Key Performance Indicator for Security Measurement at Airports

Olaf Milbredt*and Julia Strer†
German Aerospace Center (DLR)
Institute of Air Transport and Airport Research
Lilienthalplatz 7, 38108 Braunschweig, Germany

Airport Management nowadays is based on scattered information. The flow of such important information as an unattended piece of luggage from security officers to airline personnel is tenacious. A collaborative airport management culture can speed up the flow provided that appropriate data are available. We introduce the notion of a Level of Security comprising of a number, which sums all security facts to make the overall security situation easily accessible, and a management structure. With the help of this notion, decisions handling security situations are not only based on intuition and experience, but also on an indicator, which mines all internal and external sources. Determining the Level of Security involves opinions and is subjective. With the help of Fuzzy Logic, such subjective arguments can be addressed in a systematic fashion.

Keywords: Collaborative Airport Decision Making; Total Airport Management; Airport Security; Decision Support System; Fuzzy Logic

Nomenclature

KPI	Key Performance Indicator
KCP	Key Control Parameter
A-CDM	Airport Collaborative Decision Making
TAM	Total Airport Management
FIS	Fuzzy Inference System
HCD	Human Centred Design

I. Introduction

Facing security issues is one of the most serious challenges of airport management. To minimize attrition of information flow between different stakeholders, a collaborative communication method needs to be applied. The infrastructure was introduced in Europe by EUROCONTROL named Airport Collaborative Decision Making (A-CDM).[1,2] This infrastructure was enhanced by EUROCONTROL and the DLR by including a collaborative plan for the whole airport. This concept is called Total Airport Management (TAM).[3] Besides information sharing a key ingredient of both concepts are the definition of so-called Key Performance Indicators (KPIs) providing an overview of the state of an airport. As an enhancement we introduce the notion of Key Control Parameters (KCPs) denoting parameters that can be adjusted to influence the KPIs. There may be other parameters having an impact on the state of an airport, but are not adjustable. KPIs can therefore be seen as functions of the variables KCPs and non-adjustable parameters.

In this study, we focus on the management concept for security at airports including computing and visualizing security facts in one KPI called Level of Security, the influencing KCPs, and non-adjustable parameters. The proposed list of the influencing parameters only contains the most important one and is not intended to be exhaustive. The depiction of the value of the Level of Security should respect the elements of Human Centered Design (HCD).[4] It is

*Ph. D. , Research Assistant, olaf.milbredt@dlr.de
†Research Assistant, julia.strer@dlr.de

intended to help being aware of the overall security situation while including at the same time all relevant facts. A characteristic situation is a security door provided with a card reader. If an attempt to pass this door fails, how is this situation to be assessed? It may be a technical failure or a possible security breach. In this case, an indicator based on the overall security situation would help a security officer to interpret this situation.

Experience is one of the key ingredients to cope with security situations. Since it can not be described in terms of numbers, a more flexible notion needs to be used. At this point, Fuzzy Logic comes naturally into play, because the rules of a Fuzzy Inference System (FIS) can be interpreted as linguistic statements. Subjective knowledge can be captured and used within a computer program.

Siu described a general probabilistic risk approach like it is used in safety-related decision-making and applied it to an aviation security context.[5] The approach includes scenario identification and definition of undesired consequences. Siu also considers security measures and scenarios resulting when the security barriers fail. For measurement of security situations quantitative scenario probabilities are determined. According to Siu the probabilistic risk approach is faced to special requirements of the aviation security, namely threats trying to overcome security measures, a broad potential range of threats, human factors and influence of global factors. For this reason Siu concludes that the probabilistic risk approach has to be adapted to these characteristics of the aviation security problem before it can be used for aviation security decision making.

Tamasi and Demichela propose some quantitative and qualitative methods to assess the risk in civil aviation security, where quantitative risk assessment techniques are based on threats, vulnerabilities and criticality concepts.[6] RAMS methods were transferred to obtain vulnerability and criticality. The threat assessment, which is described as critical because of large uncertainties and lack of objectivism, completes the risk assessment procedure. The result of this risk assessment is the likelihood, that an attack is successful in the selected scenario. Shafieezadeh *et al*. present a similar approach of security risk analysis consisting of scenario identification, consequence and criticality assessment, security vulnerability assessment, threat likelihood assessment and life-cycle cost assessment.[7] Especially the stage of success of attackers and defenders is implemented. Another approach to deal with the assessment of security at airports was presented by Cole and Maurer.[8] It enables to identify weaknesses in the airport security system. The proactive approach works by utilization of scenario analysis and structural complexity management, for example Domain Mapping Matrices are used. It allows systematically considering and analyzing a multitude of possible threat scenarios. Portfolio representations visualize the potential for improvement of the security level by assessment of security measures related to the analyzed thread scenarios.

Our approach to airport security is management-driven and not risk-driven. It is not an attempt to determine or calculate the actual risk of an attack at any time, since this may be hard to determine.[a] Especially, the probabilities contained in a risk-based approach may be hard — if not practically impossible — to fathom. A risk analysis founds the basis for any work in the security field. A criticism of our approach may be the circumstance that we do not calculate the "Level of Security"as such. We see the approaches not to compete,but to complement each other.

Fuzzy Logic has been applied to airport ground operations. A fuzzy representation of the time needed for a specific operation was used to study air cargo ground operations.[9] With the help of semantic modeling of the situations occurring the security of ground operations is studied.[10] Here, fuzziness is used to model airport situations such as runway conflicts.

II. Theory

In this section, we develop a Fuzzy Logic framework for the Level of Security.

II.A. Fuzzy Inference System

In this section we shortly depict the properties of a FIS.

II.A.1. Fuzzy sets

Fuzzy logic is based on so-called fuzzy sets introduced by L. Zadeh.[11,12] An element of a fuzzy set can have a degree of membership different from $\{0, 1\}$. Analog to sets and their characteristic function, a fuzzy set $U \subset X$ is represented by its membership function $\mu(x)$. It maps elements from the universe of discourse X to the interval $[0,1]$ attaining

[a] Assessing the overall risk may be challenging. If one considers the placement of a bomb, there are at least three different parameters: place, time, and destructiveness. These parameters are continuous and therefore, the consideration of a finite number of scenarios may not capture the full feature of the underlying probability distribution.

the degree of membership for each element $x \in X$. Logical operations such as AND, OR are carried out in an analog manner to "ordinary" sets using the membership function.

II.A.2. Linguistic variable

To connect the values of a variable with values in an interval $[a,b]$ to the concept of fuzzy sets we introduce the notion of a *linguistic variable*. Its values are a weighted sum of *linguistic terms* or *categories* which represent fuzzy sets within the interval $[a,b]$. The union of all linguistic terms of a linguistic variable cover the interval $[a,b]$, therefore no value has a membership value of 0 with respect to all linguistic terms. A crisp value can now be divided up in parts belonging to different linguistic terms. This procedure is called *fuzzification*. The inverse procedure is called *defuzzification*. There are different ways of extracting a crisp value from a linguistic variable. We use the *center of gravity (COG)* defined by

$$COG(\mu) = \frac{\int_X \mu(x)\, x\, dx}{\int_X \mu(x)\, dx}\,. \tag{1}$$

II.A.3. Rules

The key ingredient of a FIS is a link between input and output parameters based on rules.[13] A rule is an IF-THEN-clause consisting of conditions for the fuzzified input parameters and a statement for the output variable. Different styles exist for the form of this statement. All rules are evaluated for given crisp parameters and are *aggregated* to a value for the output linguistic variable using the logical OR. We use the min and max for the logical operators AND and OR, respectively.
The workflow of a FIS can be summarized by

$$\text{crisp input} \to \text{fuzzification} \to \text{rule evaluation} \to \text{aggregation of rule consequences} \to \text{defuzzification} \to \text{crisp output}\,.$$

EXAMPLE To get an image of the technique we present an example of controlling heating of a room. As crisp input value we take the temperature and the output variable named heating consists of a linguistic variable with linguistic terms "low", "medium", and "high". The input linguistic variable has the linguistic terms "cold", "average", and "hot". We use triangle shape for all linguistic terms, e. g. "medium" is defined by the fuzzy set with the membership function μ given by

$$\mu(x) = 0,\ x \le 15,\ \mu(x) = 1,\ x \in [16,19],\ \mu(x) = 0,\ x \ge 20\,,$$

and μ attains the value of the linear connection on the intervals $(15,16)$ and $(19,20)$. A crisp temperature is then a linear connection of linguistic terms, e. g.

$$19.5 = \alpha_1 \text{ average} + \alpha_2 \text{ hot} \quad \text{with factors } \alpha_1, \alpha_2 > 0.$$

A rule is e. g. given by

$$\text{IF TEMPERATURE IS HOT THEN HEATING IS LOW.}$$

II.B. Application to the Level of Security

Experts are supposed to identify different parameters influencing the overall security situation of an airport. These are treated as input parameters of a FIS. The output parameter is supposed to be the Level of Security.

II.C. Parameters

This section is devoted to parameters used by the Fuzzy Logic framework. We use the notion "pax" for passenger. In the following we show two tables. One shows KCPs and the other shows non-adjustable parameters. We also listed the dimension and the domain of the respective quantity. The lists are not intended to be exhaustive and may be amended or altered.

Tab. 1 shows parameters influencing the security situation that are adjustable and therefore are treated as KCPs. Some of them are depending on a long-time planning ("training" and "experience") and others are adjustable in a short period of time as e. g. "patrols per pax". X-ray machines belonging to "technical equipment" have an adjustable sensitivity, therefore this parameter is classified as KCP.

Table 2 shows parameters that are given by the circumstances of the specific airport and time, and are therefore classified as non-adjustable. The weight of the different parameters may be different, e. g. the existence of an actual

Table 1. Key Control Parameters influencing the overall security situation

KCP	Dimension	Domain
patrols per pax	number per pax	$[0,\infty)$
training	days per year	$[0,\infty)$
stress of security officers	stages	generic $[0,10]$
queue length	pax	$\mathbb{N}$
working conditions	stages	generic $[0,10]$
experience	years	$[0,\infty)$
technical equipment	stages	generic $[0,10]$

Table 2. Parameters influencing the overall security situation

Non-adjustable Parameter	Dimension	Domain
airport volume	pax per year	$\mathbb{N}$
density of persons	pax per m^2	$[0,\infty)$
actual flight	state $\times$ state	origins $\times$ destinations
national threat level	stages	$\{1,\ldots,5\}$
actual threat	yes/no	$\{0,1\}$

threat has a great impact on the security situation in contrast to the airport volume influencing the attractiveness for an attack. We classify this parameter as globally affecting the risk situation of a specific airport. It is therefore not considered for the calculation of the KPI for all-day use.

II.D. Rules

In this section we outline the plot for deriving rules from questionnaires of security experts providing the weighting of the parameters shown in Tabs. 1 and 2.

II.D.1. Generic rules

Exemplary, we use two parameters, namely "patrols per pax" and "density of persons". The parameters can be thought of as corresponding in the way that a higher value for "patrols per pax" increases and a higher value for "density of persons" decreases the "Level of Security".

We use five categories named "very low", "low", "medium", "high", and "very high" for both parameters and the "Level of Security". The following table shows a set of rules which are derived by identifying "very low" with $-1/2$ and "very high" with $1/2$.

Table 3. Generic rules for a positively and a negatively influencing parameter

	very low	low	medium	high	very high
very low	medium	high	very high	very high	very high
low	low	medium	high	very high	very high
medium	very low	low	medium	high	very high
high	very low	very low	low	medium	high
very high	very low	very low	very low	low	medium

The horizontal parameter of Tab. 3 is supposed to influence the "Level of Security" in a positive way, while the vertical one is assumed to have negative impact. The identification leads to a symmetric table of rules as a consequence of the assumption that both parameter have equally weighted impact.

Each entry of Tab. 3 represents one rule. The antecedent consists of the conjunction of the two parameters, i. e. the table leads to a set of rules as e. g.

IF DENSITY OF PERSONS IS HIGH AND PATROLS PER PAX IS MEDIUM THEN LEVEL OF SECURITY IS LOW.

II.D.2. Adaption by weights

In this section we show, how to alter generic rules according to weights of the parameters. Assume the importance of "patrols per pax" to be α-times higher than "density of persons". The coefficient α is supposed to be positive. A value of 1 leads to equally weighting of the parameters. Since we used the sum to combine the identified values of the different categories, we need to alter the combination process. We introduce a new identification with an additional summand β for "patrols per pax". The importance factor of the identification can be derived by

$$(\text{“patrols per pax”} = \text{low})/(\text{“density of persons”} = \text{high}) = 4\beta + 1 \stackrel{!}{=} \alpha\,.$$

This condition is consistent with the denotation of α.

EXAMPLE The next table shows the case $\alpha = 2.5$. The set of rules in Tab. 4 is not symmetric as in Tab. 3. The

Table 4. Rules for positively and negatively influencing weighted parameters

	very low	low	medium	high	very high
very low	low	medium	very high	very high	very high
low	very low	low	high	very high	very high
medium	very low	very low	high	very high	very high
high	very low	very low	medium	high	very high
very high	very low	very low	medium	medium	high

influence of the horizontally aligned positively influencing parameter has slightly increased.

III. Management Structure

In this section, we discuss different methods to implement a Level of Security embedded in an Airport Operation Center (APOC).[3]

A Level of Security as a number is in itself useless, if it is not embedded in a user-friendly system. The parameters of Tables 1 and 2 are automatically generated whereas an unattended piece of luggage poses a threat which has to be announced manually. The context of such a threat can be identified using the actual Level of Security, because all information influencing the strength of the threat are summarized in this indicator. If the actual threat level for the specific airport is high, then the situation has to be cleared with more caution. In Fig. 1 the flow chart of the

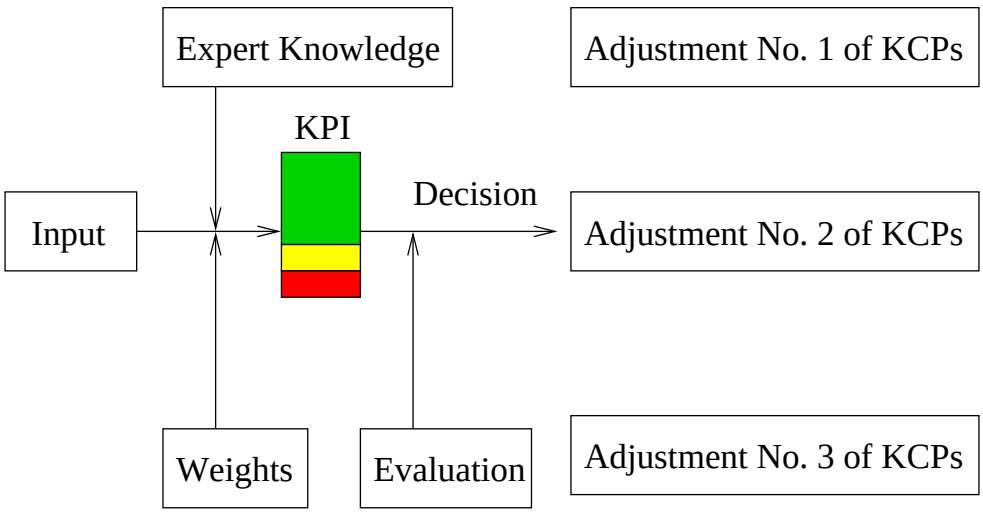

Figure 1. Flow chart and information flow of the management structure for the KPI "Level of Security"

management structure is shown, in which the number Level of Security is embedded. The figure is to be read from left to right. From an input, the number Level of Security is computed respecting expert knowledge, which is encoded in the rules (cf. Tabs. 3 and 4) of the FIS, and the weights of the different parameters identified by the experts, where input denotes the parameters of Tabs. 1 and 2. The number is displayed in a colour-coded way using the colours of

a traffic sign to be easily accessible. The colour correspond to the regions preferred, possible, impossible of KPIs proposed by A-CDM and TAM. Here, we use the wording normal region, region with increased attention, and critical region for green, yellow, and red.

If the number Level of Security lies in a non-normal region, an adjustment of the KCPs described in Tab. 1 is necessary. A Decision Support System identifies possible reactions and the evaluation of these is performed by the FIS to compute the Level of Security. The Decision Support System is then able to recommend an adjustment of specific KCPs on basis of the evaluation result.

Since the Level of Security is computed per room, every security breach can be located and should be enriched with information about what happened, who, if there is one, announced the breach, what has to be done, and who is responsible. What has to be done is dependent on the local Level of Security.

IV. Application

In this section we show examples of a FIS employing generic rules described in Tab. 3. We employ the parameters "revealing risks" and "density of persons", where the first one is a combination of various KCPs as e. g. "patrols per pax", sensitivity of technical equipment, etc.

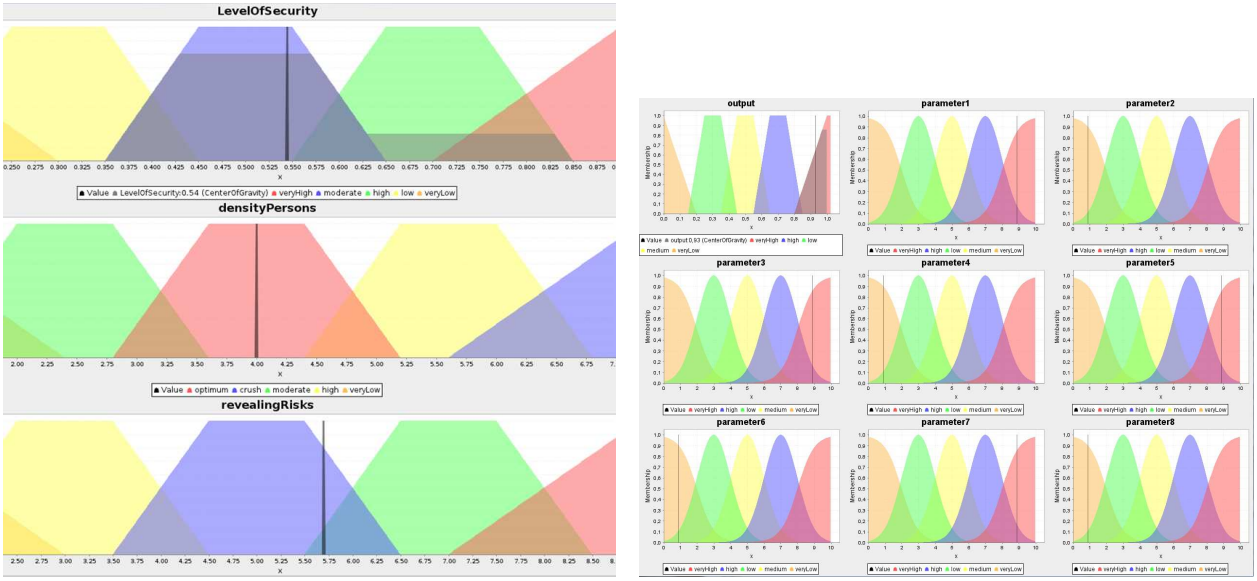

Figure 2. Left: FIS with two input parameters; Right: FIS with eight input parameters and Level of Security as output parameter

On the left of Fig. 2 five categories together with generic rules are used. Parameter "densityPerson" is assumed to be negatively influencing the output parameter LevelOfSecurity, whereas the parameter "revealingRisks" is assumed to have positive impact. The output parameters is computed by the COG of the grey filled region. Whereas on the left rectangular membership functions are used, on the right of Fig. 2 this type of function is only used for the output parameter. All other membership functions are chosen as Gaussian. Eight different input parameters are shown, several of which have positive effect and several have negative impact on the output parameter. The challenge in this case was the generation of generic rules, since in this case $390,625$ rules need to be generated.

The following figure show the Level of Security calculated with a FIS comprising of two parameters called "density of persons" and "revealing risks". The first one is supposed to have negative impact and the second one is assumed to have positive influence on the Level of Security. The range of the two parameters is taken to be $[0, 10]$ and the Level of Security is assumed to have values in $[0, 1]$. We use sigmoidal and Gaussian functions for the membership functions of both parameters as shown on the right of Fig. 2. We calculated the Level of Security with one parameter fixed in the case of symmetric weighted parameters as given by Tab. 3 and in the case of the parameters "revealing risks" to be $\alpha = 2.5$ times more important than "density of persons" as given by Tab. 4. In Fig. 3 it can be seen that "density of persons" has negative impact on the Level of Security. The graphs shown in Fig. 4 are closer together and are overall subordinate than the graphs shown in Fig. 3. This stems from the weighting introduced, since the parameter "revealing risks" is assumed to be more important than the other.

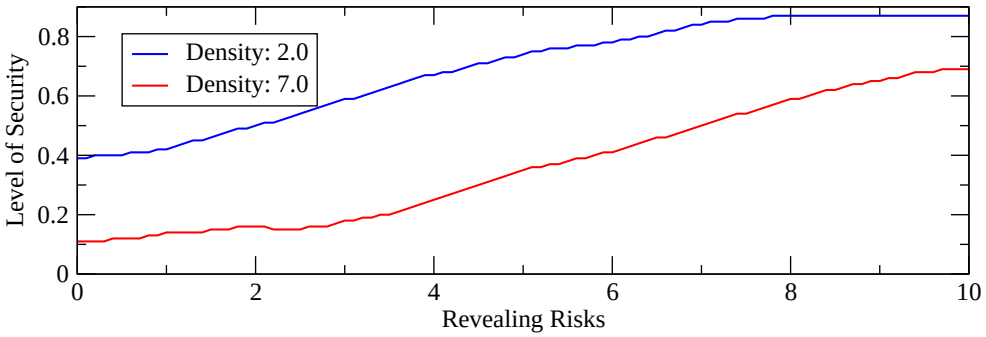

Figure 3. Level of Security calculated with fixed "density of persons" and symmetrically influencing parameters (cf. Tab. 3)

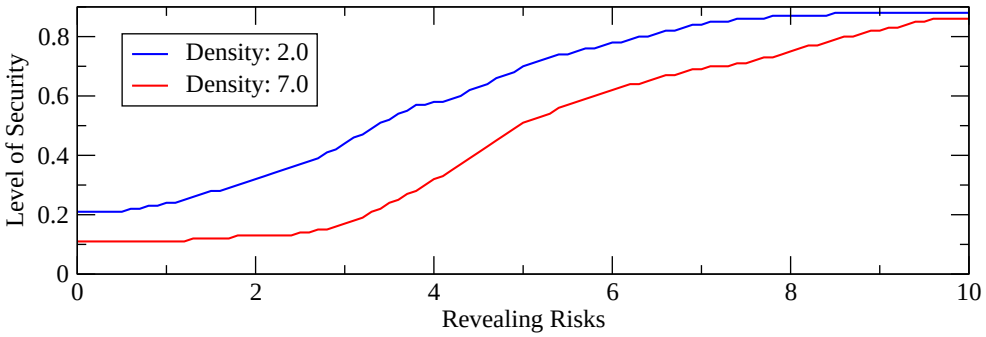

Figure 4. Level of Security calculated with fixed "density of persons" and weighted parameters (cf. Tab. 4)

For completeness we calculated the Level of Security for fixed "revealing risks" depicted in Fig. 5. The symmetric weighting can be seen, since the shape of the two graphs coincide roughly with the shape in Fig. 3 The last picture, Fig. 6, better unveils the weighting. The blue graph is higher than the blue graph in Fig. 5 and the red graph is lower. This shows that the value of "revealing risks" has more impact on the Level of Security than "density of persons".

V. Conclusions

Ensuring air transport to be safe and secure is one of the key issues of air transport management. Data retention and storing of passenger flight data suggest the possibility to automatically identify the "bad guys". In the end, experienced security personnel is required to identify not only the traces in virtual reality, but in the real world.

In this paper, we developed the concept of a KPI named "Level of Security". It consists of a value representing the overall security situation at an airport and a Decision Support System with an interface respecting the key elements of Human Centered Design. A list of parameters influencing the overall security situation is presented. The parameters are combined into one value by Fuzzy Logic. It is therefore able to scientifically extract experience from security personnel. Such a system would increase the situational awareness of security relevant incidents, but otherwise mine the rich experience of the security personnel to mark incidents that are not relevant as such.

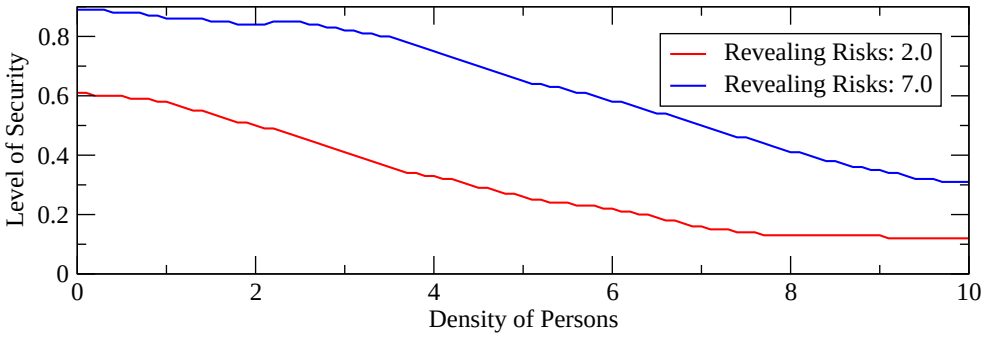

Figure 5. Level of Security calculated with fixed "revealing risks" and symmetrically influencing parameters (cf. Tab. 3)

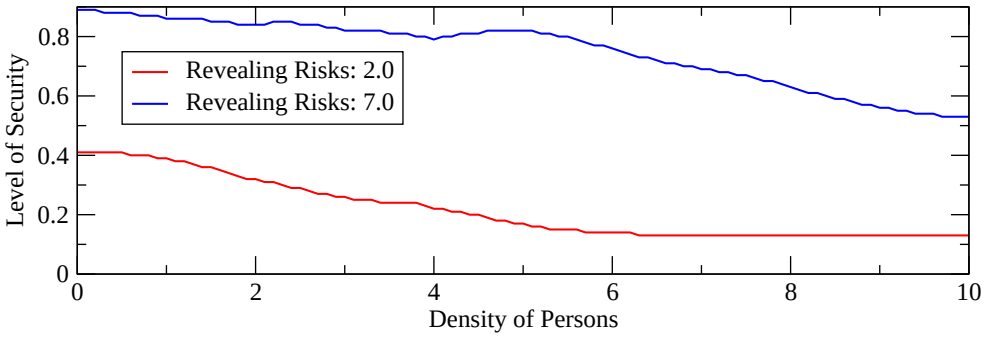

Figure 6. Level of Security calculated with fixed "revealing risks" and weighted parameters (cf. Tab. 4)

A set of rules for the calculation on basis of the parameters "patrols per pax" and "density of persons" and its application to some example incidents is shown. Furthermore, we give a suggestion for implementing the proposed Decision Support System enabling the security personnel to face challenges concerning security issues in day-to-day operations.

To adapt the Fuzzy Inference System to meet the needs of a specific airport, questionnaires of local security personnel may be necessary. The outcome can be used to adapt the calculation of the "Level of Security". We developed a method for including the weightings derived by such a questionnaire in the rule set of a FIS. This method is apply to a fixed weight and a FIS consisting of two parameters producing a set of rules. From this set it can be seen that the symmetry of a generic set of rules is broken to include the fact that one parameter is more important than the other. The generic case and the weighted case are shown in pictures, where the Level of Security is calculated for one parameter fixed.

An enhancement of the approach comprises of using a Neuro-Fuzzy system. With such a system, the Decision Support System is enabled not only to include the expert knowledge as such, but also the reaction on specific situation occurring in all-day operations. The advantage over a pure Neural Network consists of the possibility to retrace, how the system came to its decision, whereas a Neural Network comes to a value without this ability.

The approach can be combined with a risk assessment of an airport to further adjust calculation and treatment of incidents. In such a way new weightings for the parameters or even new parameters for calculation can be obtained providing a more accurate picture of the overall security situation.

References

[1]EUROCONTROL, "Airport CDM Operational Concept," http://www.euro-cdm.org/library/cdm_ocd.pdf, September 2006.

[2]EUROCONTROL, "Airport CDM Implementation — The Manual, v. 4," http://www.eurocontrol.int/sites/default/files/publication/files/2012-airport-cdm-manual-v4.pdf, April 2012.

[3]EUROCONTROL and German Aerospace Center (DLR), "Total Airport Management Operational Concept," http://www.bs.dlr.de/tam/Dokuments/TAM-OCD-public.pdf, October 2006.

[4]Maguire, M., "Methods to support human-centred design," *International Journal Human-Computer Studies*, Vol. 55, 2001, pp. 587–634.

[5]Siu, N., "Probabilistic risk assessment: a tool for aviation security decision making," *The Aviation Security Problem and Relates Technologies*, edited by W. H. Makky, Vol. CR42, 1992, pp. 182–211.

[6]Tamasi, G. and Demichela, M., "Risk Assessment Techniques for Cicil Aviation Security," *Reliability Engineering and System Safety*, Vol. 96, No. 8, 2011, pp. 892–899.

[7]Shafieezadeh, A., Cha, E., and Ellingwood, B., "A decision framework for managing risk to airports from terrorist attack," *Risk Analysis*, Vol. 35, No. 2, 2015, pp. 292–306.

[8]Cole, M. and Maurer, M., "Managing complex socio-technical systems: A proactive approach to airport security," *International Journal of Knowledge-Based and Intelligent Engineering Systems*, Vol. 18, No. 3, 2014, pp. 191–200.

[9]Han, T.-C., Chung, C.-C., and Liang, G.-S., "Application of Fuzzy Critical Path Method to Airport's Cargo Ground Operation Systems," *Journal of Marine Science and Technology*, Vol. 14, No. 3, 2006, pp. 139–146.

[10]Furno, D., Loia, V., and Veniero, M., "A fuzzy cognitive situation awareness for airport security," *Control and Cybernetics*, Vol. 39, 2010.

[11]Zadeh, L., "Fuzzy sets," *Inf. Control*, Vol. 8, 1965, pp. 338–353.

[12]Zadeh, L., "The Concept of a Linguistic Variable and Its Application to Approximate Reasoning I, II, III," *Information Sciences*, Vol. 8, 1975, pp. 199–249.

[13]Takagi, T. and Sugeno, M., "Fuzzy identification of systems and its applications to modeling and control," *Systems, Man and Cybernetics, IEEE Transactions on*, Vol. SMC-15, No. 1, Jan 1985, pp. 116–132.