NOVEL RISK ASSESSMENT METHODOLOGY FOR CULTURAL HERITAGE SITES

FABIO GARZIA[1,2,3]
[1]Safety & Security Engineering Group – DICMA, SAPIENZA – University of Rome, Italy
[2]Wessex Institute of Technology, UK
[3]European Academy of Sciences and Arts, Austria

ABSTRACT

Cultural heritage sites are places subjected to certain risks embodied, for example, by theft, vandalism, damaging, terrorism which could harm equally persons and cultural heritage. For this reason, it is necessary to activate suitable countermeasures to avoid the above risks and to defend against them by means of intrusion detection, access control, video surveillance, communication systems, security personnel and procedures suitably combined to achieve an integrated system or solution. In the present work a new risk assessment method for cultural heritage sites (RACHS) is shown, illustrating as a case study, with no loss of its broad applicability, its usage with a museum. The suggested risk assessment method permits of finding the precise quantity of physical security defences (intrusion detection system, access control, video surveillance, communication devices, security personnel, etc.) which a given cultural heritage site requires and the correlated features depending on the potential targets that can be damaged. It also permits to avoid of overrating the risk as in the case of considering superfluous defensive countermeasures which occasionally can be not necessary, thus decreasing the associated additional costs.

Keywords: risk assessment, risk analysis, security, safety, cultural heritage sites.

1 INTRODUCTION

Cultural heritage sites are places subjected to certain risks embodied, for example, by theft, vandalism, damaging, terrorism which could arm equally persons and cultural heritage.

For this reason, it is necessary to activate suitable countermeasures to avoid the above risks and to defend against by means of intrusion detection, access control, video surveillance, communication systems, security personnel and procedures suitably combined to achieve an integrated system or solution [1]–[3].

Considering the devices and installations prospective, it is also essential them to be suitably powered and to be able to transmit the data and information necessary for security management. This implies that power providers and communication tools and networks have to be correctly shielded to prevent potential attacks versus them which could damage the performances of integrated technologies employed and therefore let the entire site to be subjected to excessive risks [4].

For this reason, it is essential to evaluate all the potential risks to select the correct countermeasures that have to be implemented versus every possible malicious action. If security systems are already present, their correctness must also be assessed every time the risk framework varies [5]–[7].

In the present work a new risk assessment method for cultural heritage sites (RACHS) is shown, illustrating as a case study, without no loss of its broad applicability, its usage with a museum.

The suggested risk assessment method permits of finding the precise quantity of physical security defences (intrusion detection system, access control, video surveillance, communication devices, security personnel etc.) which a given cultural heritage site requires and the correlated features depending on the potential targets that can be damaged. It also

WIT Transactions on The Built Environment, Vol 203, © 2021 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/STR210131

permits to avoid of overrating the risk as in the case of considering superfluous defensive countermeasures which occasionally can be not necessary, thus decreasing the associated additional costs.

It is also a new method with respect to other security risk assessment methods for heritage sites [7]. As a matter of fact, it utilizes a suitable initial risk analysis to continue further, estimating the level of defence of every target associated to every threats. So, it gives additional valuable knowledge as demonstrated afterwards.

2 DESCRIPTION OF THE METHODOLOGY

The suggested method of risk assessment applied to cultural heritage sites (RACHS) characterizes a particular application obtained from the Physical Security Adapted Layer of Protection Analysis (PSA-LOPA) method [8], [9]. It allows of obtaining the correct quantity of physical security protections (video surveillance, access control, intrusion detection system, etc.) which a certain location needs and the related features. It even supports the specialist in preventing risk overestimate, avoiding of including superfluous protective countermeasures that occasionally results to be futile, thus reducing any needless expense.

For these reasons, the right application of the RACHS methodology means to use an easy and useful examination technique to fix not only which physical security protections (PSPs) the given cultural heritage site necessitates to be classified as properly protected but mainly whether the existing PSPs are essential and adequate.

The LOPA method is divided into diverse subsequent phases:

1. Identification of the physical security risk scenario.
2. Analysis of the severity of the consequences of the above scenario and distribution of a specified Target Factor score.
3. Identification of the initial trigger (Initiating Event).
4. Assessment of the occurrence of incidence of the Initiating Event.
5. Identification of any other elements (Enabling Factors) that, joined with the Initiating Event, activate the scenario.
6. Assessment of the certain time in which the risk is revealed (Time at Risk).
7. Identification of independent defences (Independent Protection Layers, IPLs).
8. Assessment of the probability of failure of the physical security protections (Probability of Failure on Demand, PFD).
9. Assessment of credits.
10. Assessment of the suitability of risk and associated improvement activities.

To achieve the risk assessments, it is necessary to fix how the existing PSPs can diminish the probability of occurrence of the scenario, establishing the notion of ‘credit’. The sense of credit is associated to the probability of failure, linked to every precise PSP$_i$, according to the next equation [10]:

$$credits(IPL)_i = -log(PFD)_i. \tag{1}$$

After that the various credits have been computed, the PSA-LOPA evaluation [8] is achieved with the evaluation of the risk coefficient, correlated to the k scenario, utilizing the equation [10]:

$$R_k = TF_k - F_k^I - F_k^E - I_k^T - \sum_i credits(IPL)_i, \tag{2}$$

where:

TF is the Target Factor.

F^I is the opposite of the logarithm of the incidence of the Initiating Event.

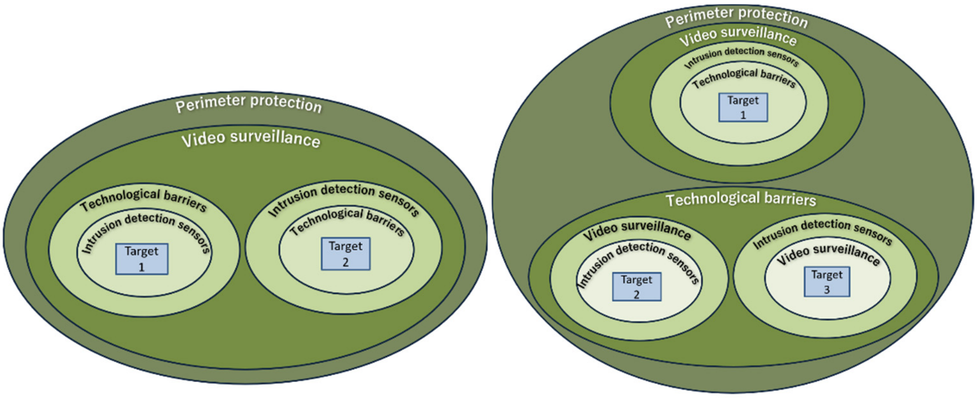
F^E is the opposite of the logarithm of the rate of incidence of the Enabling Factor.
I^T is the indicator of the Time at Risk.
IPLs are the Independent Protection Layers tath, in the contemplated situation, represents the physical security defences, or levels of protections, which IE triggers.

Since LOPA method [10] was firstly thought to estimate industrial risk, the above-mentioned expression required to be accustomed. By adjusting it to the physical security risk, it gave extremely precise and useful results where the PSA-LOPA methodology [8], [9] has been employed. The same results were obtained when the derivative RACHS method was applied to cultural heritage sites.

Physical security is ordinarily applied using the concept of layers of protection since every intruder face various layers of shields as perimeter protection, video surveillance, technological barriers, sensors etc., before reaching the desired goal. This justify the appropriateness of LOPA when the considered flow of risk is reversed.

In fact, LOPA evaluates the different layers of shields beginning from the target and advancing through different levels of protection which could gradually generate harms.

In the PSA-LOPA the progressions are suitably inverted, seeing the various layers of protection as a sort of successive defences to avoid that an aggressor could reach a particular target, causing the expected damages (Fig. 1).



(a) (b)

Figure 1: Graphic illustration of various kind of layers of protections. (a) Two targets; and (b) Three targets.

In this work technological defences are solely contemplated even if the technique can be extended by considering not only technological protections but even physical defences and human factor [11] that are crucial parts for security management.

Some assertions were set to make simpler the technique indicated. These assertions can certainly be adjusted to achieve a better grade of evaluation even if they are not contemplated in this basic estimation. They are embodied by:

- The F^I factor was supposed to be equal to 1, as the intrusion security system is calculated when the incursion has already occurred.
- The I^T factor is not contemplated to simplify even if the times of exposure to a security risk can be identified in some situations.

- The F^E factor is not contemplated to simplify even if in some security incidents it is conceivable to distinguish 'enabling' factors or factors that enable the progress of a security incident.

As PSA-LOPA intends only technological protections and devices whose failure rate is lesser than one and since the failure rate is applied in eqn (1) as probability of failure, the sign the logarithm calculation is adjusted since the outcome of the argument (failure rate, lesser than one) delivers already a negative outcome.

Evidently, the greater the reliability of a specific security shield and the lesser its failure rate. This indicates that the number expected with eqn (1) significantly decreases, diminishing the correlated R factor of the connected risk scenario. This is an obvious consequence because it signifies that the shield used is reliable, ensuring an enhanced grade of security shield and a resultant reduction of the connected risk. The interesting advantage of the proposed method is embodied by its capacity of estimating the various level of defences from the semi-quantitative point of view, leading to an estimation of whether extra levels of protection are required. This additionally provides all the needed evidence to improve the cost/benefit ratio.

In the starting it is needed to categorize the damage levels and the needed level of performances of the security defences for the associated physical security risks and these activities are peculiar of a certain site of a particular organization. An instance is shown in Table 1 where the reliability of security solution (RSS) is shown as well.

Table 1: Summary table of the requested performance levels of the security system, the damage levels, and the PSA-LOPA coefficients.

Requested level of performance	Damage	TF	R (PSA-LOPA)	RSS	PFD
5	SEVERE	9–10	R < –3	>99.99%	<0.0001
4	HIGH	7–8	–3 < R < –2.1	99.9–99.99%	0.001–0.0001
3	MODERATE	5–6	–2 < R <–1.1	99–99.9%	0.01–0.001
2	LIMITED	3–4	–1 < R < 0	90–99%	0.1–0.01
1	NEGLIGIBLE	1–2	R > 0		

The performance level of the security shield is associated to the degree of damage that the security incident can generate. The five levels of damage have been obtained by a standard classification of a general organization, that connects every level to the calculation of economic, physical, company's reputation, legal, expenses etc. damages. So, the PSA-LOPA technique has been adapted and customized to a plenty of situations and it is valid for every sort of organization.

The TF target factor (attained through an appropriate initial risk assessment prepared by the studied organization) has been associated to every level of damage. For instance, a potential target of the greatest strategic and economic importance for the studied organization (data centre, vaults etc.) is correlated with the greatest damage level, and the designated score can vary from 9 to 10, and so on for the levels considered as lower risk.

Different sort of initial evaluations can be done applying, for example, risk matrixes such as: interaction matrix accesses – target/security protections (Table 2), interaction matrix targets-security protections (Table 5), interaction matrix impact on targets-threats (Table 6), etc., which provide significant data to calculate the level of damage of every target of the given site of the studied organization required for the successive PSA-LOPA semi-quantitative assessment.

Table 2: Instance of table of interaction matrix accesses: Targets/security protections.

Access	Target i						Target i + 1				……. .
	Intrusion detection	Access control	Video surveillance	Security personnel	…….	Number of level of protections	…….	…….	…….	Number of level of protections	…….
Access j											

The R factor, i.e. the valuation of the risk factor achieved from eqn (2), is linked with the damage levels of considered organization, thus associating each of them to the associated levels of total reliability of the security solution (RSS) and its likelihood of failure on demand (PFD).

Consequently, the PSA-LOPA method is applicable to all possible targets T_i inside the considered site of the studied organization that are exposed to physical security risks. The choice of the objectives comprised in the assessment is performed pondering the cruciality of them for the organization, considering the information on the exposure to the physical security risk which a fitting initial risk assessment can guarantee.

The suggested risk assessment method for cultural heritage sites (RACHS), shown in the following, embodies an appropriate development and adjustment of PSA-LOPA.

3 DESCRIPTION OF RACHS METHODOLOGY

In cultural heritage sites there are definite risks embodied, for example, by theft, vandalism, damaging, or terrorism which could damage people and the cultural heritage equally.

Thus, suitable measures are required for risk prevention and protection, such as: intrusion detection, access control, video surveillance, communication systems, security personnel and procedures aptly merged to achieve an integrated system or solution [1]–[3]. Further, these technologies can be appropriately integrated to guarantee the safety distance between people, when necessary, during pandemic and post pandemic periods.

It is essential to keep in mind that it is vital that security countermeasures are as non-invasive as feasible. In this way, cultural heritage sites are no subjected to aesthetics and architectural impacts, but their safety and security are always ensured.

It is also particularly vital that devices and installations are appropriately powered and can transmit all the data and information required for security management. This means that power providers, communication tools and networks have to be aptly protected. This is to prevent that a possible assault versus them could generate a reduction or a breakdown of the performances of the integrated technologies being utilized, consequently exposing the whole location to higher risks [4].

Moreover, in cultural heritage sites there can be security personnel endowed by radio communication tools through the day but nobody, or a decreased guarding, through the night. This involves that to be confident the targets to be suitably safeguarded, two distinct assessments must be made, one for day and one for night conditions.

The key elements that are usually present in a cultural heritage site, such as, for example, a museum, and which can be imaginable objectives of intentional attacks are embodied by: external space around the site, entrance hall, ticket office, coffee shop, toilets, shop, luggage depot, internal exhibit rooms with different works of art, offices, control room, data centre, warehouse, main electrical power room, generator set, uninterruptible power supply – UPS, air conditioning central device, external electrical power delivery point, external data network delivery point.

After the potential threats and the possible targets of a cultural heritage sites are focused, RACHS method continues with the construction of a suitable interaction matrix impact on targets-threats. In this matrix all the targets are associated with the respective and different impacts of the diverse threats, introducing, in each link box, a numerical value between 1 and 10, dependent on the impact generated by each threat on each target (0: absent; 1, 2: negligible; 3, 4: limited; 5, 6: moderate; 7, 8: high; 9–10: severe). In this way it becomes possible to determine a mean value of threats for each target focused.

An instance of the considered matrix, for the targets of the case study of a museum considered in the following, is shown in Table 6, while the impact scale is summarized in Table 3.

Table 3: Impact scale with related numerical values.

Impact	Numerical values
SEVERE	9–10
HIGH	7–8
MODERATE	5–6
LIMITED	3–4
NEGLIGIBLE	1–2
ABSENT	0

The levels of physical security shields that can be thought for the RACHS methodology are symbolized by video surveillance, access control, intrusion detection and radio communication devices utilized by security personnel. They are labelled P_1, P_2, P_3, P_4, respectively, even if the method warrants of considering numerous levels of defences, as indicated before, not restricted to technological defence systems since it is certainly extensible to physical barriers and human factor reliability and errors [11].

The likelihood of failure of protection levels P_1, P_2, P_3, P_4, are achieved from the failure levels of every sort of used means. About video surveillance, the failure rate is multiplied by the percentage of visual coverage of the area evaluated (i.e. equal to 1 if all the considered area is comprised). Similar issues, with suitable variation, are applicable for security personnel endowed by radio devices.

After that all the targets of the site have been appropriately focused, it is possible to assess for every target T_i, applying the associated level of defences P_{1i}, P_{2i}, P_{3i}, P_{4i}, through the prior equations, the connected PSA-LOPA risk factor R_i, i.e. achieving the actual physical security level of defence of all the targets of the location.

It is now possible to produce a concise table (as shown in Table 4) where:

- the first column expresses the different targets.
- the second and the third columns express the possible damages confrontable by the actual level of protection determined via PSA-LOPA (using eqns (1) and (2)), through the day and through the night, respectively, converted using Table 1.
- the fourth column expresses the expected damage calculated by means of the results of initial analysis, converted using Tables 1 and 3.
- the fifth and the sixth columns express the actual level of performance of the security protections through the day and through the night, respectively, computed via PSA-LOPA (by means of eqns (1) and (2)), converted using Table 1.

- the seventh column expresses the required level of performance of the security protections necessary to face the expected damages calculated by means of the results of initial analysis, converted using Tables 1 and 3.

Table 4: Instance of a summary table of the RACHS method outcomes.

Target	Damage confrontable by the actual level of protection (day)	Damage confrontable by the actual level of protection (night)	Estimated damage	Actual level of performance (day)	Actual level of performance (night)	Requested level of performance
Target i						
…..						

The damage confrontable by the actual level of protection and the actual level of performance has been judged in a different way for the day from the one for the night since the number of defence levels could be different in the two circumstances. For example, there could be greater quantity of security personnel components endowed by radio communications tools through the day and their number could be decreased through the night. If it is planned the absence of security personnel during the night, there can be other sort of protection defences activated.

The outcomes attained allows of evaluating rapidly if the performance level of protections of every target, and consequently of the whole site, are fitting or the current layers of protection of each target need reinforcement (increasing their reliability, for example) or augmenting their number to scope the required performance level. Then, a proper decision is made for the level of protection of each target as a function of the probability of the related threat, and therefore of the associated risk.

Table 4 can also be condensed using a suitable histogram graph to obtain suddenly a clear view of the state or in a further manner via a radar graph. Both are shown in the next general case study of a museum.

4 EXAMPLE OF APPLICATION TO A MUSEUM

In the following, a museum is considered as a general case study, without any loss of generality with respect to other kind of cultural heritage sites.

For our purposes we presume that in the museum all the targets earlier focused are present, and that external and internal video surveillance, access control, intrusion detection and security personnel endowed by radio are used to protect them. This excludes now other countermeasures which can utilized as supplementary security defences, if needed. For the consequent analytic calculation, these security defences are judged as being categorized by mean technical/operative characteristics of commercial devices (that are not shown here for briefness). An outline of the context for day and night is shown in Table 5 (interaction matrix targets-security protections), where “internal exhibit room” represents the ith room of the museum and “work of art(j) of exhibit room(i)” represents the jth exposed element of room(i). Since there can be different works of art in the different exhibit rooms, these two targets must be repeated in Table 5 a number of times equal to the number of different elements protected by different levels of protection, if they are interested by different layers of protections. If the levels of protections are the same for all the exhibition rooms and related works of art, they must be considered only once. In this way it is possible to reach a great detail in the analysis

Table 5: Interaction matrix targets – security protections in the studied museum ('X' signifies the presence, '–' signifies the absence).

Target	Kind of protection				
	External video surveillance (day/night) [X/–]	Internal video surveillance (day/night) [X/–]	Access control (day/night) [X/–]	Intrusion detection (day/night) [X/–]	Security personnel equipped with radio (day/night) [X/–]
External space around the site	X/X	–/–	–/–	–/–	X/–
Entrance hall	–/–	X/X	–/–	–/–	X/–
Ticket office	X/X		X/X		X/–
Coffee shop	X/X	–/–	–/–	–/–	X/–
Toilets	X/X	–/–	–/–	–/–	–/–
Shop	–/–	X/X	–/–	–/–	X/–
Luggage depot	–/–	X/X	X/X		
Internal exhibit room (i)	–/–	X/X	–/–	–/–	X/X
Work of art (j) of exhibit room (i)	X/X	–/–	–/–	X/X	X/X
Offices	X/X	–/–	X/X	–/–	–/–
Control room	X/X	–/–	X/X	–/–	X/X
Data centre	X/X	X/X	X/X	–/–	–/–
Warehouse	X/X	X/X	X/X	X/X	X/–
Main electrical power room	X/X	X/X	X/X	–/–	–/–
Generator set	X/X	X/X	X/X	–/–	–/–
Uninterruptible Power Supply – UPS	X/X	X/X	X/X	–/–	–/–
Air conditioning central device	X/X	X/X			
External electrical power delivery point	X/X	–/–	–/–	–/–	X/–
External data network delivery point	X/X	–/–	–/–	–/–	X/–

since it is conceivable to consider the levels of protection of each work of art that can different according to their value.

All the required information to carry out an initial assessment have been obtained through open-source data available on the Internet. In this manner it has been conceivable to develop the interaction matrix impact on targets – threats for the studied site whose outcomes are displayed in Table 6, where mean values of each target are rounded to the upper integer to use a precautionary approach.

Table 6: Table of interaction matrix impact on targets – threats for the studied location.

Target	Vandalism	Physical violence against people and/or objects	Damage	Sabotage	Espionage	Theft	Arson	Robbery	Explosive device	Terrorist attack	Mean value
External space around the site	7	6	7	7	0	7	7	6	8	8	7
Entrance hall	8	8	7	7	0	7	8	8	10	10	8
Ticket office	8	8	7	7	6	8	8	9	8	8	8
Coffe shop	8	8	7	7	0	6	8	6	8	8	7
Toilets	7	8	7	7	0	6	8	3	8	8	7
Shop	8	8	7	3	0	8	8	6	8	8	7
Luggage depot	4	8	6	3	0	7	8	8	8	8	6
Internal exhibit room(i)	9	9	9	8	4	9	10	10	10	10	9
Work of art(j) of the exhibit room(i)	10	10	10	8	4	10	10	10	10	10	10
Offices	7	8	7	7	7	8	7	7	8	8	8
Control room	8	9	8	8	8	4	9	7	9	8	8
Data centre	8	9	8	8	8	8	9	7	9	8	9
Warehouse	8	9	8	8	4	8	10	8	9	9	9
Main electrical power room	8	9	8	8	4	8	8	8	9	9	8
Generator set	8	9	8	8	4	8	8	8	9	9	8
Uninterruptible Power Supply (UPS)	8	9	8	8	4	8	8	8	9	9	8
Air conditioning central device	7	9	8	7	6	8	8	6	7	6	8
External electrical power point delivery	8	8	9	9	6	9	8	8	9	9	9
External data network delivery point	8	8	9	9	6	9	8	8	9	9	9

It is now conceivable to continue with the computation, according to what specified previously, bearing in mind that mean values of every target of Table 6 are considered as the associated target Factors (TF) and they embody the estimated damage and the related requested level of performance in Table 7, after suitable numerical translation by using Tables 1 and 3. Results of Table 7 are shown in Figs 2 and 3.

As it is possible to see from Figs 2 and 3, except for targets 7, 9, 11, 12, 13, 14, 15, 16, targets are categorized by an actual level of performance (equally during the day and the night or just during one of them), that are lesser with respect to the demanded level of performance. In some situations, the night decrease depends on the lack or the reduction of

Table 7: Resuming table of RACHS methodology results for the considered site.

Target	Damage confrontable by the actual level of protection (day)	Damage confrontable by the actual level of protection (night)	Estimated damage	Actual level of performance (day)	Actual level of performance	Requested level of performance
External space around the site	HIGH	NEGLIGIBLE	HIGH	4	1	4
Entrance hall	MODERATE	NEGLIGIBLE	HIGH	3	1	4
Ticket office	SEVERE	MODERATE	HIGH	5	3	4
Coffe shop	HIGH	NEGLIGIBLE	HIGH	4	1	4
Toilets	NEGLIGIBLE	NEGLIGIBLE	HIGH	1	1	4
Shop	HIGH	NEGLIGIBLE	HIGH	4	1	4
Luggage depot	SEVERE	SEVERE	MODERATE	5	5	3
Internal exhibit room(i)	LIMITED	LIMITED	SEVERE	2	2	5
Work of art(j) of the exhibit room(i)	SEVERE	SEVERE	SEVERE	5	5	5
Offices	MODERATE	MODERATE	HIGH	3	3	4
Control room	SEVERE	SEVERE	HIGH	5	5	4
Data centre	SEVERE	SEVERE	SEVERE	5	5	5
Warehouse	SEVERE	SEVERE	SEVERE	5	5	5
Main electrical power room	SEVERE	SEVERE	HIGH	5	5	4
Generator set	SEVERE	SEVERE	HIGH	5	5	4
Uninterruptible Power Supply (UPS)	SEVERE	SEVERE	HIGH	5	5	4
Air conditioning central device	MODERATE	MODERATE	HIGH	3	3	4
External electrical power point delivery	LIMITED	NEGLIGIBLE	SEVERE	2	1	5
External data network delivery point	LIMITED	NEGLIGIBLE	SEVERE	2	1	5

security personnel endowed by radio. This implies that is required to augment of one or more the levels of security protection for them. This be done by introducing, for example, a suitable intrusion detection system, thermal camera, motion detection, video analysis or other type of countermeasures. If high quality strengthening countermeasures are used, it is possible to verify, repeating the computation process, if the upgraded actual level of protection (equally in the day and in the night) scopes, or in some cases exceeds, the demanded level of protection, guaranteeing the apt security defending of every targets of the studied site.

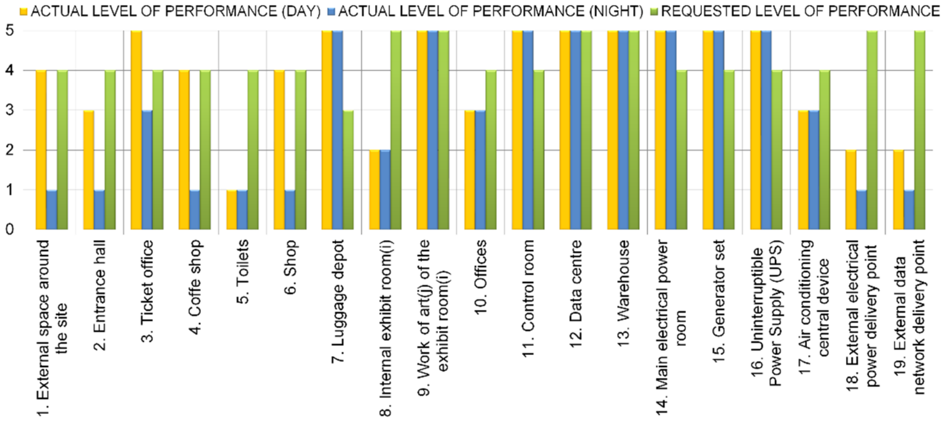


Figure 2: Histogram graph of the obtained results.

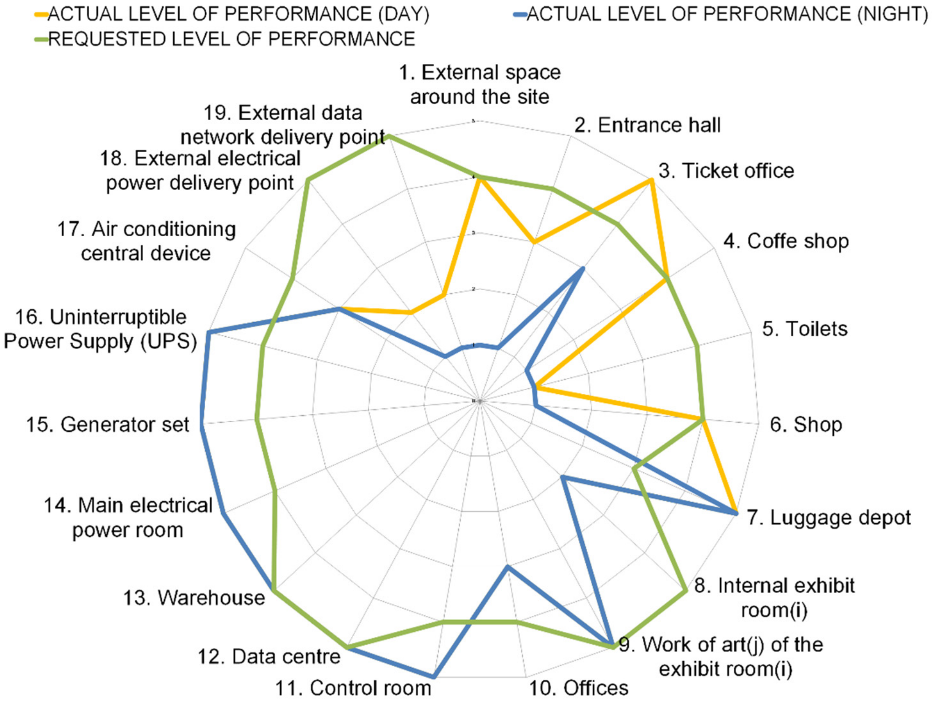


Figure 3: Radar graph of the obtained results.

So, it is conceivable to evaluate and definitively achieve all the needed and extra defences, carefully pondering the cost/benefit ratio, to guarantee the desired level of protection to the various targets, also considering the related likelihood of the threats.

5 CONCLUSIONS

The proposed RACHS method embodies a general technique suitable for any sort of cultural heritage site and permits of evaluating, in a relatively fast and effective mode, the level of physical security risks and the connected countermeasures, envisioned as layers of protection, essential to scope the required protection level, if needed, as it happened in a lot of real situations where it was applied. The delivered results permit of obtaining also solutions characterized by an optimal cost/benefit ratio.

REFERENCES

[1] Garzia, F., Sammarco, E. & Cusani, R., The integrated security system of the Vatican City State. *International Journal of Safety and Security Engineering*, **1**(1), pp. 1–17, 2011.

[2] Garzia, F., The Internet of Everything based integrated system for security/safety/general management/visitors' services for the Quintili's Villas area of the Ancient Appia way in Rome, Italy. *WIT Transactions on the Built Environment*, vol. 174, WIT Press: Southampton and Boston, pp. 261–272, 2018.

[3] Garzia, F., Lombardi, M. & Ramalingam, S., An integrated Internet of Everything – Genetic algorithms controller – Artificial neural networks based framework for security systems management and support. *Proceedings of IEEE International Carnahan Conference on Security Technologies*, 2017.

[4] Garzia, F., *Handbook of Communication Security*, WIT Press: Southampton and Boston, 2013.

[5] Broder, J.F. & Tucker, E., *Risk Analysis and the Security Survey.* Butterworth-Heinemann: New York, 2012.

[6] Norman, T.L., *Risk Analysis and Security Countermeasure Selection*, CRC Press, 2010.

[7] CCI/ICC & ICCROM, *The ABC Method*: *A Risk Management Approach to the Preservation of Cultural Heritage*, Canadian Conservation Institute, 2016.

[8] Garzia, F., Lombardi, M., Fargnoli, M. & Ramalingam, S., PSA-LOPA – A novel method for physical security risk analysis based on LOPA – Layers of protection analysis. *Proceedings of IEEE International Carnahan Conference on Security Technologies*, pp. 187–191, 2018.

[9] Garzia, F., Sammarco, E., New risk analysis methodology for religious buildings. *WIT Transactions on Engineering Sciences*, vol. 129, WIT Press: Southampton and Boston, pp. 215–227, 2020.

[10] Willey, R., J., Layer of protection analysis. *Proceedings of 2014 International Symposium on Safety Science and Technology, Procedia Engineering*, vol. 84, pp. 12–22, 2014.

[11] Borghini, F., Garzia, F., Borghini, A. & Borghini, G., *The Psychology of Security, Emergency and Risk*, WIT Press: Southampton and Boston, 2016.