International Journal of Safety and Security Engineering
Vol. 10, No. 6, December, 2020, pp. 727-732
Journal homepage: http://iieta.org/journals/ijsse

Application of Quality Function Deployment to the Management of Information Physical Security

Mara Lombardi[1], Fabio Garzia[1,2,3*], Mario Fargnoli[1], Anselmo Pellizzi[1], Soodamani Ramalingam[4]

[1] Safety & Security Engineering Group – DICMA, SAPIENZA – University of Rome, Rome 00184, Italy
[2] Wessex Institute of Technology, Southampton SO40 7AA, UK
[3] European Academy of Sciences and Arts, Salzburg A-5020, Austria
[4] School of Engineering and Computer Sciences, University of Hertfordshire, Hatfield AL10 9AB, UK

Corresponding Author Email: fabio.garzia@uniroma1.it

https://doi.org/10.18280/ijsse.100601

Received: 30 June 2019
Accepted: 17 July 2019

Keywords:
data security, data protection, data physical security, quality function deployment, house of security

ABSTRACT

Information physical security (IPS) refers to the prevention from intended attacks against all material devices and to the protection against deliberate attacks by supporting and managing related data/information. Information in today's world represents an important asset to be protected and for this reason it is necessary to adopt a suitable method for risk and security management. The Quality Function Deployment (QFD) method was originally developed as a tool capable of ensuring a valuable help in the design of products and services, guaranteeing customer satisfaction and value creation. The core of the method is the set of matrices called the 'House of Quality' (HoQ), which relates the Customer Requirements (CRs) with Engineering Characteristics (ECs): in other words, the HoQ is a way of translating customer requirements into design parameters. Numerous studies have demonstrated its use in a wide range of sectors. In particular, its application in the security engineering context has been investigated by means of the House of Security (HoS). Its objective is represented by the classification of the components of a security system in response to different scenarios of voluntary attacks. Based on this, the aim of the study consists in extending such an approach to information physical security. More in detail, the purpose of this paper is the development of a systematic model, based on the HoS and applicable to information physical security, that allows the definition and raking of the vital components of an information physical security system (IPSS). In this way, it is possible to perform a proper cost/benefit analysis, considering a general physical layout of a certain organization so that the results can be wide-ranging and applicable in different contexts.

1. INTRODUCTION

Information physical security takes care of prevention from intended attacks against all material devices and supports of data/information, as well as of protection against those voluntary attacks [1]. Public and private organizations generally deal with a large amount of confidential information about their employees, customers, products, research, financial and economic aspects, etc. If such information is stolen or lost, it could cause irreparable damages to the organizations themselves from different points of views.

Further, the recent introduction of the EU Regulation n.679/2016, known as General Data Protection Regulation (GDPR) [2], increases the need of personal data protection and contemplates heavy penalties when those data are not properly protected. In fact, with this regulation, the European Commission intends to strengthen and harmonize the protection of personal data of citizens of the European Union (EU) and of residents in the European Union, both within and outside the borders of the European Union.

It is therefore clear that information in today's world represents an important asset to be protected and for this reason it is necessary to adopt a suitable method for risk and security management. From this point of view, the technical standard ISO/IEC 207001 [3] can be a proper reference since it represents the most used international standard in the field of security information management, considering both physical and logical aspects of information security.

In order to cope with new threats and new attacks, it is essential, for any kind of organization, to develop a strategy to prioritize investments necessary to protect information in a proper way. The main goal of information security is represented by confidentiality, integrity, and availability and, from the physical security point of view, it is important to use technology, procedures, and human resources to realize a proper integrated multidisciplinary security management system that could efficiently reach the desired targets [4-7].

A vital problem in the design of components for information security is represented by the optimal use of financial resources, that are normally quite limited. For this reason, it is important to find a suitable method which allows identifying the most essential components (CCTV cameras, access control, intrusion detection, fire detection, fire extinguishing, electrical backup, air conditioning, procedures, security personnel, etc.) from the cost/benefit point of view and allows to realize a suitable strategic planning process for any organization.

The Quality Function Deployment (QFD) was born in Japan in the second half of the 60s to create a quality improvement tool, capable of ensuring a valuable help in the design of products and services [8]. The core of the method is the set of matrices called the “House of Quality” (HoQ), which relates the Customer Requirements (CRs) (i.e. the so-called “whats”) with Engineering Characteristics (ECs) (i.e. the so-called “hows”) [8]. In other words, the House of Quality (HoQ), whose innermost part is represented by the relationship matrix, is a way of translating customer needs and expectations into design parameters, ranking them based on a cause-effect mechanism [9]. Numerous studies have demonstrated its fruitful use in a vast range of different sectors [10]. In particular, its application in the security engineering context has been investigated by means of the House of Security (HoS) [11, 12], which allows the definition and ranking of the components of a security system in response to different scenarios of voluntary attacks. Following such an approach, the purpose of this paper is extending the knowledge of QFD in the security field extending its application to information physical security.

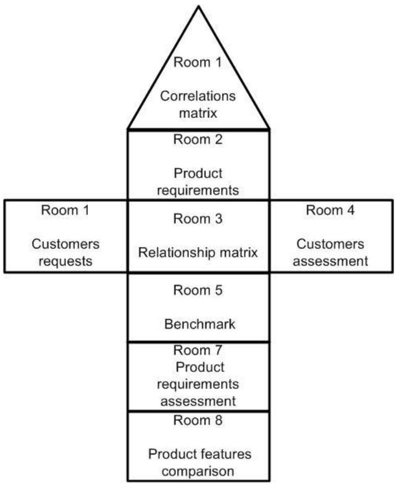
In fact, the goal of the study consists in the development of a systematic procedure, based on the HoS, for the IPS management, allowing the definition and prioritization of the vital components of an information physical security system. In this way, it is possible to perform a proper cost/benefit analysis, considering a general physical layout of a certain organization so that the results can be wide-ranging and applicable in most of contexts.

The achieved results have demonstrated the ability of the proposed approach in maximizing the benefits of the HoS when dealing with the integration of normative requirements with security needs, providing a valuable basis for further developments and extensions.

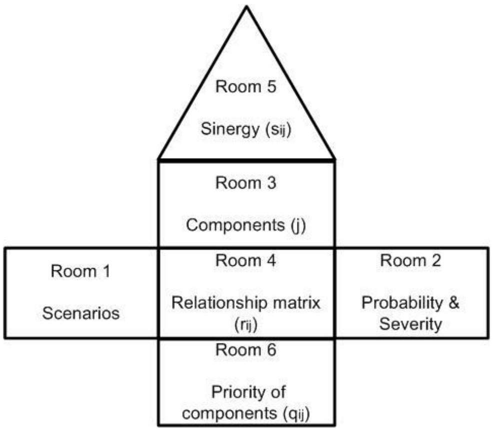
2. QUALITY FUNCTION DEPLOYMENT AND HOUSE OF SECURITY

The Quality Function Deployment and the House of Security tools have been illustrated briefly in the previous section, due to the limited space available. A graphical comparison between the House of Quality and the House of Security is shown in Figure 1.

The objective of the HoQ is to design a product or a service in order to satisfy the needs of the customers. The roof of the HoQ consists in the correlation matrix, which is aimed at evaluating the mutual interactions between the technical characteristics [8].



(a) House of Quality (HoQ)

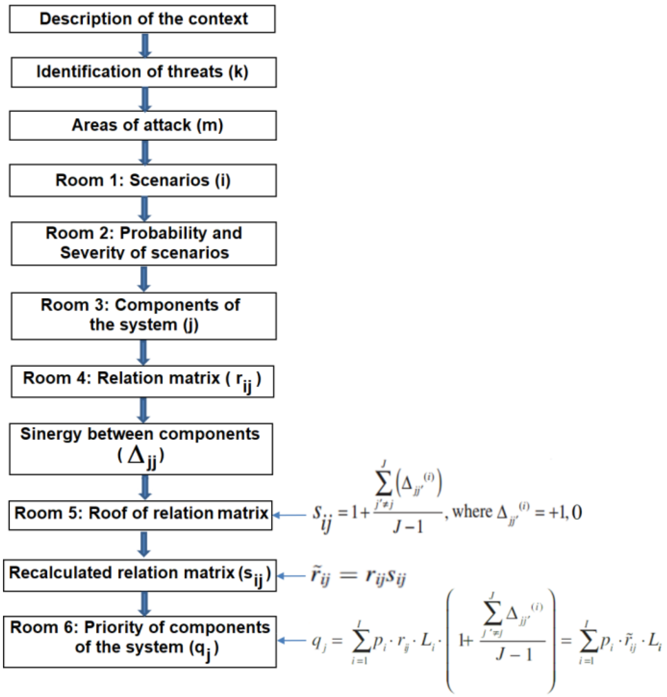


(b) House of Security (HoS)

Figure 1. Schemes of HoQ and HoS

Similarly, the objective of the HoS is to highlight the effects of potential threats and the related attacks in the considered context [11, 12]. Hence, shifting such an approach to the analysis of a company’s IPSS in order to bring to light the components of the system and their relevance depending on different scenarios of attacks.

3. CASE STUDY


Description of the context
Identification of threats (k)
Areas of attack (m)
Room 1: Scenarios (i)
Room 2: Probability and Severity of scenarios
Room 3: Components of the system (j)
Room 4: Relation matrix (r_ij)
Sinergy between components (Δ_jj)
Room 5: Roof of relation matrix
Recalculated relation matrix (s_ij)
Room 6: Priority of components of the system (q_j)

$$s_{ij} = 1 + \frac{\sum_{j' \neq j}^{J} \left(\Delta_{jj'}{}^{(i)} \right)}{J-1}, \text{ where } \Delta_{jj'}{}^{(i)} = +1, 0$$

$$\tilde{r}_{ij} = r_{ij} s_{ij}$$

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

Figure 2. Flowchart of the method applied to the considered case study (adapted from [11])

The model which is used is therefore based on a modified version of the QFD, represented by HoS, where the objective is not to satisfy the customer's requirements, but to find the vital components of an information physical security system (IPSS) of the case study, represented by a site for tertiary activities, to face the threats that could compromise the data and information. The physical information security is considered from the regulatory point of view, referring to both the General Data Protection Regulation (EU Regulation n. 2016/679) and to the ISO / IEC 27001 standard. Then, the set of means and technologies used in the information security sector aimed at protecting data from voluntary, accidental, and environmental threats in terms of availability, confidentiality and integrity are defined and considered. Accordingly, following the procedure proposed by Dror et al. [11], the flowchart of the method applied to the considered case study is shown in Figure 2.

The meaning of equations shown in Figure 2 and the related terms are properly illustrated in subsection 3.10.

3.1 Description of the context and layout of the considered case study

To apply the proposed model, a site for tertiary activities was chosen as a case study. The first step is to have an in-depth knowledge of the context and of the protection of information physical security system (IPSS). Then, to protect the data and information it is necessary to identify the components and the threats regarding the IPSS. The layout of the considered general case study is shown in Figure 3.

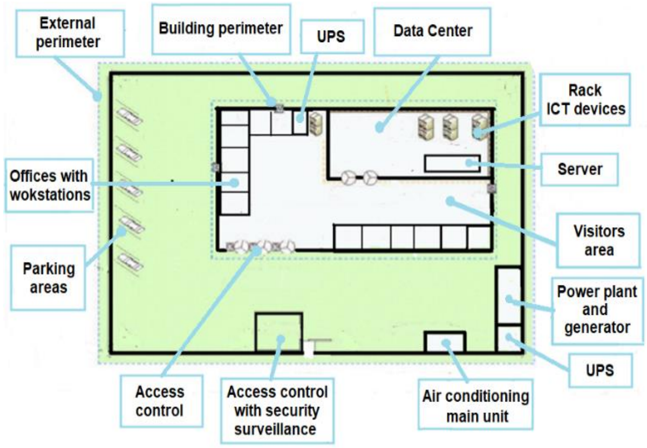


Figure 3. Layout of the considered case study

3.2 Areas exposed to attacks

Threats can act in different parts of the considered site and can cause data loss or violation.

For simplicity, the areas are grouped into 6 different sets:

1) Site or external perimeter (m=1).
2) Building perimeter (m=2).
3) Visitors area (m=3).
4) Offices and workstations (m=4).
5) Data Center (m=5).
6) Racks ICT devices and equipment (m=6).

3.3 Threats identification

The difficulty of this step lies in the not complete and immediate availability of reference data related to all the possible attacks that an organization might suffer. Companies that have been victims of an attack against the security of their IPSS are reluctant to divulge information relating to the way the attack took place, so as not to incentivize attackers to repeat these actions.

In the present analysis, the ISO 27001 standard is used as reference, dividing threats into 5 major categories and then for each category the most common are properly identified and shown in Table 1.

Table 1. Considered threats of the case study

Type of threat	Description
Passive attacks (k=1)	Eavesdropping: communications (data, information, voice, etc.)
Active attacks (k=2)	Theft: documents, devices, etc.; damages: networks, devices, etc.; illegal access: server, strongbox, etc.
Human errors (k=3)	File deletion, installation of incompatible components, errors of procedures, hardware & software maintenance errors, etc.
Malfunctions (k=4)	Hard disk: PC, server, etc.; network: server, devices, etc.; peripherals: backup units, etc.; air conditioning; power transformers; generator; UPS, etc.
Natural events (k=5)	Fire: burning; water: flooding, excessive humidity, etc.; noise: electromagnetic disturbance, etc.; excessive voltage variations and blackout: lighting, corrosion, freezing, etc.

3.4 Relevant scenarios

The relevant scenarios are generated by the combination of the areas exposed to the attacks with the identified threats. Due to the large variety and complexity of the threats, they have been synthetically grouped into the 5 macro-categories of Tab 1. Since the identified areas exposed to attacks are 6, the total number of scenarios reported in room 1 of HoS are 30.

3.5 Probability and severity of scenarios

The probability and severity of scenarios have been assigned according to what reported in Tables 2, 3 and inserted in room 2 of HoS.

3.6 The components of Information Physical Security System

Once the characteristics of the information physical security system (IPSS) have been defined and threats and possible scenarios have been identified, it is possible to go ahead to room 3 of HoS. In this room the components of the Information Physical Security System (IPSS), whose objective is to minimize or eliminate the probability that any attacks can be carried out, are identified. The IPSS components can be grouped into three broad categories: physical and logical technologies; human resources; procedures. The components were chosen by comparing the ISO27001 standard and current research and report results. Due to the excessive number of components to be analysed, the components are grouped into 23 sets basing on the function they perform to reduce threats, as shown in Table 4.

3.7 Relationship matrix

This HoS construction phase of room 4 is essential, but it also represents one of the most difficult parts of the process. This matrix is composed by 30 threat scenarios (i-rows), 23 components (j-columns) and 690-cell modules given by the multiplication of the 30 scenarios (i) for the 23 components (j). Each cell contains an assessment of the risk level reduction generated by the considered component in the corresponding scenario.

Any value is measured basing on the four degrees of interaction, as in the QFD way, represented by:

1) No interaction (= empty).

2) Low interaction (= 1).
3) Average interaction (= 3).
4) High interaction (= 9).

This evaluation is usually performed using proper reference data [1, 12, 13].

Table 2. Probability levels

Probability levels	Description
Unlikely	It is applicable to at least one of the following: - The threat can occur less frequently than reported by the most accredited researches and reports. - In the event of a deliberate attack, the data is unattractive, and the image of the considered organization is not compromised and therefore the attempts to attack or have not started or are conducted by poorly skilled from a technical point of view attackers, with scarce resources available. - In case of accidental error, the context is not very complex and therefore it is difficult to make mistakes. - In the case of natural events, current researches and reports show that the threat can occur very rarely.
Probable	It is applicable to at least one of the following: - The threat can occur as reported by the most accredited researches. - In the event of a deliberate attack, the data is not very attractive and the image of the considered organization is not compromised and therefore can be conducted by attackers who are not particularly motivated, on average prepared from a technical point of view and with scarce resources available; or alternatively, researches and reports confirm that attempts of attack are still rare. - In the event of a non-deliberate attack, the scope is on average complex and therefore errors can be made. - In the case of natural events, current research and reports show that the threat can occur in the average of the cases studied.
Very probable	It is applicable to at least one of the following: - The threat can occur more frequently than reported by the most accredited researches. - In the event of a deliberate attack, the data is attractive, or the image of the considered organization is compromised, and therefore can be conducted by highly motivated, technically prepared and with considerable resources available attackers; or alternatively, researches and reports confirm that attempts of attack are still carried very frequently. - In the event of a non-deliberate attack, the context is highly complex (for example due to the multiplicity of sites, types of information systems, internal and / or external users) and therefore it is easy to make mistakes. - In the case of natural events, current researches and report show that the threat almost certainly occurs.

Table 3. Severity levels

Severity		Effects on:	
	Confidentiality	Integrity	Availability
Low	The lack of confidentiality has slight impacts, which create small difficulties, costs, fear, misunderstanding, stress.	The lack of integrity has minor impacts (e.g. discomfort and time required to correct information)	The lack of availability has minor impacts (e.g. discomfort and time required to restore information). The unavailability of data beyond the contractually established deadlines does not imply fines or relevant penalties.
Medium	The lack of confidentiality has a high impact that can be overcome with difficulty. It has high impact on the organization and the related compliance with current legislation or on the image of the organization itself.	The lack of data integrity has high impact on operating activities or on compliance with current legislation. Lack of integrity has a high impact on the working, social or personal life of those concerned.	The unavailability of data beyond the contractually established deadlines entails fines or relevant penalties. Lack of availability has a high impact on the working, social or personal life of those concerned.
High	The lack of confidentiality has non-reversible impacts on the data of the interested parties and high impact on the organization and the related compliance with current legislation or on the image of the organization itself.	The lack of integrity of the information has high impacts on the organization and the related compliance with current legislation such as to compromise the sustainability of the organization itself.	The unavailability of data beyond the contractually established deadlines implies fines or penalties that endanger economic and image sustainability or have an impact on the safety and security of individuals. Lack of availability has non-reversible impacts on the life of the interested persons.

3.8 Sinergy between IPSS components

The construction of the roof of the HOS is the part that distinguishes it from the correlation matrix of the HoQ. Unlike the conventional QFD, the presence of positive or zero synergy values must be analysed for each scenario. In the analysed case study, 30 different roofs were developed, one for each scenario. Accordingly, for each scenario and its roof, an analysis of how the IPSS components interact to produce an independent combined result was carried out. The synergy values are assigned not considering negative correlations: i.e. only the values Δj=1 (positive correlation) and Δj=0 (null correlation) were taken into account [11, 12].

A joint action of two IPSS components can prevent or reduce the specific threat of the scenario or reduce the damage. In the considered case study, 30 tables were developed in order to consider all possible scenarios. Values (0,1) must be assigned using proper reference data [1, 13-19].

3.9 Roof of the relationship matrix

In room 5 of the HoS, synergistic effects are considered adding to the value 1 of the cell (i, j) the value of the sum of the Δj scenarios (30) divided by j-1 [11], using the formula indicated in Figure 2.

Table 4. Considered components of Information Physical Security Systems (IPSS)

Categories	Components		Description
Physical and logical technologies	1	Video surveillance	Cameras
	2	Access control	Authentication (3 factors), authorization, accounting
	3	Safety detection	Flooding, fire, temperature, humidity sensors
	4	Security detection	Intrusion detection sensors
	5	Monitoring	Performance of components and maintenance
	6	Security alarms	Intrusion
	7	Safety alarms	Flooding, fire, etc.
	8	Interconnections	Network and power wires
	9	Lightning	Ordinary and emergency
	10	Shielding	Shields for wires, building and rooms against electromagnetic interferences
	11	Eavesdropping's checks	Instruments for Technical Surveillance Countermeasures (TSCM)
	12	UPS	UPS (Uninterruptable Power Supply)
	13	Physical layout	Reinforced masonry, armored glass, security locks, raised floor, etc.
	14	Electrical generators	Electrical generators
	15	Fire extinguishers	Sprinkler, gas extinguisher, motor pumps, etc.
	16	Air conditioning	Heating, cooling, fanning
	17	Logical intrusion countermeasures	Firewall, Intrusion Detection System (IDS), Proxy server, VPN, antiviruses, etc.
	18	Cryptography	Data on internal physical supports, internal data communication, external data communication
	19	Physical/cloud backup	Backup on internal physical supports, backup on remote physical supports, cloud
Human resources	20	Internal personnel	Employees
	21	External personnel	Housekeeping staff, maintenance staff, external companies, visitors, customers.
	22	Security personnel	Physical checks and security activities such as: TV monitor, access control, patrolling, etc.
Procedures	23	Procedures	Accountability, control, registration, authorizations, key assignments, password assignments, etc.

3.10 Recalculated relationship matrix

In this phase the relationship matrix is recalculated with the results obtained from the roof of the Sij correlation matrix, using the formula indicated in Figure 2.

3.11 Priority of Information Physical Security System components

In room 6 of HoS, the priorities of Information Physical Security System (IPSS) components are calculated using the formula indicated in Figure 2 [11] where:

- q_j is the importance of the IPSS component j.
- i is the number of possible scenarios (30 in the considered case study).
- j is the number IPSS components being studied (23).
- p_i is the probability that the scenario i will occur.
- r_{ij} is the risk / harm reduction of each scenario i because of the use of IPSS component j.
- L_i is the expected loss (severity) when scenario i occurs.
- $\Delta_{ij}{}^{(i)}$ is the synergy between IPSS component j and IPSS component j '(j' ≠ j) for the considered scenario i.

3.12 Results

The obtained results are shown in Figure 4 where the IPSS components are ordered from the most vital to the least vital.

From Figure 4 it is possible to draw the following conclusions for the considered case study:

1) the most important IPSS components are represented by the human/organizational component (procedures: 7.84%, internal personnel: 7.63%, security personnel: 4.42%).

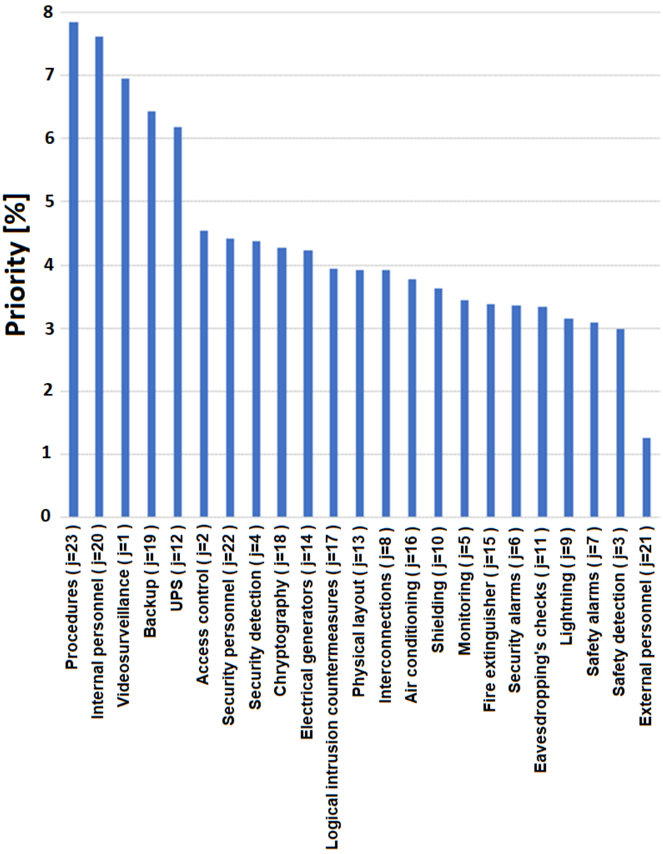


Figure 4. Priority of Information Physical Security Systems components

2) video surveillance (6.95%) represents an essential IPSS component for both safety and security.

3) the devices aimed at guaranteeing business continuity and disaster recovery represent IPSS vital components too (backup: 6.42%, UPS: 6.19%).

4) the IPSS components for managing authentication, authorizations and accounting are also essential for the desired goal (access control: 4.54%, encryption: 4.26%, logical intrusion detection measures: 3.93%).

5) the IPSS components related to energy supply and conditioning are significant too for the desired objectives (electrical generator 4.24%, air conditioning 3.76%).

4. CONCLUSIONS

A systematic procedure, based on the HoS and applicable to information physical security, that allows to classify the vital components of an information physical security system, according to a priority order, has been developed and studied, applying it to a case study represented by a typical site of tertiary activities. It represents a general approach that can be applied to different contexts, allowing to perform a proper and useful cost/benefit analysis. The obtained results could represent the basis for further QFD analyses in order to obtain more detailed information that allow to optimize the information physical security system from the cost/benefit point of view.

REFERENCES

[1] Garzia, F. (2013). Handbook of Communication Security. WIT Press.

[2] Regulation, E.G.D.P. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation) 2016. OJ L, 119(1).

[3] Schweizerische, S.N.V. (2013). Information technology-Security techniques-Information security management systems-Requirements. ISO/IEC International Standards Organization.

[4] Garzia, F. (2016). An integrated multidisciplinary model for security management and related supporting integrated technological system. 2016 IEEE International Carnahan Conference on Security Technology (ICCST), Orlando, FL, pp. 1-8. http://dx.doi.org/10.1109/CCST.2016.7815690

[5] Garzia, F., Lombardi, M. (2018). Safety and security management through an integrated multidisciplinary model and related integrated technological framework. WIT Transactions on The Built Environment, 174: 285-296. http://dx.doi.org/10.2495/SAFE170261

[6] Borghini, F, Garzia, F., Borghini, G, Borghini, A. (2016). The Psychology of Security, Emergency and Risk. WIT Press.

[7] Garzia, F., Lombardi, M., Fargnoli, M., Ramalingam, S. (2018). PSA-LOPA - A novel method for physical security risk analysis based on LOPA - Layers of Protection Analysis. 2018 International Carnahan Conference on Security Technology (ICCST), Montreal, QC, pp. 1-5. http://dx.doi.org/10.1109/CCST.2018.8585593

[8] Akao, Y. (1990). Quality Function Deployment: Integrating Customer Requirements into Product Design. Productivity Press - Cambridge.

[9] Fargnoli, M., Lombardi, M., Haber, N., Puri, D. (2018). The impact of human error in the use of agricultural tractors: A case study research in vineyard cultivation in Italy. Agriculture, 8(6): 82. http://dx.doi.org/10.3390/agriculture8060082

[10] Fargnoli, M., Sakao, T. (2017). Uncovering differences and similarities among quality function deployment-based methods in design for X: Benchmarking in different domains. Quality Engineering, 29(4): 690-712. http://dx.doi.org/10.1080/08982112.2016.1253849

[11] Dror, S., Bashkansky, E., Ravid, R. (2012). House of security: A structured system design & analysis approach. International Journal of Safety and Security Engineering, 2(4): 317-329. http://dx.doi.org/10.2495/SAFE-V2-N4-317-329

[12] Kuselman, I., Kardash, E, Bashhkans, E., Pennecchi, F. (2013). House-of-security approach to measurement in analytical chemistry: Quantification of human error using expert judgments. Accreditation and Quality Assurance, 18(6): 459-467. http://dx.doi.org/10.1007/s00769-013-1020-9

[13] ENISA - European Union Agency for Network and Information Security (2017). Handbook on Security of Personal Data Protection.

[14] ENISA - European Union Agency for Network and Information Security (2017). Guidelines for SMEs on the security of personal data processing.

[15] ENISA - European Union Agency for Network and Information Security (2015). Privacy and data protection by design.

[16] ENISA - European Union Agency for Network and Information Security (2013). Securing personal data in the context of data retention.

[17] Norman, T.L. (2015). Risk Analysis and Security Countermeasure Selection. CRC Press.

[18] Freund, J., Jones, J. (2014). Measuring and Managing Information Risk: A FAIR Approach. Butterworth-Heinemann.

[19] Hubbard, D.W., Seiersen, R. (2016). How to Measure Anything in Cybersecurity Risk. Hoboken: Wiley. https://doi.org/10.1002/9781119162315