it is unable to identify 4 out of 6 of the prohibited items used in this simulation. Also the Body Scanner is unable to detect 1 of the items. This only leaves the ETD test to detect the prohibited items in case of explosives.

The second weakness is the lack of follow-up actions once a prohibited item gets detected. The item gets confiscated, but secondary screening is very rare if the item is not recognized as an explosive or gun. This leaves the possibility to the attacker to try again.

Apart from the weaknesses, the checkpoint configuration has large consequences on the number of weapons confiscated. First the choice of equipment plays an important role. A WTMD only detects 33% of the prohibited items, where a Body Scanner detects 76%. Also the task distribution and communication between agents impacts the performance of the checkpoint as a whole. In the International configuration there was no communication between the officer monitoring the x-ray and the officer searching the bag. This resulted in a 32% decrease in detected items.

Next to that, the performance of the X-Ray officer can be improved by providing a continuous stream of bags. This increases performance by 21%. The reason for this is that the X-Ray officer is currently idle most of the time and does not reach its potential PQ in the one second he needs to evaluate the X-Ray image.

7 Conclusion

In this work the relation between employee behaviour and the emergence of vulnerabilities is investigated. This chapter discusses the main findings from this work and its contribution to science and industry. First Section 7.1 presents the main findings in light of the research questions. After that Section 7.2 discusses the contribution of this work.

7.1. Main Results of this Work

The research question central in this work is shown below.

> *Can the role of employee characteristics in the emergence of vulnerabilities at an airport checkpoint be identified and quantified using Agent-Based Modeling?*

To answer this question, four sub-questions were formulated. These will be discussed subsequently.

How can the security operators be modeled using an agent based approach?

To simulate employee behaviour use is made of two behavioural models to model employee decision making and performance. Both of these models are rooted in behavioural science as have empirical support.

Decision making of the security operators is modeled using decision field theory. In this model the operators make a trade-off based on certain goals he wants to achieve. From literature many factors that influence the decision making process have been identified, but in this model it is brought back to three goals: maximize speed, maximize accuracy and minimize the perceived risk. The importance of each of those goals is dependent on the operator.

The performance of the agent is modeled using the functional state model which relates performance to the task level of the activity which is performed. This model is calibrated for the performance of operators on analyzing x-ray images. Unfortunately there was no information available on the performance of operators on bag searches and pat downs, so assumptions about the performance of the operators on these tasks had to be made.

How is the outcome of employee activities and decisions influenced by their characteristics?

In the agent based model, the security operators have the following characteristics:

- Skill Level (SL)
  - This characteristic represents the skill level of the security operator. It is assumed the SL is the same for every task. The magnitude of this value is either set to 0.8, 0.9 or 1.0 and influences the performance effort and performance quality of the operator.
- Personality Type (PT)
  - The performance of the security operators is modeled using the functional state model. The authors of this model have added two example personality types which are used in this project. The main difference between those personality types is that PT II experiences more stress than PT I.

- Goal Importance (GI)
  - Each security operator has the same three goals: to do its work as *fast* and *accurate* as possible while *minimizing risk*. These three goals serve as decision criteria in each decision the operator makes, but the importance of each criteria depends on the operator and can take the value of 0.33, 0.5 or 0.67. These values are then normalized, such that the sum for all the three criteria is 1.

To answer the research question, the effect of each characteristic on the performance is investigated. First the effect of SL and PT on the agents performance quality (PQ) is investigated and after that the effect of GI on the agents choices is analyzed.

The biggest factor influencing the PQ of the security operator is the PT of the operator. PT II outperformed PT I on any task with 20%. Apparently stress helps to motivate the agents to generate some effort despite of the rather boring tasks.

The SL of the security operator also impacts PQ, but an increase in SL does not necessarily mean an increase in PQ. The highest skilled operators outperformed their lowest skilled counterparts with 5.2% on analyzing X-Ray images, but performed worse on both searching baggage and performing pat downs. Their PQ is 4.0% lower when searching a bag and 6.6% lower when performing a pat down. The main reason for this is that the security operators with the highest SL, find the tasks too easy and are unable to motivate themselves to put in the required effort.

During the experiments it was observed is that the PQ of security operators on analyzing X-Ray images was 20% lower than on the other two tasks. This is due to the nature of the task and not the agents characteristics. Scanning an X-Ray image takes approximately one second and this duration does not give the operator enough time to generate enough effort. If the security operator is provided with a constant stream of bags, PQ increases with 21.3%.

The biggest factor in the agents decision making is the GI for speed. Varying this factor from low to high decreases the number of bag searches by 12% and the number of rescans by 54%. The second most important factor is the GI for accuracy. increasing this parameter from low to high results in a 11% increase in bag searches and a 50% increase in rescans. The factor which is by far the least relevant is Risk. Varying the GI for risk from low to high gives 5.3% increase in bag searches. The influence of the GI for risk on the number of rescans cannot be established with 95% confidence. The reason for the relatively small influence of this factor on the decision making process is that the security operators do perceive most of the prohibited items as having a limited risk. Finally, the effect of the GI of each decision criteria on the decision to send someone to secondary screening could not be established with 95% confidence. The reason for this is that while this decision was made 3601 times, only 5 passengers received additional screening.

How is the outcome of each screening process influenced by the characteristics of the employees?
At an airport checkpoint three different screening procedures are performed:

- Screening Baggage
- Screening Passengers
- Scanning for Explosives

In this model it is assumed that the agent performing the explosive trace detection does not have an influence on the outcome of the test. Therefore the result from this test is completely dependent on the equipment and the presence of explosive traces. This assumption leaves two processes in which employee behaviour may effect the outcome of the screening procedure.

In the baggage screening process it is found that the outcome of the screening is mainly influenced by the goal importance of speed and accuracy for the x-ray officer. Other factors which contributed to the outcome of the screening process are personality type and goal importance of risk. No statistically significant relation was found between skill level and the outcome of the screening process.

The role of the baggage searching officer on the outcome of the screening process depends on the configuration. At the Regional Airport this officer has less responsibilities compared to the International Airport and no statistically significant relations are found between the characteristics of this agent and the outcome of the process. However, at the International Airport the impact of the officer is even larger than the impact of the X-Ray Operator. The biggest factor influencing the outcome is again the trade-off between speed and accuracy. Also the personality of the X-Ray Operator plays a significant role on the outcome of the process.

The impact of the operator on the screening process of passengers is much smaller compared to the baggage screening process. No significant relations could be found between the outcome of this screening process and the characteristics of the officer operating the WTMD or Body Scanner.

From the analysis of the different processes it is found that the biggest contribution of employees to the emergence of vulnerabilities comes from their trade-off between speed and accuracy. Changing the goal importance of speed and accuracy results in a 15% change in weapons confiscated. The goal importance of perceived risk is less influential, since most prohibited items are not seen as a threat. The second most important factor which influences vulnerability is the personality of the operator. Interestingly enough the skill level of the operator shows no significant relation to the outcome of the screening process. The reason behind this is that the performance of the agents is not limited by their cognitive abilities, but by the effort they generate and this is mainly dependent on the personality type.

What is the vulnerability for each threat scenario and what is the role of the employees in each of these scenarios?

To identify the weaknesses in the checkpoint the passengers in the simulation are given weapons which they can hide either on their body or in their baggage. In total six types of weapons are defined which can be hidden either on the passenger or in the baggage. Combining these six weapons with two means of transportation and two checkpoints, results in 24 possible scenarios.

Analyzing the results from those threat scenarios shows that some weapons cannot be detected. This inability to detect weapons is not caused by the behaviour of security operators, but results from the limitations of the equipment used. Especially the usage of a walk through metal detector makes the airport vulnerable since it is unable to detect 4 out 6 items used in this simulation. This leaves only a randomly performed ETD test to detect explosives which are smuggled on someones body. With only 10% of the passengers subjected to this test, the an airport which uses WTMDs is extremely vulnerable for this type of attacks. A body scanner on the other hand performs better, but is still unable to detect explosive powders. To minimize the vulnerability against these threat scenarios, two improvements can be made. First of all, this threat can be partially mitigated by using state of the art equipment. For example: the WTMD detected only 33% of the weapons, where the body scanner detected 76% of the weapons. The second countermeasure could be increasing the percentage of passengers that are screened for explosive traces.

In a second group of threat scenarios the weapons are identified as prohibited items and confiscated, but the operator does not see these items as a threat. Especially when the passenger carries something common like a liquid or a (legal) knife it is highly unlikely the passenger will receive additional screening. The bottle with liquid or knife will be thrown away and the passenger is free to go. This is understandable due to the high frequency of these items being confiscated, but it leaves a potential terrorist the possibility to try again. Given the relatively low detection probabilities, it is likely the attacker will get its weapon through in a few tries. The main problem in these threat scenarios is the lack of follow-up action once a prohibited item is detected, which is a direct consequence of the beliefs of the security operator about the item.

Employees have the largest influence on vulnerabilities that involve weapons in the carry-on baggage. This is because the screening process for carry-on baggage is the process that is most dependent on employee performance and decision making. Another big factor influencing the vulnerabilities related to weapons in carry-on luggage is the organization of processes on the checkpoint. In this work two configurations are tested and in one of those configurations there was no communication between the security operator assigned to the X-Ray machine and the one searching bags. This lack of communication causes the X-Ray image to be analyzed twice which leads to a loss in performance of 32%.

Answering the main research question

In this work the role of employee characteristics in the emergence of vulnerabilities of the checkpoint have been analyzed by using an agent-based model of an airport checkpoint. It is found that employees mainly influence the vulnerabilities related to weapons hidden in the carry-on luggage. The resulting vulnerabilities for these weapons depend on the speed/accuracy trade-off the security operator makes and his personality. The other processes are less effected by employee behaviour. The main reason for this is that employees play a less important role in these processes.

Furthermore, the airport checkpoint seems vulnerable against weapons which are not recognized as threat. These weapons may be recognized as prohibited items, but as long as the employees do not really see these items as a serious threat no further action may be taken and the attacker is free to try again.

7.2. Contributions to Science and Industry

This work is part of a larger project in which the trade-off between efficiency and security within an airport terminal is investigated by using agent-based modeling. At the beginning of this thesis a preliminary version of this agent-based model was available which is developed by the PhD candidate Stef Janssen. His work provided an excellent starting point for this thesis.

The main contribution of this project to the agent-based model is the implementation of checkpoint procedures and developing the architecture of the security operators. These contributions make it possible to assess vulnerabilities emerging from the airport checkpoint, which is crucial step in each risk assessment method.

The results of this work show how vulnerabilities are effected by employee behaviour and these insights can aid policy makers in the development of new policies and in the assessing the effectiveness of current screening procedures. Furthermore this work provides some insight in how the configuration of a checkpoint and the choice of equipment effects the vulnerabilities emerging from it. This aids the managers which are responsible for implementing the regulations in understanding how the choices they make effect the vulnerabilities in their airport checkpoint.

8

Recommendations

In this report a new technique was developed to systematically identify vulnerabilities at an airport checkpoint. This has never been tried before and this work leaves some possibilities for further research. In this chapter an overview is given of the main recommendations to improve and extend this model.

Give attackers the possibility to wipe explosive traces
In the model as developed in Chapter 5, it was assumed that if a bag or a passenger has a bomb, it is always contaminated with explosive traces. Terrorists have shown in the past that they are capable of erasing explosive traces and thus this assumption does not hold. Therefore the passenger smuggling a weapon through airport security should be able to wipe explosive traces. Based on this model, some weapons will then be completely undetectable for airport security.

Give attackers the possibility to bring multiple prohibited items
In the agent-based model it is assumed that attackers will bring only one prohibited item. At first this assumption seems intuitive, since the attacker wants to minimize the risk of getting caught. However, it leaves out the possibility to use a prohibited item as a decoy for a weapon. Penetration testers have successfully tried this strategy and were able to smuggle a bomb through an x-ray machine by using a water bottle as a decoy. The operator searching the baggage, removed the bottle and then considered the bag cleared [45].

To implement this, it must be better understood how the attention of a security operator is drawn to particular objects on the X-Ray image and what the operator does when he detects a prohibited item: does he continue looking for other items or does he immediately alert the security operator responsible for searching the bag.

Give the security operators the possibility to profile passengers based on their characteristics.
In the current model, the risk as perceived by the operator is solely based on the prohibited item they detected. The whole model is based on screening passengers and not people. In reality the beliefs of the security operator about the passenger also contribute to his decisions.

The easiest to model are beliefs about passengers which are shared by the organization. For example, the TSA has trained behavioural officers which screen passengers behaviour. The idea behind it is to identify potential terrorists based on their behaviour [15]. Another country which successfully employs this method is Israel [46]. In this country the screening process is completely focused on passengers and not their baggage. Their screening is not only focused on behavioural tells, but also on passenger characteristics like age, gender and ethnicity. The effects of these type of characteristics on the agents decision making would be easiest to include in the model. After that shared beliefs about passenger behaviour can be incorporated.

Extend the model by modeling other layers of security
The security checkpoint is considered the most important layer of defense in airport security, but there are many other layers. While the effectiveness of most of this layers is questionable, there are a few which may contribute to the mitigation of vulnerabilities and should be included in the model.

The first layer to be mentioned are the behavioural detection officers as employed in the United States. This layer is focused on screening passengers and not baggage and may be able to identify potential terrorist

based on their behaviour. Including this in the model would probably increase the performance of airport security and mitigate or minimize some vulnerabilities.

Other layers to be considered are the no-fly list, customs and border protection and the travel document checker. All these layers must allow a passenger to fly and may aid in deterring a potential terrorist from entering an aircraft.

Extend the model with a data analysis method to systematically identify vulnerabilities from the model
As the model becomes more complicated, the data will increase in size and it becomes easy to miss significant results. To prevent this and make sure all relevant vulnerabilities and underlying factors are identified from the simulation it is important to analyze the output of the simulation in a structured way. The best way to do this is to identify and implement a method which is capable of identifying trends in large sets of data. This was beyond the scope of this project, but is absolutely required if this model gets extended and becomes more complex.

Bibliography

[1] *AATOM - An Agent-based Airport Terminal Operations Model.*

[2] Neuron firing rates in humans, April 2015. URL https://aiimpacts.org/rate-of-neuron-firing/. [Online; posted 14-April-2015].

[3] Airport data contact information, January 2018. URL https://www.faa.gov/airports/airport_safety/airportdata_5010/. [Online; posted 4-January-2015].

[4] Torbjörn Åkerstedt, Peeter Fredlund, Mats Gillberg, and Bjarne Jansson. Work load and work hours in relation to disturbed sleep and fatigue in a large representative sample. *Journal of psychosomatic research*, 53(1):585–588, 2002.

[5] Bo An, James Pita, Eric Shieh, Milind Tambe, Chris Kiekintveld, and Janusz Marecki. Guards and protect: Next generation applications of security games. *ACM SIGecom Exchanges*, 10(1):31–34, 2011.

[6] Andreas Angenendt. Safety and security from the air traffic control services' point of view. 2003.

[7] Norman Ashford, Pierre Coutu, and John Beasley. *Airport operations*. 2013.

[8] Ludwig Benner. Accident investigations: Multilinear events sequencing methods. *Journal of safety research*, 7(2):67–73, 1975.

[9] Brian Bennett. Red team agents use disguises, ingenuity to expose tsa vulnerabilities, June 2015. URL http://www.latimes.com/nation/nationnow/la-na-tsa-screeners-20150602-story.html. [Online; posted 2-June-2015].

[10] Vicki M Bier and M Naceur Azaiez. *Game theoretic risk analysis of security threats*, volume 128. Springer Science & Business Media, 2008.

[11] Bruce M Blumberg and Tinsley A Galyean. Multi-level direction of autonomous creatures for real-time virtual environments. In *Proceedings of the 22nd annual conference on Computer graphics and interactive techniques*, pages 47–54. ACM, 1995.

[12] Anton Bolfing and Adrian Schwaninger. Selection and pre-employment assessment in aviation security x-ray screening. In *Security Technology, 2009. 43rd Annual 2009 International Carnahan Conference on*, pages 5–12. IEEE, 2009.

[13] Tibor Bosse, Fiemke Both, Rianne Van Lambalgen, and Jan Treur. An agent model for a human's functional state and performance. In *Proceedings of the 2008 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology-Volume 02*, pages 302–307. IEEE Computer Society, 2008.

[14] Tibor Bosse, Fiemke Both, Mark Hoogendoorn, S Waqar Jaffry, RIANNE VAN LAMBALGEN, Rogier Oorburg, Alexei Sharpanskykh, Jan Treur, and Michael De Vos. Design and validation of a model for a human's functional state and performance. *International Journal of Modeling, Simulation, and Scientific Computing*, 2(04):413–443, 2011.

[15] Bob Burns. 'tsa spot program: Still going strong, May 2010. URL https://www.tsa.gov/blog/2010/05/21/tsa-spot-program-still-going-strong. [Online; posted 21-May-2010].

[16] John F. Burns. Yemen bomb could have gone off at east coast, November 2010. URL http://www.nytimes.com/2010/11/11/world/europe/11parcel.html. [Online; posted 10-November-2010].

[17] Jerome R Busemeyer and James T Townsend. Decision field theory: a dynamic-cognitive approach to decision making in an uncertain environment. *Psychological review*, 100(3):432, 1993.

[18] CNN. Shoe bomb suspect to remain in custody, December 2001. URL http://edition.cnn.com/2001/US/12/24/investigation.plane/. [Online; posted 25-December-2001].

[19] Mara Cole and Andreas Kuhlmann. A scenario-based approach to airport security. *Futures*, 44(4):319–327, 2012.

[20] European Commission. Aviation security: Commission adopts new rules on the use of security scanners at european airports, November 2011. URL http://europa.eu/rapid/press-release_IP-11-1343_en.htm?locale=en. [Online; posted 14-November-2011].

[21] European Commission. Liquids, aerosols and gels, August 2017. URL https://ec.europa.eu/transport/modes/air/security/aviation-security-policy/lags_en.

[22] Roger M. Cooke and Louis L.H.J. Goossens. Tu delft expert judgment data base. *Reliability Engineering and System Safety*, 93:657–674, 2008.

[23] Alan Cowell and Dexter Filkins. Airlines terror plot disrupted, August 2006. URL http://www.nytimes.com/2006/08/10/world/europe/11terrorcnd.html. [Online; posted 10-August-2006].

[24] Mary Dejevsky. Are planned airport scanners just a scam?, January 2010. URL http://www.independent.co.uk/news/uk/home-news/are-planned-airport-scanners-just-a-scam-1856175.html. [Online; posted 3-January-2010].

[25] Gerald L Dillingham. Weaknesses in airport security and options for assigning screening responsibilities. *The Government Accountability Office*, 21, 2001.

[26] Nancy G Edmunds. Indictment, June 2010.

[27] Justin Fishel. Exclusive: Undercover dhs tests find security failures at us airports, June 2015. URL http://abcnews.go.com/US/exclusive-undercover-dhs-tests-find-widespread-security-failures/story?id=31434881. [Online; posted 01-June-2015].

[28] Matthias Gebauer. World scrambles to tighten air cargo security, November 2010. URL http://www.spiegel.de/international/world/foiled-parcel-plot-world-scrambles-to-tighten-air-cargo-security-a-726746.html. [Online; posted 2-November-2010].

[29] Cleotilde Gonzalez. Task workload and cognitive abilities in dynamic decision making. *Human Factors*, 47(1):92–101, 2005.

[30] Michael Grabell. Just how good are the tsa's body scanners?, December 2011. URL https://www.propublica.org/article/just-how-good-are-the-tsas-body-scanners. [Online; posted 22-December-2011].

[31] Michael Grabell and Christian Salewski. Sweating bullets: Body scanners can see perspiration as a potential weapon, December 2011. URL https://www.propublica.org/article/sweating-bullets-body-scanners-can-see-perspiration-as-a-potential-weapon. [Online; posted 19-December-2011].

[32] Peter A Hancock. A dynamic model of stress and sustained attention. *Human factors*, 31(5):519–537, 1989.

[33] Miles Ed Hewstone, Wolfgang Ed Stroebe, and Geoffrey Michael Ed Stephenson. *Introduction to social psychology: A European perspective* . Blackwell Publishing, 1996.

[34] G Robert J Hockey. Compensatory control in the regulation of human performance under stress and high workload: A cognitive-energetical framework. *Biological psychology*, 45(1):73–93, 1997.

[35] Serge P Hoogendoorn and Piet HL Bovy. Pedestrian route-choice and activity scheduling theory and models. *Transportation Research Part B: Methodological*, 38(2):169–190, 2004.

[36] CE Ii. Fault tree analysis-a history. In *17th International System Safety Conference. System Safety Society*, 1999.

[37] Stef Janssen and Alexei Sharpanskykh. Agent-based modelling for security risk assessment. In *International Conference on Practical Applications of Agents and Multi-Agent Systems*, pages 132–143. Springer, 2017.

[38] Thomas H Kean, Lee H Hamilton, et al. *The 9/11 Report: The national commission on terrorist attacks upon the United States*. St. Martin's Paperbacks, 2004.

[39] Alan Avi Kirschenbaum. The cost of airport security: The passenger dilemma. *Journal of Air Transport Management*, 30:39–45, 2013.

[40] Alan Avi Kirschenbaum. The social foundations of airport security. *Journal of Air Transport Management*, 48:34–41, 2015.

[41] Alan Avi Kirschenbaum, Michele Mariani, Coen Van Gulijk, Sharon Lubasz, Carmit Rapaport, and Hinke Andriessen. Airport security: An ethnographic study. *Journal of air transport management*, 18(1):68–73, 2012.

[42] Alan Avi Kirschenbaum, Carmit Rapaport, Sharon Lubasz, Michele Mariani, Coen Van Gulijk, and Hinke Andriessen. Security profiling of airport employees: complying with the rules. *Journal of Airport Management*, 6(4):373–380, 2012.

[43] Gary Klein. The effect of acute stressors on decision making. *Stress and human performance*, pages 49–88, 1996.

[44] Gregory D Kutz and John W Cooney. *Aviation Security: Vulnerabilities Exposed Through Covert Testing of TSA's Passenger Screening Process: Testimony Before the Committee on Oversight and Government Reform, House of Representatives*. US Government Accountability Office, 2007.

[45] Oren Liebermann. Fake bomb eludes airport test, September 2007. URL `http://www.timesunion.com/AspStories/story.asp?storyID=603177&category=REGIONOTHER&BCCode=&newsdate=7/9/2007`. [Online; posted 7-September-2007].

[46] Oren Liebermann. In airport security, many say ben gurion in israel is the safest, May 2016. URL `http://edition.cnn.com/travel/article/ben-gurion-worlds-safest-airport-tel-aviv/index.html`. [Online; posted 28-May-2016].

[47] Shu-Hui Lin, Wen-Chun Liao, Mei-Yen Chen, and Jun-Yu Fan. The impact of shift work on nurses' job stress, sleep quality and self-perceived health status. *Journal of nursing management*, 22(5):604–612, 2014.

[48] SJ Mason, RR Hill, L Mönch, O Rose, T Jefferson, and JW Fowler. Dynamic security: An agent-based model for airport defense.

[49] Keaton Mowery, Eric Wustrow, Tom Wypych, Corey Singleton, Chris Comfort, Eric Rescorla, J Alex Halderman, Hovav Shacham, and Stephen Checkoway. Security analysis of a full-body scanner. In *USENIX Security Symposium*, pages 369–384, 2014.

[50] Peter Neffenger. 'reform and improvement: Assessing the path forward for tsa, October 2015. URL `https://www.tsa.gov/news/testimony/2015/10/08/testimony-reform-and-improvement-assessing-path-forward-transportation`. [Online; posted 8-October-2015].

[51] BBC News. Airlines terror plot disrupted, August 2006. URL `http://news.bbc.co.uk/1/hi/uk/4778575.stm`. [Online; posted 10-August-2006].

[52] House Committees on Transportation, Infrastructure, Oversight, and Government Reform. A decade later: a call for tsa reform, 2011.

[53] Amanda Ota. 'boring' tsa jobs may be difficult for tsa to fill, May 2016. URL http://katv.com/news/nation-world/tsa-faces-challenges-in-increasing-staff-size. [Online; posted 18-May-2016].

[54] James Pita, Manish Jain, Janusz Marecki, Fernando Ordóñez, Christopher Portway, Milind Tambe, Craig Western, Praveen Paruchuri, and Sarit Kraus. Deployed armor protection: the application of a game theoretic model for security at the los angeles international airport. In *Proceedings of the 7th international joint conference on Autonomous agents and multiagent systems: industrial track*, pages 125–132. International Foundation for Autonomous Agents and Multiagent Systems, 2008.

[55] James Pita, Harish Bellamane, Manish Jain, Chris Kiekintveld, Jason Tsai, Fernando Ordóñez, and Milind Tambe. Security applications: Lessons of real-world deployment. *ACM SIGecom Exchanges*, 8(2):5, 2009.

[56] Ben Popken. Full-body scanners don't work, israeli security expert says, April 2010. URL https://consumerist.com/2010/04/30/post-1/. [Online; posted 30-April-2010].

[57] Benn Quinn. Why europe doesn't want an invasion of body scanners, January 2010. URL https://www.csmonitor.com/World/Europe/2010/0126/Why-Europe-doesn-t-want-an-invasion-of-body-scanners. [Online; posted 26-January-2010].

[58] Craig W Reynolds. Steering behaviors for autonomous characters. In *Game developers conference*, volume 1999, pages 763–782, 1999.

[59] Anthony Roman. Tsa is 'security theater': Pro, Jun 2015.

[60] John Roth and Ben Sasse. Some cool motion sensor stuff. URL https://www.youtube.com/watch?v=OInfEePiJI0.

[61] Mark B Salter. *Politics at the Airport*. U of Minnesota Press, 2008.

[62] Bruce Schneier. Attack trees. *Dr. Dobb's journal*, 24(12):21–29, 1999.

[63] Adrian Schwaninger, Stefan Michel, and Anton Bolfing. A statistical approach for image difficulty estimation in x-ray screening using image measurements. In *Proceedings of the 4th Symposium on Applied Perception in Graphics and Visualization*, pages 123–130. ACM, 2007.

[64] Michael Shermer. The mind of the market. *Scientific American*, 298(2):35–36, 2008.

[65] AM Stefani. Aviation security federal aviation administration. office of inspector general, department of transportation. Technical report, Report Number AV-2000-070. Washington, DC, 2000.

[66] Sybert H Stroeve, Henk AP Blom, and GJ Bert Bakker. Contrasting safety assessments of a runway incursion scenario: event sequence analysis versus multi-agent dynamic risk modelling. *Reliability Engineering & System Safety*, 109:133–149, 2013.

[67] Kathleen M Sweet. *Terrorism and airport security*, volume 68. Edwin Mellen Press, 2002.

[68] TSA Blog Team. Rapiscan backscatter contract terminated - units to be removed, January 2013. URL https://www.tsa.gov/blog/2013/01/18/rapiscan-backscatter-contract-terminated-units-be-removed. [Online; posted 18-January-2013].

[69] *SCREENING MANAGEMENT STANDARD OPERATING PROCEDURES*. Transportation Security Administration, May 2008.

[70] TSA. Liquids rule, August 2017. URL https://www.tsa.gov/travel/security-screening/liquids-rule.

[71] Alan Wales, Tobias Halbherr, and Adrian Schwaninger. Using speed measures to predict performance in x-ray luggage screening tasks. In *Security Technology, 2009. 43rd Annual 2009 International Carnahan Conference on*, pages 212–215. IEEE, 2009.

[72] ASME Washington. All-hazards risk and resilience: prioritizing critical infrastructures using the ramcap plus [hoch] sm approach. ASME, 2009.

A

Appendix A

The functional state model as described in Section 5.4.3 has a lot of input parameters. The authors of the model have set these parameters based on empirical data and have developed two example personality types. Table A.1 contains the input parameters which hold for both personality types and Figure A.1 contains the parameters which are dependent on PT.

Table A.1: Input parameters of the FSM independent of PT [14]

Parameters independent of PT

$\alpha = 0.02$	$\pi = 1$
$\beta = 1$	$\phi = 0.002$
$\gamma = 60$	$BCA = 250$
$\epsilon = 1$	$LCP = 150$
$\zeta = 4$	$w_1 = 0.1$
$\eta = 0.0002$	$w_2 = 0.8$
$\mu_1 = 0.07$	$w_3 = 0.1$
$\mu_2 = 0.07$	

Table 1. Personality profiles.

Person 1 (high pq)	*Person 2 (low pq)*
Experienced pressure change parameters	Experienced pressure change parameters
PN=1.1;	PN=0.3;
PS=0.5;	PS=0.3;
ES=0.2;	ES=0.7;
HES=0.2;	HES=0.7;
LES=0.7;	LES=0.3;
NS=0.2;	NS=0.6;
Experienced pressure influence parameters	Experienced pressure influence parameters
LPS=1.2;	LPS=0.8;
HPS=0.8;	HPS=1.2;
OEP=0.8;	OEP=0.3;

Figure A.1: Input parameters of the FSM dependent on PT [14]