1. Introduction

Security checks are known amongst the public within several sectors. Train stations, events with many visitors, high risk industries or airports are some examples where one can encounter security measures. In order to better understand why security measures are taken, it firstly is important to understand what security is. This can be explained by the difference in definition of safety and security. Burns, McDermid, and Dobson (1992) define a safety critical system as a system "whose failure could do us immediate, direct harm". A security critical system is a system "whose failure could enable, or increase the ability of, others to harm us". Talbot and Jakeman (2009) extent this definition: "security is the condition of being protected against danger of loss. It is achieved through the mitigation of adverse consequences associated with the intentional or unwarranted actions of others". Security checks at the entrance of security critical systems thus are established in order to prevent visitors with malicious intends to enable their attack.

Creating security checks at the entrance of a 'system' cause the operator of the system to make different complex trade-offs. This paper will discuss three of this trade-offs. The first trade-off is that between the intensity of the security check and the effect on the system. The second is that of the privacy of the passers of the security check vs. the quality of the security check. The third is the trade-off between the performance of the security checkpoint and the deployment of security agents and the consequent costs of deployment. For this last trade-off, it is described how the use of discrete simulation could help to make this trade-off.

2. Intensity of security check.

One trade-off that has to be made by the operator of a system concerns the intensity of the security check. This is a trade-off between the level of risk and the level of costs concerned with risk mitigating measures. Risk can be defined as "the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation" (Dubois, Heymans, Mayer, & Matulevičius, 2010). The concept of ALARP (As Low As Reasonably Practicable) risks is defined as "a level of risk that is tolerable and cannot be reduced without the expenditure of costs disproportionate to the benefit gained or where the solution is impractical to implement’ (Talbot & Jakeman, 2009). The risk
should, in other words, be minimized to a level at which the cost of more treatment is excessive compared to the decrease of the level of risk (Guikema & Aven, 2010). Costs in this sense are not exclusively financial costs but also e.g. effort, time and resources (Figure 1).

The tolerability of risk can be explained by defining three regions of tolerability (HSE, 2001):

- The unacceptable region represents risk that are unacceptable, whatever the level of benefits is associated with the activity.
- The broadly acceptable region defines risk that is "generally regarded as insignificant and adequately controlled".
- The tolerable region defines risk that "people are prepared to tolerate in order to secure benefits". Toleration happens when the assessment of the risk is based on the best available scientific evidence or, when lacking, on the best scientific advice; when the residual risks are kept ALARP and when the risks are assessed periodically to ensure they still meet the ALARP criteria.

What is ‘reasonably practicable’ could be a point of discussion. Already in 1949, a UK court of appeal decision made a statement on the definition (Asquith & Edwards, 1949): “‘Reasonably practicable’ is a narrower term than ‘physically possible’ and seems to me to imply that a computation must be made by the owner, in which the quantum of risk is placed on one scale and the sacrifice involved in the measures necessary for averting the risk (whether in money, time or trouble) is placed on the other; and that if it be shown that there is a gross disproportion between them – the risk being insignificant in relation to the sacrifice – the defendants discharge the onus on them”.

Gaining an ALARP level of risk is illustrated by applying it to aviation security. For passengers, vehicles and cargo to be allowed into the security restricted area (SRA) of an airport, all should undergo a security check. Metal detectors are used to check whether people carry forbidden items on their body (Official Journal of the European Union, 2010). The metal detector is not completely fail safe. In order to be sure that no one carries a forbidden object, everyone entering the SRA should undergo a manual body search. X-ray equipment is used to analyse checked bags, personal belongings and cargo. Perhaps a better search could be executed when all bags and cargo going into the SRA would be hand searched. In both the case of the manual body check and the hand search of bags however, this would mean such an impact on the operational processes of the airport, that a compromise is made between the level (intensity) of the security check and the corresponding mitigation of risk.

3. Privacy of security check subjects

Air passengers now are used to security checks but at the moment that the first security checks at airports were performed in 1974, questions raised about the influence on the privacy or liberty of air passengers (TSA, 2014). Still, some airline passengers are concerned with their privacy when they have to pass a walk through metal detector or full body scanner (Elwazi, 2010). The opinion of the public on involvement of security authorities on the privacy or liberty of air passengers has been subject of research. Lewis (2005) describe the outcomes of an American research where the following question is posed: "is it necessary for the average person to sacrifice liberties to curb terrorism?" Only directly and up to three months after the terrorist attacks in the USA of September 11, 2001 a majority of the public answers this question with ‘necessary’. For other moments (from April 2005 to June 2002), a minority
answers with 'necessary'. Although the privacy or liberty issue thus lives amongst the public, not everyone is against less privacy or liberty for more security.

In the present day, due to the existence of computers and database systems, much more data can be collected about persons than in the time of the first aviation security measures. The American TSA uses the Computer Assisted Passenger Prescreening System (CAPPS) to separate high risk airline passengers from the other passengers. The CAPPS system screens the information airlines have about their passengers (e.g. one way or return ticket, method of payment, time of making the reservation in relation to the flights departure). When this information complies with a classified combination of factors, the passenger is indicated as high risk and has to undergo extra security measures at the check-in gate. TSA is developing a successor of CAPPS, CAPPS II. Using the passenger name record information from the airlines’ reservation system, much more governmental and private databases can be used to apply data-mining techniques in order to determine whether a specific airline passenger poses a risk to the civil aviation sector (Poole & Passantino, 2003). This CAPPS II system will use much more person specific data and thus will, according to opponents of sacrificing liberties to curb terrorism, make a bigger infringement on airline passengers’ privacy.

Poole and Passantino (2003) identify as the main privacy or liberty issue in security related questions the difference between the choice of undergoing a screening at a private company voluntarily or undergoing a screening at a governmental body involuntarily. Voluntarily screenings exist at e.g. AAS for frequent flyers who participate in the Privium programme: members of this programme agree to keep a scan of their iris in a database in order to be able to scan their passports their self and avoid long queues at immigration (Schiphol Group, 2014). Airline passengers scanned by the CAPPS II system are involuntarily subjected to a scan of their personal data and storage of this data for 50 years when marked as a high risk passenger.

4. Performance of security checkpoints

The third discussed trade-off that the operator of a safety critical system should make is between the performance of a security checkpoint and the costs involved with the deployment of security agents. Security checks do not cause financial benefit but only cost money. From a commercial point of view, the operator of the system wants to cut these costs as much as possible, whilst being compliant to the applicable rules and/or legislation on the system and/or positioning the level of risk to the aforementioned level of ‘tolerable’. From this same commercial viewpoint however, the systems operator does not want his clients to have to wait for such a long time that their satisfaction in the security check decreases. On the other hand, it is expensive for the systems operator to have its employees waiting for a security check instead of being productive. There is thus a trade-off between costs and performance of security checkpoints.

5. Using simulation to deal with the trade-off between performance and deployment

Analysing this trade-off between costs and performance of security checkpoints was subject of research of (de Graaf, 2014). At Amsterdam Airport Schiphol (AAS) the vehicle security checkpoints (VSC) were subject of analysis. These VSC’s are the barrier for vehicles (catering, contractors, maintenance, cleaners) that have a destination at the airside of the airport and travel between the public area of the airport and the security restricted area.

First, different performance indicators are formulated so that the performance of a security checkpoint can be assessed (see the output of the simulation model in Figure 2). Then, a general applicable discrete event simulation model is made of the non-passerger security checkpoints.
With registrations from a database in which the use of the airport identity card is logged, the arrival patterns of employees and vehicles are subtracted. This serves as input for the simulation model. The simulation model is made in such a way that it delivers the performance indicators as output after simulation.

The performance indicators for the security checkpoints at AAS are as follows:

- Wait time (average per 15 minutes)
- Throughput time (average per 15 minutes, sum of wait time and process time)
- Percentage of vehicles that has a wait time within the defined wait time norm.
- Efficiency of deployed security agents in the vehicle search lane (% active time / (active time + idle time))
- Costs per vehicle passage (€/vehicle)

For this research, the process time of a vehicle security check is not incorporated in the performance indicators, since this is a result of the security procedure. Reviewing the actual security procedure and possibly improving it is out of scope of this research. The simulation model presents the aforementioned performance indicators over the day. Because the simulation model uses a predefined random distribution to determine the process time of a security check, it is important not to base the analysis on only one model run or execution.

Simulating the system for several days and taking the average values for the performance indicators per unit of time gives insight in the average value for the performance indicators and the confidence interval of the results. Due to e.g. an earlier system error, an accident on the access road or strong disturbance of the airlines’ schedules it could however occur that more vehicles arrive at the security checkpoint than in the average case. For this reason, different arrival patterns (average, average + 0.5σ and average +1σ) are used in the analysis.

The parameter that AAS as operator of the system easily can influence is the number of deployed security agents over the day. The number of deployed security agents in the vehicle search lane has an effect on the wait time, throughput time, efficiency (all negative causal relations), the costs per passage and the percentage of vehicles with a wait time within the norm (both positive causal relations). By adapting the number of deployed security agents, the minimum number of needed security agents per unit of time can be determined, whilst taking into account the percentage of vehicles that has a wait time within the norm. The ‘reaction’ of the system to the increase of arriving vehicles in relation to the normal arrival rate tells something about the efficiency of the deployment of security agents. When the system performs the same under the average arrival pattern as under the extreme arrival pattern; this tells that perhaps too much security agents are deployed. When however a slight increase of arrivals cause a drastic increase of wait time, this means that the security checkpoint under analysis is not capable of handling minor deviations and thus the performance of the security checkpoint is sensitive for disturbances. By incorporating the different performance indicators, a good deployment schedule for security agents can be formulated.
6. Conclusion

Three trade-offs that operators of security critical systems have to make are discussed. The first trade-off is between intensity of a security check and the performance of the system: security risks should be ALARP. This means that the risk should be at such a level that exposure to less risk could only be achieved by making excessive costs. The second trade-off is about privacy of the users of the security critical system. A distinction is made between voluntarily and obliged participation in security scans from either private companies of governmental bodies. The discussed trade-off is between performance of a security checkpoint and the deployment of security agents. An approach using a simulation model is discussed, which can help to make the trade-off and determine the best deployment of security agents.

7. References


EU Regulation 185/2010 on laying down detailed measures for the implementation of the common basic standards on aviation security, 4 C.F.R. (2010).


