HOUSE OF SECURITY: A STRUCTURED SYSTEM DESIGN & ANALYSIS APPROACH

S. DROR, E. BASHKANSKY & R. RAVID
Industrial Engineering and Management Department, ORT Braude College, Israel.

ABSTRACT

Security managers must always be on guard to prevent terrorist and criminal attacks against their organizations. This paper presents a comprehensive methodology for organizational security decision-making process and security system design. It builds on the house of quality (HOQ) (a customer-requirements planning matrix) by developing a house of security (HOS) that can translate the likelihood and severity of attack scenarios against organizations into a structure comprising security system components ranked according to their likely effectiveness in preventing an attack. We assume that correlations between the system components might be changed for each scenario, i.e. several roofs, corresponding to the number of rows in the HOS matrix. For comparing different security systems designed to prevent the same threats, a measure of effectiveness is proposed. The analysis of variance method is utilized to select the vital security components by dividing the security components into two groups: vital few and trivial many.

The HOS method is implemented for hotel protection from a terrorist attack, revealing five components as dominant for security: Operating procedures, TV cameras, internal personnel, entry control, and visual information analysis. A partial analysis to identify the most important component for protecting a specific place (parking area) shows that the number of the vital components decreases and the dominant components for preventing parking area threats are operating procedures and internal personnel.

Keywords: Decision making, quality functional deployment (QFD), security system.

1 INTRODUCTION

With terrorism threatening targets around the world, especially in unstable regions, and the growing sophistication of criminals and their machinations, the tasks of security managers have never been more formidable. The security system design process involves a difficult and complex balancing act that must take into account many different interests and values such as risk probabilities and costs. Each system component requires separate consideration, in tandem with analysis of the interaction between components. Understanding a client's risk perceptions and effectively communicating risk is critical in helping clients make informed decisions regarding the security system needed. Disciplines such as operations research, statistics and quality management are usually applied in order to provide a framework for constructing models of security decision making.

A variety of analytical methodologies and algorithms has been developed for this purpose. Transportation security systems have received special attention in the literature, particularly since the September 11 terrorist attacks on the U.S. Stewart and Mueller [1] presented a cost–benefit analysis of advanced imaging technologies (AITs) for passenger screening. Threat probability, risk reduction, losses and costs of security measures were taken into consideration in the calculation of estimated costs and benefits. The authors concluded that the attack probability per year needs to be extremely high in order for AIT installation and use to become cost-effective.

Majeske and Lauer [2] developed Bayesian decision models of two passenger prescreening systems: two-way and three-way classification schemes. Each scheme is explored from

ISSN: 2041-9031 (paper format), ISSN: 2041-904X (online), http://journals.witpress.com
DOI: 10.2495/SAFE-V2-N4-317-329

both the government and passenger perspective. The authors developed optimal levels of undesirable personal characteristics that would enable people to be categorized, taking into account the probability of undesired passengers, misclassification probabilities and costs.

Xiaofeng [3] studied the case where passengers are categorized as one of several risk classes, according to their risk characteristics. Every passenger has to be checked by a set of mandatory stations and by an additional group of check stations that is adapted to his or her risk class. The author used mixed integer programming to determine the check station assignments for each class of risk in order to minimize the overall Type II error probability and keep the overall Type I probability within a set limit, subject to time available and staffing needs at each check station. The authors concluded that by 'tailoring' a screening process for each passenger, according to his or her risk class, the same probability of a Type I error may be achieved, while probability of a Type II error can be reduced using fewer screeners.

Lee and Jacobson [4] introduced passenger assignment procedures that balance the trade-off between maximizing security and minimizing the expected duration of the passenger security process. Using elements from queuing theory, the authors presented a static and dynamic passenger allocating system. In the first procedure the security system is assumed to be in steady state. Passengers are assigned to a security class, regardless of all prior passenger assignments and the procedure determines the security class thresholds that minimize the expected customer delay. The second procedure is a dynamic policy for passenger assignment, assuming that the system has not yet reached steady state. The sequence of security class thresholds is determined for each passenger according to his or her risk class. Both procedures are implemented for selective security system analyses and its application to the self-select program. Numerical analyses illustrate the effectiveness of both methods in reducing the expected passenger sojourn time in the security system. The dynamic assignment policy can be implemented to create a balance between maximizing security and passenger throughput.

Hassoun *et al.* [5] used elements from queuing theory in order to model illegal border crossing and security agents' reactions. The authors proposed a stochastic attention allocation of security agents and a reactive schedule model, based on a semi-Markov decision-making process. The objective function is the overall failure rate that should be minimized under total service capability limitation and the reaction rates are the policy decision variables. The proposed policy was investigated using simulation and outperformed alternative policies.

Niyazi [6] applied game theory to security system modeling. He implemented a Stackelberg game for analyzing resource allocation strategies to improve cargo container transportation security. The model shows that there is a trade-off between the security of foreign seaports and the security of other sites such as warehouses, container yards. Niyazi also showed that the equilibrium is sensitive to security cost effectiveness.

Keeney and Von Winterfeldt [7] developed a value model for evaluating homeland security decisions and allocating the security resources' costs effectively, using estimated values of the probability of various types of threats, vulnerability, consequences and costs. The model includes four steps: identifying objects, specifying metrics to measure objectives, combining achievement of different objective and value judgments about the relative importance of reducing risks and the cost reduction. The authors conclude that such a value model would guide the decision making and actions to construct a high quality security policy. The knowledge and techniques needed for building the proposed model are summarized in the paper.

In the main, previous research related to security decision making has focused on specific systems such as aviation transportation systems and aimed to provide deep insight into the effectiveness and utility of some devices or operation policies. The security standard ISO 28000:2007 [8] was developed to organize security operations within the broader supply chain. The standard specifies the requirements for a security management system, including the aspects critical to security assurance for any organization or enterprise wishing to manage its security and activities.

In the past, organizations have tended to address various aspects of security separately, often assigning different responsibilities to different distinct departments such as information technology, physical security and fraud prevention. Today, there is a greater recognition of the interconnected nature of security requirements and that a holistic approach is needed for preventing different types of hazards. This growing awareness informs our development of a comprehensive methodology for organizational security decision-making processes and security system design.

The methodology proposed herein – the house of security (HOS) methodology – uses a generic quality function deployment (QFD)-based framework to organize security decision making and streamline the process. The QFD technique is well-known for creating a linkage between product design, customer needs and process requirements and is extended here for methodology needs. The methodology provides the client with an objective assessment of potential vulnerabilities and gaps that enable him or her to construct a risk profile. Based on the risk profile, the security engineer can propose optional security systems. The effectiveness of each security system is evaluated using the appropriate measure. The latter is based on the expected loss measure, which was developed earlier by the authors (see Bashkansky *et al*. [9]). An analysis of variance (ANOVA) procedure is implemented to divide the set of security components into a group of dominant vital components and a complementary group of less important items. The methodology implementation is demonstrated by a detailed example of a hotel security decision-making process.

2 HOUSE OF SECURITY

Leading companies around the world have been using QFD since 1966. Its two-fold purpose is to assure that true customer needs are properly deployed throughout the design, building and delivery of a new product, and to improve the product development process itself [10]. Typically, the approach is described in terms of a four-phase model consisting of four successive stages or matrices: (1) an overall customer requirement planning matrix [also called the house of quality (HOQ)]; (2) a final product characteristic deployment matrix; (3) a process plan and quality control charts; and (4) operating instructions. An HOQ maps the WHATs, representing desired customer product attributes defining voice of customer, into the HOWs, the technical characteristics as viewed by the R&D staff; see Chan and Wu [11] for an extensive review of the QFD literature.

This paper builds on the HOQ framework by developing an HOS (Fig. 1) that translates the security needs of an enterprise into the relative importance of the components of its existing security program according to their relative importance in meeting these needs.

The general building sequence of the HOS comprises the following six major steps:

1. *Relevant Scenarios (WHATs)* – Identify and classify the attackers' intentions and the *relevant* (plausible) attacks to the organization (the walls). Specify scenarios for every place in the organization that may be attacked.
2. *Likelihood and severity of these scenarios* – Assign assessments observed from security surveys; include scenario possibilities and losses when a scenario occurs.

3. *System components (HOWs)* – Select a structured set of relevant system *components* (the ceiling), i.e. technologies, people, and procedures, which are capable of preventing the identified scenario.
4. *Interrelationship matrix* – Evaluate the reduction in the risk of each scenario as a result of using each security component (the house's main contents). An appropriate scale is applied, illustrated by symbols.
5. *Synergy/trade-off between the system components* (the roof) – For each scenario, identify which system component supports (or obstructs) another system component. These synergies can highlight innovation opportunities or bring to the fore areas that need reorganization.
6. *System priorities* – Calculate the system component priorities as one block and for every specific place that may be attacked (the floor).
7. *System effectiveness* – Estimate the overall effectiveness of the security of the analyzed system. This value could be used as a selection criterion when several security systems are introduced for the same set of scenarios.

2.1 Calculation of the system components priorities

The priority of the each system component is calculated as follows:

$$q_j = \sum_{i=1}^{I} p_i \cdot r_{ij} \cdot L_i \cdot \left(1 + \frac{\sum_{j' \neq j}^{J} \Delta_{jj'}^{(i)}}{J-1} \right) = \sum_{i=1}^{I} p_i \cdot \tilde{r}_{ij} \cdot L_i, \tag{1}$$

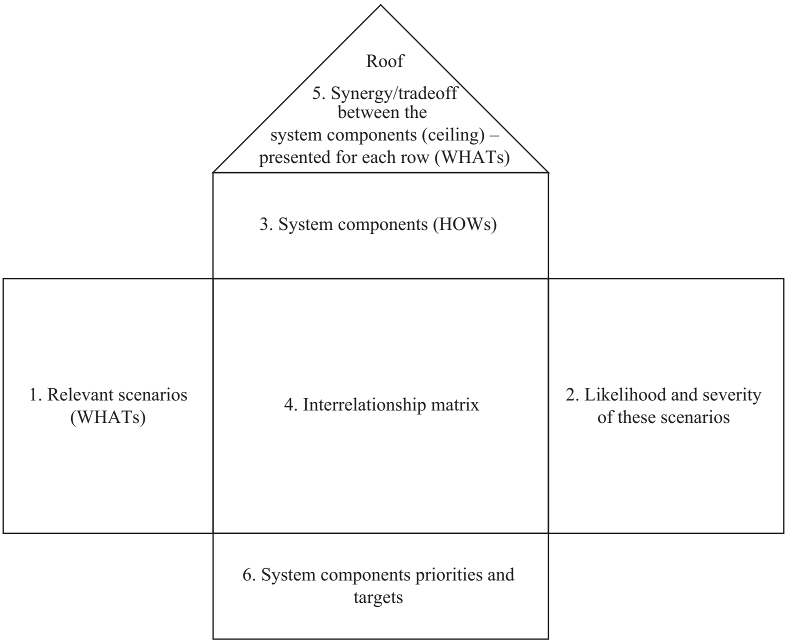
Roof
5. Synergy/tradeoff between the system components (ceiling) – presented for each row (WHATs)
3. System components (HOWs)
1. Relevant scenarios (WHATs)
4. Interrelationship matrix
2. Likelihood and severity of these scenarios
6. System components priorities and targets

Figure 1: House of security.

where:

I is the number of possible scenarios and J is the number of security components of the system under study.

p_i is the possibility that scenario i will occur.

q_i is the importance of security component j.

r_{ij} is the reduction in the risk/damage of each scenario i as a result of using each security component j.

L_i is the expected loss when scenario i occurs.

$\Delta_{jj'}^{(i)}$ is the synergy between security component j and security component j' ($j' \neq j$), given scenario i.

This formula takes into account the possibility that a scenario occurs, the reduction in the risk of each scenario as a result of using each security component, the loss when a scenario occurs, and the synergy between security components, given a specific scenario. The last part of this formula differentiates it strongly from the classic QFD formula. The classic QFD has one roof that presents correlations between the technical characteristics. Here we assume that correlations between the system components might change for each scenario, i.e. there are several roofs, corresponding to the number of rows in the HOS matrix.

To compare different security systems designed to prevent the same threats (the same p_i and L_i), the following measure of effectiveness is proposed:

$$Eff = \frac{\sum_{j=1}^{J}\sum_{i=1}^{I} p_i \cdot \tilde{r}_{ij} \cdot L_i}{\sum_{i=1}^{I} p_i \cdot L_i} = \frac{\sum_{j=1}^{J} q_j}{\sum_{i=1}^{I} p_i \cdot L_i}. \tag{2}$$

Here the denominator of (2) expresses the expected loss when no security system is involved (activated).

2.2 The analysis of variance method for selecting the components to be improved

ANOVA is a method for decomposing the total variability in a set of observations, as measured by the sum of the squares of these observations from their average, into component sums of the squares that are associated with specific, defined sources of variation. In a one-way ANOVA, there are two sources of variation: the sum of the squares of the differences between the group means and the grand mean – denoted as SSB – and the sum of the squares of the differences between group observations and the group mean – denoted as SSE. The mean square error (MSE) is an unbiased estimator of σ^2. The mean square between (MSB) groups estimates σ^2 plus a positive term that incorporates variations due to the systematic difference in the groups' means. The F-statistic is used to test for significant differences between the means of two or more groups (see, e.g. [12]).

Dror and Barad [13] utilized the MSE criterion as a quantitative tool for implementing the Pareto Principle. This principle was presented by Juran as a universal principle he referred to as the 'vital few and trivial many'. Dror [14] showed that the one-way ANOVA tools, i.e. MSE, MSB and the F-statistic, are equivalent when used for dividing a group of ordered items into two groups: the vital few and the trivial many. The ANOVA method is utilized here for selecting the vital security components to be improved.

The method suggested by Dror and Barad [13] is

1. Arrange the normalized required improvement levels of the k components in descending order, where q_1 represents the highest improvement level needed and q_k the lowest improvement level needed, $0 \leq q_j \leq 0$, $j = 1,\ldots k$.
2. While maintaining this order, divide the k components into two groups, A and B. Group A consists of the first m components, while group B comprises the remaining $k - m$ components. Assuming that each group includes at least one component, there are $k - 1$ possibilities for selecting an m value for dividing the items into two groups.
3. Calculate $MSE(m)$, $m = 1,\ldots k - 1$ using the following equation:

$$MSE(m) = \left\{ \sum_{j=1}^{m} \left(q_j - \overline{q}_A\right)^2 + \sum_{j=m+1}^{k} \left(q_j - \overline{q}_B\right)^2 \right\}, \tag{3}$$

where $\overline{q}_A$ and $\overline{q}_B$ are the average improvement levels in vital group A and in trivial group B, respectively.

4. Find,

$$MSE(m^*) = \underset{1 \leq m \leq k-1}{Min} \left[MSE(m)\right]. \tag{4}$$

3 EXAMPLE: CONSTRUCTING THE HOS FOR HOTEL TERRORIST ATTACK PROTECTION

3.1 The relevant scenarios *(WHATs)*

Hotels have often been the object of terrorist attacks. The most common kinds of such attacks are suicide bombers, car bombs, explosives, grenade assault and the taking of hostage(s). Potential attack locations: front of the hotel, entrance check point, parking area, lobby and anywhere inside the building. The left wall of the HOS (Table 1) includes 5 × 5–1 possible scenarios (the combination of 'a car bomb inside the building' is not feasible).

3.2 The likelihood and severity of the scenarios

In the second step of building the HOS (right wall), scores, based on security surveys, were assigned by experts who assessed the likelihood and severity of every scenario (Table 2). In order to emphasize the dramatic character of terrorist attacks, the geometrical and not arithmetical scale of scores was used according to:

- *Scenario likelihood*: unlikely/weak – 1, likely/medium – 3, very likely/strong – 9
- *Severity of damage to people or/and property*: light – 1, medium – 3, high – 9

3.3 The system components *(HOWs)*

The relevant hotel security system *hows* (components) include:

Technologies:

- Prevention devices: cameras (LPR, TV), video information analysis (VIA), entry control tools, boulders
- Alarm devices – detectors, distress/trouble buttons, siren

Table 1: List of relevant scenarios.

	Threat	Scenario location
1	SUICIDE BOMBER	Front of the hotel
2		Entrance check point
3		Parking area
4		Lobby
5		Inside the building
6	CAR BOMB	Front of the hotel
7		Entrance check point
8		Parking area
9		Lobby
10	EXPLOSIVES	Front of the hotel
11		Entrance check point
12		Parking area
13		Lobby
14		Inside the building
15	GRENADE ASSAULT	Front of the hotel
16		Entrance check point
17		Parking area
18		Lobby
19		Inside the building
20	TAKING OF HOSTAGE(S)	Front of the hotel
21		Entrance check point
22		Parking
23		Lobby
24		Inside the building

Human resources:

- Personnel: external, internal
- Police

Security system procedure & operating instructions
Arranged as shown below (Table 3), the components constitute the HOS ceiling.

3.4 The interrelationship matrix

This stage of constructing the HOS is very essential, but is also almost the most painstaking and laborious part of the process. 24 *what* (rows) and 12 *how* (columns) form 288 cross cells ($I = 24$, $J = 12$ and $IJ = 288$). Each cell contains the assessment of the extent to which the specific *how* might reduce the risk of occurrence or damage caused by a corresponding

Table 2: Likelihood and severity of the scenarios.

	Threat	Scenario		Likelihood	Severity
1	SUICIDE BOMBER	Front of the hotel	…	9	9
2		Entrance check point	…	9	9
3		Parking area	…	1	1
4		Lobby	…	9	9
5		Inside the building	…	3	9
6	CAR BOMB	Front of the hotel	…	9	9
7		Entrance check point	…		
8		Parking	…	1	1
9		Lobby	…	3	9
10	EXPLOSIVES	Front of the hotel	…	3	3
11		Entrance check point	…	1	1
12		Parking area	…	1	1
13		Lobby	…	9	9
14		Inside the building	…	9	9
15	GRENADE ASSAULT	Front of the hotel	…	3	3
16		Entrance check point	…	3	3
17		Parking area	…	1	1
18		Lobby	…	9	9
19		Inside the building	…	9	9
20	TAKING OF HOSTAGE(S)	Front of the hotel	…	1	1
21		Entrance check point	…	3	9
22		Parking area	…	1	9
23		Lobby	…	9	9
24		Inside the building	…	9	9

Table 3: List of system components arranged in three hierarchical levels.

Technologies								Human resources			Security system
Prevention devices					Alarm devices			Personnel		Police	Procedure
LPR cameras	TV cameras	VIA	Entry control	Boulders	Detectors	Panic buttons	Siren	External	Internal	Policemen	Operating instructions

scenario (*what*) measured, as is customary in QFD, on the basis of four degrees of interaction: high interaction (=9), medium interaction (=3), low interaction (=1) and no interaction (= blank, further considered as zero). This assessment is usually based on experts' knowledge and experience. Consensus decision making based on the Delphi method [15] was selected as the most appropriate for arriving at the final scores.

Table 4: Interrelationship matrix.

			LPR cameras	TV cameras	VIA	Entry control	Boulders	Detectors	Trouble buttons	Siren	External	Internal	Policemen	Operating instructions
1	**SUICIDE BOMBER**	**frontage of the hotel**	*1*	*9*	*9*	*1*	*1*	*1*	*3*	*1*	*9*	*1*	*9*	*9*
2		**entrance check point**	*1*	*9*	*3*	*9*	*1*	*9*	*3*	*1*	*9*	*1*	*9*	*9*
3		**parking**	*1*	*9*	*9*	*1*	*1*	*1*	*3*	*1*	*1*	*9*	*9*	*9*
4		**lobby**	*1*	*9*	*3*	*9*	*1*	*9*	*3*	*1*	*1*	*9*	*1*	*9*
5		**inside the building**	*1*	*9*	*9*	*1*	*1*	*1*	*3*	*1*	*1*	*9*	*1*	*9*

The journal's page size limitations do not allow us to reproduce the whole matrix with necessary resolution, so we present here only a single fragment (Table 4), giving, however, an overall impression of the manner of interrelationship matrix fulfilling.

3.5 Synergy/trade-off between the system components (the roof)

The HOS roof construction here differs somewhat from the usual QFD technique. In the context of this paper *synergy/trade-off* means that two *how*s functioning together produce a combined result not independently obtainable. Positive or negative synergy can exist. The latter often appears as a result of trade-off between two *how*s. Positive synergy occurs if interactions between two *how*s produce a joint effect, which is greater than the sum of the parts acting alone. In contrast to standard QFD, the presence of positive/negative synergy must be analyzed for each scenario separately. We consider the synergy effects in the following manner: For every cell (*i,j*) the existing score is multiplied by synergy factor $s_{ij} = 1 + \frac{\sum_{j'\neq j}^{J}\left(\Delta_{jj'}^{(i)}\right)}{J-1}$, where $\Delta_{jj'}^{(i)} = +1$, for positive synergy, zero or –1 for the absence of or negative synergy; i.e. $0 \leq s_{ij} \leq 2$. This approach strengthens the *how*s' components that may significantly prevent or reduce the specific threat scenario occurrence/damage. Note that we have to analyze 0.5*J*(*J*-1) possible interactions for each *i* roof (scenario). For example, recalculated in such a manner, the Table 4 scores assigned to the first scenario (front) of a suicide bomber threat produces the results shown in Table 5.

The scores were increased since the experts' assigned positive synergy between:

- cameras TV and VIA,
- policemen and operating instructions
- external personnel and operating instructions.

In the same manner all r_{ij} are recalculated to $\tilde{r}_{ij}$.

Table 5: Recalculated scores of the first row of Table 4.

		LPR cameras	TV cameras	VIA	Entry control	Boulders	Detectors	Trouble buttons	Siren	External	Internal	Policemen	Operating instructions
SUICIDE BOMBER	**frontage of the hotel**	*1*	*9.8*	*9.8*	*1*	*1*	*1*	*3*	*1*	*9.8*	*1*	*9.8*	*10.6*

Table 6: Security components importance scores.

	LPR cameras	TV cameras	VIA	Entry control	Boulders	Detectors	Trouble buttons	Siren	External	Internal	Policemen	Operating instructions
q_i	**1984**	**9762**	**5876**	**5931**	**1595**	**4562**	**2931**	**814**	**3690**	**6787**	**4187**	**9785**

3.6 System components priorities

After assigning priorities to the *how*s in the previous stage, q_j can be calculated according to (1) by multiplying three score columns: *likelihood, severity* and the corresponding *j*-th column of the interrelationship matrix. Empty cells are considered as zeros. A simple Excel© function, such as SUMPRODUCT (array1, array2, array3) can be used for this purpose, resulting – in our case – in the importance scores for the security components presented in Table 6.

The ANOVA-based MSE method described above, when applied to these data, emphasize the following five (from twelve) components as *dominant* for the hotel security system: Operating procedures – 9785; TV cameras – 9762; internal personnel – 6787; entry control – 5931; visual information analysis – 5876.

The dominant components destined to protect a certain place – parking, for example – can also be partially analyzed. In this case as shown below in Table 7, we utilize only the relevant part of the common matrix obtained by deleting unnecessary scenarios.

Now the *dominant components* preventing parking area threats are operating procedures and internal personnel.

3.7 Overall effectiveness of the security system

For this specific example, (2) equals 62. This value could be used as a selection criterion when several security systems are introduced for the same set of scenarios.

4 CONCLUSIONS

QFD, a product-oriented quality technique supported by ANOVA, a statistical technique, was applied in an innovative way to reveal the requirements of the security system to be adopted by an individual organization or the suitability of a security system already in place.

Table 7: Interrelationship matrix for parking areas.

			LPR cameras	TV cameras	VIA	Entry control	Boulders	Detectors	Trouble buttons	Siren	External	Internal	Policemen	Operating instructions	Feasibility	Severity
1	**suicide bomber**	**parking**	*1*	*9.8*	*11.5*	*1*	*1*	*1*	*3*	*1*	*1*	*9.8*	*9.8*	*10.6*	**1**	**1**
2	**car bomb**	**parking**	*1.1*	*9.8*	*10.6*	*9*	*3*	*9*	*9*	*1*	*1*	*9.8*	*9.8*	*10.6*	**1**	**1**
3	**explosives**	**parking**	*1*	*9*	*9*	*1*	*1*	*9.8*	*3*	*1*	*1.1*	*1.1*	*9*	*10.6*	**1**	**1**
4	**Firing grenades**	**parking**	*1*	*3.3*	*9.8*	*9*	*1*	*1*	*9*	*1*	*3,3*	*1*	*3*	*9.8*	**1**	**1**
5	**hostage**	**parking**	*1*	*3.3*	*1*	*3*	*1*	*1*		*1*	*1*	*9.8*	*3*	*11.5*	**1**	**9**
q_i			**13**	**62**	**50**	**47**	**15**	**30**	**24**	**13**	**12**	**110**	**59**	**145**		

The method provides useful information and understanding regarding the relative importance the management of an enterprise should attribute to its security system components as dictated by attacks scenarios as well as by its internal capabilities. QFD provides a mechanism for leveraging the security system of an individual organization. The HOS highlights potential attackers' intentions and the relevant attacks to the system and translates them into the relative importance of the security system components.

The HOS method is different from the classic QFD. In the classic QFD, a single roof presents correlations between the technical characteristics. In HOS we assume that correlations between the system components might be changed for each scenario, i.e. several roofs, corresponding to the number of rows in the HOS matrix. Hence, the calculation of the relative importance of the system components takes the synergy/trade-off between security components given a specific scenario into account. For comparing different security systems designed to prevent the same threats, a new effectiveness measure is proposed. ANOVA supports pinpointing of the vital security system components. It divides a group of items (here a set of security system components) into two groups: vital few and trivial many.

A QFD matrix is typically carried out by teams of multidisciplinary representatives from all stages of product development and manufacturing. For building the HOS, a cross functional team is established. It might include security experts, managers, technical engineers and maintenance technicians. Among its assignments, the team would be tasked with organizing the process of extracting input information for the HOS matrix.

This paper describes the implementation of the above methodology for hotel protection from a terrorist attack. The QFD team identifies the most common kinds of attacks: suicide bombers, car bomb, explosives, grenade assault and taking of hostage(s), and potential locations of the attack in or around the hotel: front of the hotel, entrance check point, parking area, lobby, and anywhere inside the building. The HOS pointed out five vital components of the security system: operating procedures, TV cameras, internal personnel, entry control, and visual information analysis. A partial analysis to identify the most important component for protecting a certain area of the hotel (parking area) showed that the number of the vital components decreases and the dominant components for preventing parking area threats are operating procedures and internal personnel.

Our method (the HOS supported by the ANOVA method) reveals the most suitable security system structure to be adopted by an individual organization. In the case study, vital five security components were found to be the best tools for reducing the risk of attack scenarios.

The method applied in this work effectively supports the selection of vital security system components. It emphasizes adopting a systemic approach for selecting the vital security system components in response to attack scenarios.

ACKNOWLEDGMENT

We would like to thank Mr. Uri Aharoni for his professional assistance in giving us a comprehensive view on the entire ***security*** issue and for his instrumental help during the experts' evaluation.

REFERENCES

[1] Stewart, M.G. & Mueller, J., Cost-benefit analysis of advanced imaging technology full body scanners for airline passenger security screening. *Journal of Homeland Security and Emergency Management*, **8**(1), 2011. doi: http://dx.doi.org/10.2202/1547-7355.1837

[2] Majeske, K.D. & Lauer, T.W., Optimizing airline passenger prescreening systems with Bayesian decision models. *Computers & Operations Research*, **39(8)**, pp. 1827–1836, 2012. doi: http://dx.doi.org/10.1016/j.cor.2011.04.008

[3] Xiaofeng N.Risk-based grouping for checked baggage screening systems. *Reliability Engineering & System Safety*, **96(11)**, pp. 1499–1506, 2012.

[4] Lee, A.J. & Jacobson, S.H., The impact of aviation checkpoint queues on optimizing security screening effectiveness. *Reliability Engineering & System Safety*, **96(8)**, pp. 900–911, 2011. doi: http://dx.doi.org/10.1016/j.ress.2011.03.011

[5] Hassoun, M., Rabinowitz, G. & Reshef, N., Security agent allocation to partially observable heterogeneous frontier segments. *IIE Transactions*, **43(8)**, pp. 566–574, 2011. doi: http://dx.doi.org/10.1080/0740817X.2010.532852

[6] Niyazi O.B., A Stackelberg game model for resource allocation in cargo container security. *Annals of Operations Research*, **187**, pp. 5–22, 2011. doi: http://dx.doi.org/10.1007/s10479-010-0793-z

[7] Keeney, R.L. & Von Winterfeldt, D., A value model for evaluating homeland security decisions. *Risk Analysis*, **31(9)**, pp. 1470–1487, 2011. doi: http://dx.doi.org/10.1111/j.1539-6924.2011.01597.x

[8] ISO 28000, Specification for security management systems for the supply chain, 2007.

[9] Bashkansky, E., Dror, S., Ravid, R. & Grabov, P., Effectiveness of a product quality classifier. *Quality Engineering*, **19(3)**, pp. 235–244, 2007. doi: http://dx.doi.org/10.1080/08982110701334577

[10] Akao, Y. & Mazur, G.H., The leading edge in QFD: past, present and future. *International Journal of Quality & Reliability Management*, **20(1)**, pp. 20–35, 2003. doi: http://dx.doi.org/10.1108/02656710310453791

[11] Chan, L.K. & Wu, M.L., Quality function deployment: a literature review. *European Journal of Operational Research*, **143(3)**, pp. 463–497, 2002. doi: http://dx.doi.org/10.1016/S0377-2217(02)00178-9

[12] Montgomery, D., *Introduction to Statistical Quality Control*, 5th edn., John Wiley & Sons: New York, 2004.

[13] Dror, S. & Barad, M., House of Strategy (HOS) – From strategic objectives to competitive priorities. *International Journal of Production Research*, **44(18–19)**, pp. 3879–3895, 2006. doi: http://dx.doi.org/10.1080/00207540600575779

[14] Dror, S., A methodology for realignment of quality cost elements. *Journal of Modelling in Management*, **5(2)**, pp. 142–157, 2010. doi: http://dx.doi.org/10.1108/17465661011060998

[15] Linstone, H.A. & Turoff, M., The *Delphi Method: Techniques and Applications*, Addison-Wesley: Boston, MA, 1975.