NEW RISK ANALYSIS METHODOLOGY FOR RELIGIOUS BUILDINGS

FABIO GARZIA[1,2,3] & ENZO SAMMARCO[4]
[1]Safety and Security Engineering Group – DICMA, SAPIENZA – University of Rome, Italy
[2]Wessex Institute of Technology, Southampton, UK
[3]European Academy of Sciences and Arts, Salzburg, Austria
[4]General Directorate for Safety, Security and Civil Protection, Vatican City

ABSTRACT

Religious buildings are sites exposed to specific risks represented, for example, by theft, vandalism, damage, and terrorism that could injure both people and cultural/religious heritage. Therefore, they need proper actions to prevent the above risks and to protect against them using intrusion detection, access control, video surveillance, communication systems, security personnel and procedures properly integrated to realize an integrated system or solution. In this paper a novel risk analysis methodology for religious buildings (RARB) is illustrated, showing as a case study, without any loss of its general validity, its application to a Catholic church. The proposed risk analysis technique allows identifying the exact number of physical security protections (intrusion detection system, access control, video surveillance, communication devices, security personnel, etc.) that the religious site needs and the related performances as a function of the possible targets which can be attacked. It also allows avoiding overestimating the risk as in the case of including redundant protective countermeasures that sometimes result to be useless, thereby reducing the related extra costs involved. Furthermore, it results in being useful and suitable for plenty of other cultural heritage sites.

Keywords: risk analysis, security, safety, religious building, heritage site.

1 INTRODUCTION

Religious buildings are sites exposed to specific risks represented, for example, by theft, vandalism, damaging, terrorism that could injure both people and cultural/religious heritage. Therefore, they need proper actions to prevent the above risks and to protect from them using intrusion detection, access control, video surveillance, communication systems, security personnel and procedures properly integrated to realize an integrated system or solution [1]–[3].

From the devices and installations point of view, it is also extremely important that they are properly powered and that they can communicate all the data and information necessary for security management. This means that also power suppliers and communication devices and networks must be properly protected to avoid that a possible attack against them could compromise the functionalities of integrated technologies used and consequently expose the whole site to high risks [4].

From this point of view, it is vital to analyse and assess all the possible risks to choose the proper countermeasures which must be adopted against all the potential attacks. In case of already existing security systems, their suitability must also be evaluated when the risk context changes [5]–[7].

In this paper a novel risk analysis methodology for religious buildings (RARB) is illustrated, showing as a case study, without any loss of its general validity, its application to a Catholic church, represented by the "Basilica of the Holy Cross in Jerusalem" in Rome (Italy).

The proposed risk analysis technique allows identifying the exact number of physical security protections (intrusion detection system, access control, video surveillance,

WIT Transactions on Engineering Sciences, Vol 129, © 2020 WIT Press
www.witpress.com, ISSN 1743-3533 (on-line)
doi:10.2495/RISK200191

communication devices, security personnel etc.) that the religious site needs and the related performances as a function of the possible targets which can be attacked. It also allows avoiding overestimating the risk as in the case of including redundant protective countermeasures that sometimes result to be useless, thereby reducing the corresponding extra costs involved. Further, it results to be useful and suitable in a plenty of other heritage sites.

It results to be a novel approach compared to other security risk analysis methodologies for heritage sites [7]. In fact, it uses a proper preliminary risk analysis to go further ahead, evaluating the level of protection of each target related to the different threats. In this way, it provides more useful information as shown in the following.

2 DESCRIPTION OF THE METHODOLOGY

The proposed methodology of risk analysis for religious buildings (RARB) represents a specific application derived from the Physical Security Adapted Layer of Protection Analysis (PSA-LOPA) technique [8]. It permits of finding the precise number of physical security defences (video surveillance, access control, intrusion detection system, etc.) that a given place requires and the associated performances. It also helps the expert avoiding risk overestimation as in the case of involving unnecessary defensive tools which sometimes result being worthless, thus decreasing any unnecessary cost.

For these reasons, the correct application of the RARB methodology signifies to use a simple and helpful testing approach to determine not only what physical security protections (PSPs) the religious building requires to be considered secure but most of all whether the current PSPs are indispensable and sufficient.

The LOPA methodology is composed by different stages:

1. Recognition of the physical security risk scenario.
2. Survey of the gravity of the effects of the above scenario and allocation of a well-defined target factor score.
3. Recognition of the starting cause (initiating event).
4. Estimation of the frequency of occurrence of the initiating event.
5. Recognition of any other components (enabling factors) which, combined with the initiating event, start the scenario.
6. Estimation of the actual time in which the risk is shown (time at risk).
7. Recognition of independent protections (independent protection layers (IPLs)).
8. Estimate of the likelihood of failure of the physical security protections (probability of failure on demand (PFD)).
9. Estimation of credits.
10. Estimation of the appropriateness of risk and related enhancement actions.

To perform the risk analysis, what is needed is determining how considerably the existing PSPs can decrease the likelihood that the scenario happen, introducing the concept of “credit”. The meaning of credit is linked to the likelihood of malfunction, associated to each specific PSP$_i$, according to the following equation [9]:

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

After the different credits have been calculated, the PSA-LOPA analysis [8] is obtained with the estimate of the risk coefficient, related to the *k* scenario, applying the equation [9]:

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

where:

- *TF* is the target factor.
- F^I is the opposite of the logarithm of the occurrence of the initiating event.
- F^E is the opposite of the logarithm of the frequency of occurrence of the enabling factor.
- I^T is the index of the time at risk.
- *IPL*s are the independent protection layers which, in the considered situation, embodies the physical security protections, or levels of protections, that activates following the IE.

Due to the fact that the LOPA technique [9] was originally considered for the evaluation of industrial risk, the aforementioned formulation needed to be adjusted. Shaping it to the physical security risk, provided very accurate and valuable outcomes whereas the considered PSA-LOPA technique [8] has been applied. The same happened for the derived RARB method utilized with religious buildings.

Physical security is normally used according to layers of protection so that any intruders encounter different layers of protection as perimeter protection, video surveillance, technological barriers, sensors etc., prior of getting the required target. For this reason, LOPA method is very fitting since it is required to reverse the considered flow of risk.

In fact, LOPA ponders the various layers of protection starting from the target and proceeding towards various levels of protection that could progressively produce damages.

In the PSA-LOPA the processes are properly reversed, considering the different layers of protection as a type of subsequent protections to prevent an intruder could get a certain target, generating the planned harms (Fig. 1).

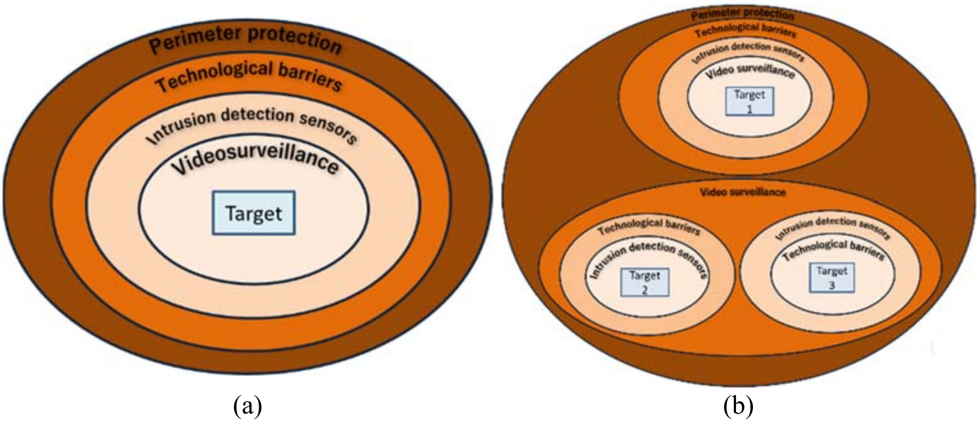


Figure 1: Schematic representation of different layers of protections. (a) 1 target; (b) 3 targets.

In this work technological protections are exclusively considered but the method can be expanded by contemplating not only technological defences but also physical defences and human factor [10] which are essential components for security managing.

Some statements were made to simplify the method suggested. These statements can obviously be revised to attain a greater degree of assessment even if they are not considered in this essential evaluation. They are represented by:

- the F^I factor was presumed to be equal to 1, because the intrusion security system is assessed when the intrusion has already occurred.

- The I^T factor is not considered for easiness even if the times of exposure to a security risk can be defined in specific circumstances.
- The F^E factor is not contemplated for easiness even if in certain security experiences it is possible to detect “enabling” factors or factors that enable the progress of a security event.

Due to the fact that PSA-LOPA aims only at technological defences and devices whose failure rate is smaller than one and since the failure rate is utilized in eqn (1) as likelihood of failure, the sign the logarithm computation is changed because the result of the argument (failure rate, smaller than one) provides already a negative result.

Obviously, the higher is the reliability of a certain security defence and the smaller is its failure rate. This implies that the quantity estimated with eqn (1) greatly reduces, decreasing the associated R coefficient of the correlated risk scenario. This is a clear outcome since it means that the protection considered is very trustworthy, guaranteeing an improved degree of security defence and a consequent decrease of the correlated risk. The countless benefit of the projected methodology is represented by its capability of evaluating the diverse level of protections from the semi-quantitative point of view, leading to an assessment of whether additional levels of protection are needed. This also offers also all the required information to optimize the cost/benefit ratio.

In the beginning it is required to classify the damage levels and the demanded level of performances of the security solutions for the correlated physical security risks and these actions are specific of a given site of a given organization. An example is shown in Table 1 where the reliability of security solution (RSS) is also indicated.

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 protection is linked to the level of damage that the security event can produce. The five levels of damage have been derived by a standard classification of a hypothetical organization, that links each level to the quantification of economic, physical, company’s reputation, legal, expenses etc. damages. This way, the PSA-LOPA method has been modified and personalized to a wide-ranging environment applicable to any type of organization.

The TF target factor (obtained by means of a proper preliminary risk analysis made by the considered organization) has been correlated to each level of damage. As an example, a possible target of the maximum tactical and economic significance for the considered organization (data centre, vaults etc.) is associated with the maximum damage level, and the assigned score can vary from 9 to 10, and so on for the levels characterized by a lower risk.

Various type of preliminary analysis can be done utilizing, for instance, risk matrixes such as: interaction matrix targets – security protections, interaction matrix impact on targets – threats, interaction matrix accesses – security protections etc., which offer valuable information to assess the level of damage of each target of the specific site of the given organization required for the subsequent PSA-LOPA semi-quantitative analysis.

The R factor, i.e. the estimate of the risk factor attained from eqn (2), is correlated with the damage levels of given organization, thus linking each of them to the related levels of overall reliability of the security solution (RSS) and its probability of failure on demand (PFD).

Therefore, the PSA-LOPA technique is applicable to all potential targets T_i within the given location of the organization considered which are subjected to physical security risks. The selection of the targets contained in the analysis is done considering the criticality of the same for the organization and basing on the information on the exposure to the physical security risk that a suitable preliminary risk analysis can ensure.

The proposed risk analysis methodology for religious building (RARB), illustrated in the following, represents a proper improvement and adaptation of PSA-LOPA.

3 DESCRIPTION OF RARB METHODOLOGY

In religious buildings there are specific risks represented, for example, by theft, vandalism, damaging, or terrorism that might injure both the people and the cultural/religious heritage.

Therefore, proper actions are needed for risk avoidance and protection, such as: intrusion detection, access control, video surveillance, communication systems, security personnel and procedures suitably joined to realize an integrated system or solution [1]–[3]. Furthermore, these technologies can be properly integrated to ensure the safety distance between people. This represents an important feature in the pandemic and post pandemic periods.

It is important to recall that religious buildings represent mainly places where pilgrims go to pray and for this reason it is essential that security measures are as non-intrusive and non-invasive as possible. In this way, pilgrims are not disturbed but their safety and security are guaranteed.

In addition, in religious places there can be objects of inestimable spiritual value which may be different from their material value, and therefore require a high level of protection.

It is also extremely important, from the devices and installations point of view, that they are correctly powered and can communicate all the data and information necessary for security management. This implies that power suppliers, communication devices and networks must be appropriately sheltered. This is to avoid that a likely attack against them could compromise the performances of the integrated technologies being used, thus exposing the entire place to elevated risks [4].

Furthermore, in religious buildings there can be security personnel equipped with radio communication devices during the day but nobody, or a reduced patrolling, during the night. This means that, to be sure that the targets are properly protected, two different analyses must be made, one for day and one for night situations.

The main elements that are normally present in a religious building and that can be possible targets of voluntary attacks are represented by: internal space for prayer and visitors, object of spiritual value/works of art, external space around the religious building and within the religious site, religious restricted rooms (symbolized by the sacristy in Catholic church), museum, religious articles shop, refreshment area and toilets, offices, control room, equipment and devices room o data centre, radio transmitting room, electrical transformer substation, generator set, uninterruptible power supply (UPS), electricity delivery point, ADSL/Internet delivery point.

Once identified, the possible threats and the likely targets of a religious building, RARB methodology proceeds with the creation of a proper interaction matrix: likelihood x impact on targets – threats. In it each target is related with the different likelihoods x impacts of the different threats, inserting, in each correlation box, a numerical value between 1 and 10, depending on the likelihood x impact produced 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 appears possible to calculate a mean value of threats for each target identified.

An example of the above mentioned matrix, for the generic targets, is represented in Table 2, while the likelihood x impact scale is resumed in Table 3.

Table 2: Example of table of interaction matrix likelihood x impact on targets – threats.

Target	Threats										
	Vandalism	Physical violence against people and/or objects	Damage	Sabotage	Espionage	Theft	Arson	Robbery	Explosive device	Terrorist attack	Mean value
Target i											
…..											

Table 3: Likelihood x impact scales are shown with related numerical values.

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

The layers of physical security protection that can be considered for the RARB method are represented by video surveillance, access control, intrusion detection and radio communication devices used by security personnel. They are named P_1, P_2, P_3, P_4, respectively, even if the methodology permits to contemplate several levels of protections, as showed previously, not limited to technological protection systems since it is easily extendable to physical barriers and human factor reliability and errors [10].

The likelihood of failure of protection layers P_1, P_2, P_3, P_4, are obtained from the failure rates of each type of utilized tools. Regarding video surveillance, the failure rate is multiplied by the percentage of visual coverage of the area considered (i.e. equal to 1 if all the considered area is covered). Similar considerations, with proper adaptation, are valid for security personnel equipped with radio.

After all, the targets of the site have been properly focused, it is possible to estimate for each target T_i, using the correlated level of protections P_{1i}, P_{2i}, P_{3i}, P_{4i}, by means of the previous equations, the associated PSA-LOPA risk factor R_i, i.e. finding the real physical security level of protection of all the targets of the location.

At this time, it is possible to create a summary table (as shown in Table 4) where:

- the first column embodies the various targets.
- The second and the third columns embody the potential damages confrontable by the actual level of protection calculated by means of PSA-LOPA (using eqns (1) and (2)), during the day and during the night, respectively, transformed using Table 1.
- The fourth column embodies the expected damage estimated applying the outcomes of preliminary analysis, transformed using Tables 1 and 3.
- The fifth and the sixth columns embody the actual level of performance of the security protections during the day and during the night, respectively, calculated by means of PSA-LOPA (using eqns (1) and (2)), transformed using Table 1.
- The seventh column embodies the requested level of performance of the security protections required to contrast the anticipated damages obtained by the outcomes of preliminary analysis, transformed using Tables 1 and 3.

The damage confrontable by the actual level of protection and the actual level of performance has been considered differently for the day from the one for the night because the number of protections levels might be different in the two situations. For example, there could be larger number of security personnel units equipped with radio communications devices during the day and this could be reduced during the night. Planning also for the absence of security personnel, can be due to the activations of other kind of protection levels.

Table 4: Example of a summary table of the RARB methodology results.

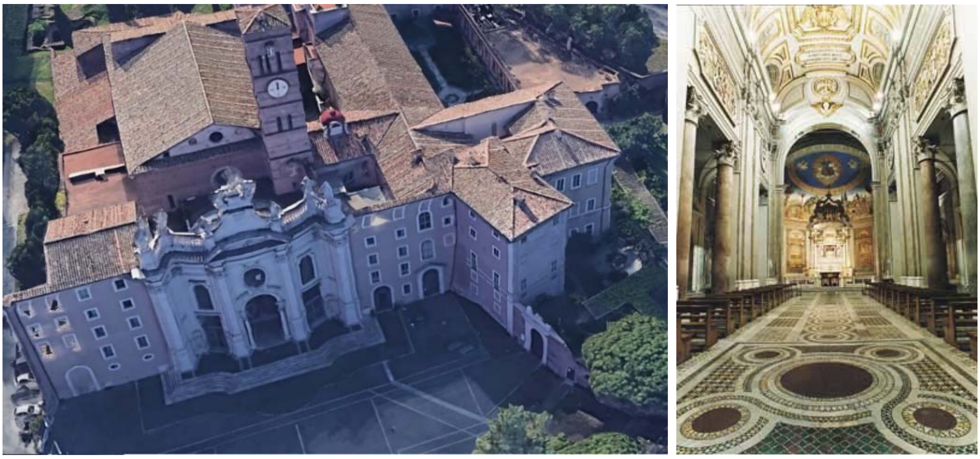
Target	Damage confrontable by the actual level of protection	Damage confrontable by the actual level of protection (night)	Estimated damage	Actual level of performance (day)	Actual level of performance (night)	Requested level of performance
Target i						
…..						

The results obtained permit assessing instantly whether the performance level of protections of each target, and therefore of the entire location, are appropriate or the current layers of protection of each target required strengthening (raising their reliability, for example) or raising their number to reach the demanded performance level.

Table 4 can also be summarized by means of a proper histogram graph to get instantly a clear vision of the situation or in a further mode by means of a radar graph. Both are shown in the following case study of a Catholic church.

4 EXAMPLE OF APPLICATION TO A CATHOLIC CHURCH

Let's consider now, as a case study, a Catholic church: the Basilica of the Holy Cross in Jerusalem, located in Rome (Italy), which is one of the seven churches in Rome that are part of the traditional pilgrimage route made famous by Saint Philip Neri (Fig. 2).



(a) (b)

Figure 2: Views of the Basilica of the Holy Cross in Jerusalem. (a) External; and (b) Internal.

The Basilica was built starting from the 4th century AD in the Sessorium palace, residence of Saint Helen, the mother of the Roman Emperor Constantine, near the Lateran zone. It was erected not to honour the memory of the martyrs, as was tradition, but exclusively to preserve a part of the Cross of Jesus, together with other relics of the Passion. According to tradition, Saint Helena had transported it back to Rome from her travel to the Holy Land in 325 AD. It was therefore conceived from the beginning as a large reliquary, intended to preserve precious testimonies of the passion of Jesus. The Basilica is called "in Jerusalem" because of the presence of consecrated land of Mount Calvary, which was placed at the base of the foundations. It was land transported on ships together with the same relics of the Cross. For this reason, since the Middle Ages the Basilica was simply called "Hierusalem" (in Latin), and for popular devotion, visiting this Basilica meant setting foot in the same holy city of Jerusalem. It has the dignity of a minor Basilica.

For our purposes as kind of protection, we assume that in the church all the targets previously identified as existing are present, requiring, external and internal video surveillance, access control and security personnel equipped with radio. This excludes at the moment, intrusion detection that is used as an additional security protection if necessary. For the subsequent analytical computation, these security protections are considered as being characterized by mean technical/operative features of commercial devices (which are not indicated here for brevity). A summary of the situation for day and night is shown in Table 5.

Table 5: Kind of protection of different targets in the considered church ("X" indicates the presence and "–", indicates 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/–)
Internal space for prayer and visitors	X/X	X/X	–/–	–/–	X/–
Objects of spiritual value/works of art	X/X	X/X	–/–	–/–	X/–
External space around the religious building and within the religious site	–/–	–/–	–/–	–/–	X/–
Sacristy	X/X	X/X	–/–	–/–	X/–
Museum	X/X	X/X	–/–	–/–	X/–
Religious articles shop	X/X	X/X	–/–	–/–	X/–
Refreshment area and toilets	X/X	X/X	–/–	–/–	X/–
Offices	X/X	–/–	–/–	–/–	X/–
Control room	X/X	X/X	X/X	–/–	X/–
Equipment and devices room or data centre	X/X	X/X	X/X	–/–	X/–
Radio transmitting room	X/X	X/X	–/–	–/–	X/–
Electrical transformer substation	X/X	–/–	–/–	–/–	X/–
Generator set	X/X	–/–	–/–	–/–	X/–
Uninterruptible power supply (UPS)	X/X	–/–	–/–	–/–	X/–
Electricity delivery point	X/X	–/–	–/–	–/–	X/–
ADSL/Internet delivery point	X/X	–/–	–/–	–/–	X/–

All the necessary data to perform a preliminary analysis have been acquired by means of inspections as ordinary visitors and by means of open source data available on the Internet. In this way it has been possible to derive the interaction matrix likelihood x impact on targets – threats for the considered site whose results are shown in Table 6.

It is now possible to proceed with the calculation, according to what indicated before, considering that mean values of each target of Table 6 are seen as the correlated target Factors (TF) and they represent the estimated damage and the related requested level of performance in Table 7, after proper numerical conversion by means of Tables 1 and 3. Results of Table 1 are shown in Figs 3 and 4.

Table 6: Table of interaction matrix likelihood x impact on targets – threats for the considered site.

Target	Threats										
	Vandalism	Physical violence against people and/or objects	Damage	Sabotage	Espionage	Theft	Arson	Robbery	Explosive device	Terrorist attack	Mean value
Internal space for prayer and visitors	10	10	10	10	0	10	10	10	10	10	9
Objects of spiritual value/works of art	10	10	10	10	0	10	10	10	10	10	9
External space around the religious building and within the religious site	10	10	10	0	0	10	10	10	10	10	8
Sacristy	10	10	10	0	0	10	10	10	10	10	8
Museum	10	10	10	0	0	10	10	10	10	10	8
Religious articles shop	2	4	6	0	0	6	8	5	10	10	5
Refreshment area and toilets	2	4	6	0	0	1	6	10	0	10	3
Offices	7	10	7	7	10	10	7	6	6	6	8
Control room	0	8	0	0	0	0	3	0	10	10	3
Equipment and devices room or data centre	10	0	10	10	10	8	10	0	10	10	8
Radio transmitting room	8	0	8	8	0	0	8	0	8	8	4
Electrical transformer substation	10	0	10	10	0	10	10	0	10	10	7
Generator set	10	0	10	10	0	10	10	0	10	10	7
Uninterruptible power supply (UPS)	10	0	10	10	0	10	10	0	10	10	7
Electricity delivery point	10	0	10	10	0	10	10	0	10	10	7
ADSL/Internet delivery point	8	0	8	8	0	0	8	0	8	8	4

As it is possible to see from Figs 3 and 4, except for targets 6, 7, 9, 10, 11, 16, targets are characterized by an actual level of performance (in both the day and the night or only one of them), which are lower than the requested level of performance. In some cases, the night reduction is due to the absence or to the decrease of security personnel equipped with radio. This means that is necessary to add one or more levels of security protection. It could be done adding, for example, a proper intrusion detection system (that was not present in the initial hypothesis on purpose) or thermal camera equipped with motion detection/video analysis. If

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

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
Internal space for prayer and visitors	SEVERE	LIMITED	SEVERE	5	2	5
Objects of spiritual value/works of art	SEVERE	HIGH	SEVERE	5	4	5
External space around the religious building and within the religious site	NEGLIGIBLE	NEGLIGIBLE	HIGH	1	1	4
Sacristy	SEVERE	MODERATE	HIGH	5	3	4
Museum	SEVERE	MODERATE	HIGH	5	3	4
Religious articles shop	SEVERE	SEVERE	MODERATE	5	5	3
Refreshment area and toilets	SEVERE	SEVERE	LIMITED	5	5	2
Offices	MODERATE	NEGLIGIBLE	HIGH	3	1	4
Control room	SEVERE	SEVERE	LIMITED	5	5	2
Equipment and devices room or data centre	SEVERE	SEVERE	HIGH	5	5	4
Radio transmitting room	SEVERE	SEVERE	LIMITED	5	5	2
Electrical transformer substation	HIGH	NEGLIGIBLE	HIGH	4	1	4
Generator set	HIGH	NEGLIGIBLE	HIGH	4	1	4
Uninterruptible Power Supply (UPS)	HIGH	NEGLIGIBLE	HIGH	4	1	4
Electricity delivery point	HIGH	NEGLIGIBLE	HIGH	4	1	4
ADSL/Internet delivery point	SEVERE	SEVERE	LIMITED	5	5	2

high quality reinforcing solutions are used, it is possible to demonstrate (not shown here for brevity) that the actual level of protection (both in the day and in the night) reaches, and in some cases overcomes, the requested level of protection, ensuring the suitable security shielding of all the targets of the considered site.

In this way, it is possible to analyse and finally obtain all the required and additional defences, correctly considering the cost/benefit ratio, to ensure the needed level of protection to the various targets.

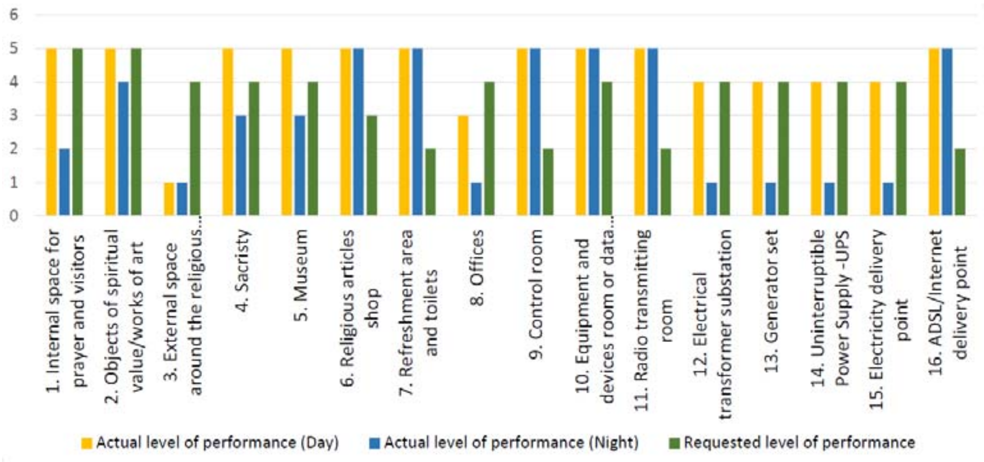


Figure 3: Histogram graph of the results.

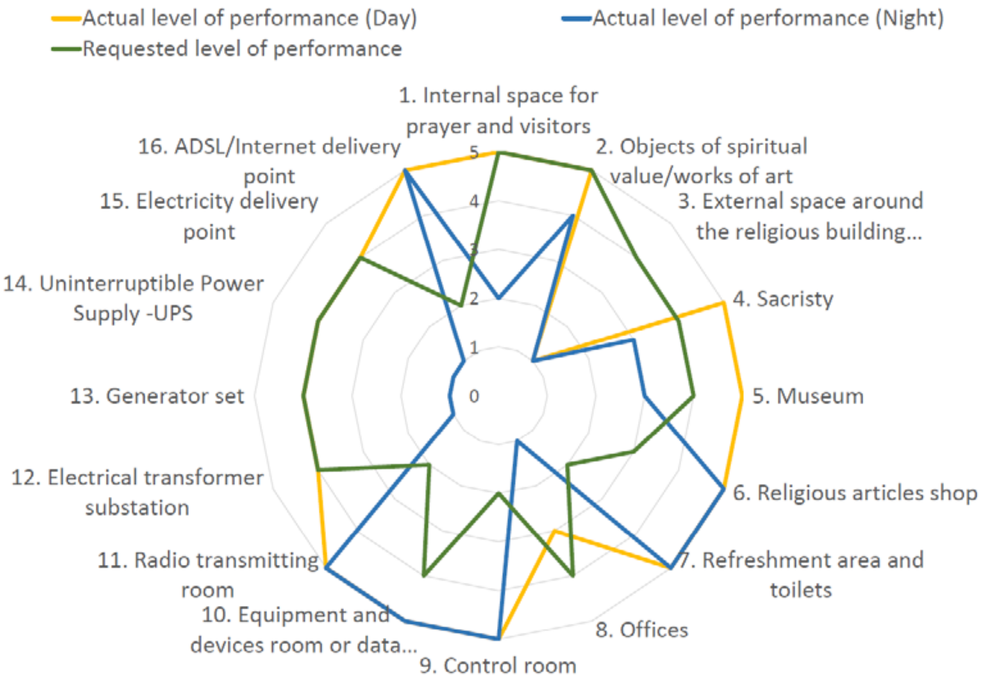


Figure 4: Radar graph of the results.

5 CONCLUSIONS

The proposed RARB methodology embodies a wide-ranging technique suitable for any type of religious site and permits one to estimate, in a rather fast and effective mode, the level of physical security risks and the associated countermeasures, intended as layers of protection, required to reach the wanted protection level, if necessary, as it happened in plenty of real contexts where it was previously applied. The given results allow providing solutions characterized by an optimal ratio from the cost/benefit point of view. Furthermore, it results to be useful and suitable in a multitude of other cultural heritage sites.

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

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