International Journal of Computational Methods and Experimental Measurements
Vol. 11, No. 1, March, 2023, pp. 45-54
Journal homepage: http://iieta.org/journals/ijcmem

# New Security Risk Assessment and Genetic Algorithms Based Methods to Optimize Risk Reduction Countermeasures for Cultural Heritage Sites

Fabio Garzia[1,2,3]

[1] Safety & Security Engineering Group, DICMA, Sapienza University of Rome, Rome 00185, Italy
[2] Wessex Institute of Technology, Ashurst, Southampton SO407AA, UK
[3] European Academy of Sciences and Arts, Salzburg 5020, Austria

Corresponding Author Email: fabio.garzia@uniroma1.it

https://doi.org/10.18280/ijcmem.110106

**Received:** N/A
**Accepted:** N/A

***Keywords:***
*cultural heritage sites, genetic algorithms optimization, risk assessment, risk analysis, risk reductions, safety, security, security countermeasures*

**ABSTRACT**

Cultural heritage sites are exposed to a variety of risks, for instance, by robbery, vandalism, harming, terrorism, and cyber attacks, which might damage people and cultural heritage place.

For this motive, it is necessary to plan appropriate countermeasures to prevent the above risks and to protect them using intrusion detection, access control, video surveillance, communication systems, cybersecurity devices and solutions, security personnel, and procedures properly mixed to attain an integrated system or solution.

In this paper, a new security risk assessment method for cultural heritage sites (SRACHS) is presented, showing as a case study, without any loss of its wide pertinence, its application to a museum. Further, a proper genetic algorithms (GAs)-based methodology to optimize risk reduction countermeasures is presented.

The proposed security risk assessment methodology allows for obtaining the correct amount of security defences (intrusion detection system, access control, video surveillance, communication devices, security personnel, etc.) that a desired cultural heritage place necessitates and the associated characteristics which depend on the probable targets that can be attacked.

It also avoids of overestimating the risks as in the situation of planning unnecessary protective countermeasures that sometimes cannot be needed, thus reducing the connected extra expenses, as properly demonstrated by the GAs-based methodology to optimize risk reduction countermeasures proposed in this paper.

## 1. INTRODUCTION

Cultural heritage sites are exposed to a variety of risks, for instance, by robbery, vandalism, harming, terrorism, etc., which may damage people and cultural heritage place.

For this motive, it is necessary to plan appropriate countermeasures to prevent the above risks and to protect these sites using intrusion detection, access control, video surveillance, communication systems, security personnel, and procedures properly mixed to attain an integrated system or solution [1, 2]. Taking into consideration the devices and installations, it is also vital them to be appropriately powered and to be able to communicate the data and information required for a proper security managing. This involves that power suppliers and transmission devices and networks have to be appropriately secured to prevent potential attacks versus them that might harm the operations of integrated technologies utilized and therefore leave the entire site exposed to extreme risks [3].

For this reason, it is crucial to estimate all the probable risks to select the appropriate countermeasures that have to be applied versus any possible malevolent activity. If security systems are already present, their suitability have also to be evaluated any time the risk context modifies [4, 5].

Risk assessment is very important in cultural heritage sites, and different methods have been proposed such the one suggested by CCI (Canadian Conservation Institute) and ICCROM (International Centre for the Study of the Preservation and Restoration of Cultural Property) named ABC method based on the three ABC components for quantification of risk, where ABC scales are represented by frequency of rate (A scale), loss of value to each affected item (B scale), and items affected (C scale) [6].

Security countermeasures following a proper risk assessment are not so simply to be applied as it has been demonstrated that the responsibility to ensure public access, stimulate art appreciation, and safeguard collections represent a conflict of interest between professionals working in museums that continue to challenge the development of preventative measures [7].

Terrorism can also affect cultural heritage sites and the counter-terrorism security measures at museums represent a form of securitization, after a proper highlighting of risk and related management [8].

Archives represent a particular type of cultural heritage sites characterized by different kind of risks that have been analysed, such a study made to detail what actions have been taken at The National Archives UK to improve issues such as

environmental conditions within storage areas, mitigating risk of physical damage to documents from handling, policies on the use of archival microfilm masters, and to reduce damage and loss of original records by substitution copying [9].

Even the Canadian Museum of Nature developed a risk model for preventive conservation that has proven helpful in application to a Portuguese archive. The work utilizes this model to assess the magnitudes of precise risks estimated for this same archive collection when located in either of two pairs of storage rooms. These rooms are in two different parts of this building: two are in an older part and two are in a recent addition. It was, therefore, necessary to assess the building itself, both structurally and environmentally, as well as analyse its common human practices. In terms of the overall risk magnitude, the best room was found to be in the recent building and the worst in the older building. However, the risks related to water problems were found to be higher in the new building. In this work, cost-free measures and easy to implement recommendations are given in order to improve the quality of the storage rooms [10].

Between the different proposed method, there are also specific methodology such as QuiskScan, a quick risk scan, which yields an overview over a collection, its values, and the vulnerabilities with comparatively modest effort. The QuiskScan utilizes a matrix-based approach to map value and vulnerability to the agents of deterioration for different collection units to highlight where considerable losses to the collection might occur. Like other risk assessment approaches, the QuiskScan involves expert input from across the organization thus helping to create a shared insight into the collection and an institutional awareness of risks. The method should be regarded as a tool that fits in between relying on best practice and conducting a comprehensive risk assessment [11].

Another method is represented by CPRAM (Cultural Property Risk Analysis Model), which was developed to guide priorities for resource allocation to preventive conservation under conditions of uncertainty. This model recognizes the preservation system as a subsystem within a collection management system, which, in turn, nests within progressively broader systems. Within this set of systems and subsystems, the contribution of preventive conservation to the continuance and betterment of humanity is recognized. Carefully defining the scope of the preservation system ensures clear understanding of interactions with surrounding systems. The risk analysis model then disaggregates risk through hierarchies both of sources of risk and of divisions of collections. The level of technical risk analysis varies throughout these hierarchies depending on the potential significance of the disaggregate portion considered. This approach makes the entire modelling process as efficient as possible [12].

CPRAM was employed by the American Museum of Natural History (AMNH) to identify a complete picture of its collections priorities and is accomplishing an overall risk assessment of its research, exhibit, and library/archive collections. The assessment model used for this three-phase project is based on the CPRAM and adapted to accommodate the specific needs of a large, complex institution. These assessments have provided AMNH administrators with information crucial to making long-term strategy and policy decisions about reducing and mitigating risks to collections [13].

CPRAM was also employed by the Royal British Columbia Museum (RBCM) that has a large and precious collection of archival records, artifacts, specimens, and associated information pertaining to the Province of British Columbia's human and natural history. In 2004 and again in 2010, the RBCM performed a comprehensive risk assessment to identify and quantify the potential impact of threats to the collections. Methodology was based on the CPRAM. The RBCM risk assessment projects, which involved over 30 staff members, were each completed over a period of several months. The results of the latest comprehensive review provided a corporate-wide perspective of the risks to the collection. Some risk-related assumptions were confirmed and new issues came to light. As a result of these risk assessments, a Risk Management Implementation Plan has been developed to address the most damaging and imminent threats to the collections [14].

CPRAM was also utilized by the Denver Museum of Nature & Science's (DMNS) risk assessment estimated hazards for the collections in storage using it to structure a comprehensive assessment and calculate magnitude of risk (MR). MR is the fraction of collection value expected to be lost given one hundred years exposure to current conditions. The MR is the simple product of four variables (Fraction Susceptible [FS], Loss in Value [LV], Probability [P], and Extent [E]) that are multiplied as follows: $MR=FS\times LV\times P\times E$. Using this approach, the DMNS could derive proper collections preservation strategies that results in safe and more accessible storage of the 1.4 million objects the museum holds in public trust [15]. In this paper, a new security risk assessment method for cultural heritage sites (SRACHS) is presented, showing as a case study, with any loss of its wide pertinence, its application to a museum. Further, a proper genetic algorithms (GAs)-based methodology to optimize risk reduction countermeasures is presented. The proposed security risk assessment methodology allows for obtaining the correct amount of security protections (intrusion detection system, access control, video surveillance, communication devices, security personnel, etc.) that a desired cultural heritage place necessitates and the associated characteristics depending on the possible targets that can be attacked. It also avoids overestimating the risks as in the instance of planning unnecessary protective countermeasures that sometimes is not needed, thus reducing the connected extra expenses, as properly demonstrated by the GAs-based methodology to optimize risk reduction countermeasures.

It also represents a new technique with respect to other security risk assessment techniques for heritage sites [6-15]. As a matter of fact, it employs an appropriate introductory risk assessment to go on further, estimating the degree of defence of every target correlated to each threat, properly aided by the GAs-based method. So, it provides supplementary worthwhile knowledge, as shown in the following.

## 2. THE SECURITY RISK ASSESSMENT METHOD

The proposed methodology of security risk assessment employed for cultural heritage sites (SRACHS) exemplifies a specific use acquired from the Physical Security Adapted Layer of Protection Analysis (PSA-LOPA) methodology [16-19]. It permits of attaining the right amount of security defences (video surveillance, access control, intrusion detection system, etc.) that a specified location necessitates and the connected characteristics. It also aids the expert in avoiding risk overvalue, preventing the realization of needless protective countermeasures, which occasionally can be useless,

hence diminishing any unneeded expenses.

For these motives, the right use of the SRACHS method represents an efficient and valuable scrutiny methodology to evaluate not only which security protections (SPs) the considered cultural heritage place requires to be categorized as suitably sheltered but principally if the present SPs are indispensable and satisfactory.

To attain the security risk evaluations, it is required to evaluate how the current SPs are capable of reducing the likelihood of incidence of the scenario, creating the notion of 'credit'. The sense of credit is connected to the possibility of failure (Probability of Failure on Demand [PFD]), related to each specific SPi, according to the next equation [19]:

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

Afterward that the diverse credits have been estimated, the PSA-LOPA evaluation [17] is attained with the estimation of the risk coefficient, associated to the k scenario, using the equation properly simplified for the considered context, without any loss of generality [19]:

$$R_k = TF_k - \sum_{i(k)} \text{credits}(IPL)_{i(k)} \quad (2)$$

where TF is the Target Factor, IPLs are the Independent Protection Layers that, in the considered context, symbolize the security defences, or levels of protections, that security attacks trigger in the considered k scenario characterized by a risk coefficient $R_k$.

Security is normally utilized applying the notion of layers of protection as any intruder clash with diverse layers of defences as perimeter protection, video surveillance, technological barriers, sensors, etc., before achieving the wanted objective. This justifies the aptness of LOPA when properly adapted, seeing the diverse layers of protection as a kind of sequential defences to avoid an aggressor to reach a particular objective, producing the estimated damages.

**Table 1.** Outline 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 | | |

**Table 2.** Interaction matrix targets - security protections in the considered museum ('X' means the presence and '-' means the absence)

| Target | Type 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 | −/− | −/− |
| Warehouse | X/X | X/X | X/X | X/X | X/− |
| Control room | X/X | −/− | X/X | −/− | X/X |
| Data centre | X/X | X/X | X/X | −/− | −/− |
| Main electrical power room | X/X | X/X | −/− | −/− | −/− |
| Generator set | X/X | X/X | −/− | −/− | −/− |
| Uninterruptible power supply | X/X | X/X | −/− | −/− | −/− |
| Air conditioning central device | X/X | −/− | −/− | −/− | −/− |
| External electrical power delivery point | X/X | −/− | −/− | −/− | X/− |
| External data network delivery point | X/X | −/− | −/− | −/− | X/− |
| Central radio transmitter | X/X | X/X | −/− | −/− | −/− |

In the present work, technological defences are exclusively considered even if the proposed methodology can be extended by considering physical barriers and also human factor [20] that represents vital elements for security management.

Initially, it is mandatory to categorize the damage stages and the required level of performances of the security protections for the associated security risks, and these activities are definite of a considered location of a given organization. An instance is illustrated in Table 1, where also the impact scale (IS) and the reliability of security solution (RSS) are included.

The proposed security risk assessment methodology for cultural heritage sites (SRACHS), showed in the following, expresses a suitable enhancement and modification of PSA-LOPA. Further details about adaptation and modification of PSA-LOPA can be found in reference [18].

Cultural heritage places are exposed to specific risks, for instance, by robbery, vandalism, harming, terrorism, etc. that can harm both people and the cultural heritage place. Hence, appropriate activities are required for risk prevention and protection, such as intrusion detection, access control, video surveillance, communication systems, security personnel, and procedures suitably combined to attain an integrated system or solution [1-3]. Moreover, these tools can be aptly combined to ensure the safety distance between people, when required, during pandemic and post pandemic periods.

The significant elements that are typically existing in a cultural heritage place, such as, for instance, a museum, and that may be conceivable aims of deliberate attacks are symbolized 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, warehouse, control room, data centre, main electrical power room, generator set, uninterruptible power supply (UPS), air conditioning central device, external electrical power delivery point, external data network delivery point, and central radio transmitter.

As a case study, a general museum is considered without losing generalization with respect to other type of cultural heritage sites. For the analysis, it is assumed that in the museum all the objectives previously determined are existing, and that external and internal video surveillance, access control, intrusion detection and security personnel equipped with radio are utilized to defend them. Other defences that can be employed as additional security shields, if necessary, are ignored now. For the subsequent analytical computation, these security shields are considered as being characterized by mean technical/operative features of commercial devices (that are not indicated for brevity).

A summary of the situation for day and night is illustrated in Table 2 (interaction matrix targets - security protections), where ‘internal exhibit room’ embodies the i-th room of the museum and ‘work of art(j) of exhibit room(i)’ embodies the j-th exposed element of room(i). As there can be several works of art in the various exhibition rooms, these two objectives must be replicated in Table 2, a number of times equivalent to the number of various works of art shielded by distinct levels of protection, if they are involved by various layers of defences. If the levels of defences are the same for all the exposition rooms and associated works of art, they have to be counted only one time. Using this approach, it is feasible to attain a detailed evaluation as it is feasible to consider the levels of protection of every work of art, which can be diverse as a function of its worth.

**Table 3.** Table of interaction matrix impact on targets - threats for the considered museum

| Target | Vandalism | Physical violence against people and / or objects | Damage | Sabotage | Espionage | Theft | Arson | Robbery | Explosive device | Terrorist attack | Cyber attack | Rounded mean value |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **External space around the site** | 7 | 6 | 7 | 7 | 2 | 7 | 7 | 6 | 8 | 8 | 6 | 7 |
| **Entrance hall** | 8 | 8 | 7 | 7 | 2 | 7 | 8 | 8 | 10 | 10 | 6 | 8 |
| **Ticket office** | 8 | 8 | 7 | 7 | 6 | 8 | 8 | 9 | 8 | 8 | 8 | 8 |
| **Coffee shop** | 8 | 8 | 7 | 7 | 2 | 6 | 8 | 6 | 8 | 8 | 4 | 7 |
| **Toilets** | 7 | 8 | 7 | 7 | 2 | 6 | 8 | 3 | 8 | 8 | 2 | 6 |
| **Shop** | 8 | 8 | 7 | 3 | 3 | 8 | 8 | 6 | 8 | 8 | 4 | 7 |
| **Luggage depot** | 4 | 8 | 6 | 3 | 3 | 7 | 8 | 8 | 8 | 8 | 4 | 7 |
| **Internal exhibit room(i)** | 9 | 9 | 9 | 8 | 5 | 9 | 10 | 10 | 10 | 10 | 6 | 9 |
| **Works of art(j) of the exhibit room(i)** | 10 | 10 | 10 | 8 | 5 | 10 | 10 | 10 | 10 | 10 | 8 | 10 |
| **Offices** | 7 | 8 | 7 | 7 | 7 | 8 | 8 | 8 | 9 | 9 | 9 | 8 |
| **Warehouse** | 9 | 9 | 9 | 9 | 4 | 9 | 10 | 9 | 9 | 9 | 8 | 9 |
| **Control room** | 9 | 9 | 9 | 9 | 8 | 8 | 10 | 8 | 10 | 10 | 10 | 10 |
| **Data centre** | 9 | 9 | 9 | 9 | 8 | 8 | 10 | 8 | 10 | 10 | 10 | 10 |
| **Main electrical power room** | 9 | 9 | 9 | 8 | 4 | 8 | 9 | 8 | 10 | 9 | 9 | 9 |
| **Generator set** | 10 | 9 | 10 | 10 | 7 | 8 | 10 | 8 | 10 | 9 | 9 | 10 |
| **Uninterruptible power supply** | 10 | 9 | 10 | 10 | 7 | 8 | 10 | 8 | 10 | 9 | 9 | 10 |
| **Air conditioning central device** | 8 | 9 | 8 | 7 | 6 | 8 | 7 | 7 | 8 | 8 | 8 | 8 |
| **External electrical power point delivery** | 8 | 8 | 9 | 9 | 6 | 9 | 8 | 8 | 9 | 9 | 9 | 9 |
| **External data network delivery point** | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 |
| **Central radio transmitter** | 9 | 8 | 9 | 8 | 8 | 6 | 10 | 7 | 8 | 9 | 9 | 9 |

Since technological support provided, for example, by control room, data centre, main electrical power room, generator set, UPS, air conditioning central device, external electrical power point delivery, external data network delivery point, and central radio transmitter are fundamental for the correct operativity and the security functionality of the different targets individuated, a proper matrix, named interaction matrix targets - technological supports for security functionality, is derived, not shown here for lacking of space.

In this table, all the targets are related to the different technological supports, that are specific for each museum or cultural heritage site, indicating their essentiality for each target. This table of pondering allows to consider, in the following phase, the impact of a possible attack against the technological supports since their interruption could provoke cascade effects on the correct functionality, including security, of the other targets and therefore for the whole site.

**Table 4.** Resuming table of SRACHS method outcomes for the considered museum

| Target | Damage confrontable by the actual level of protection (day) | Damage confrontable by the actual level of protection (night) | Estimated damage |
|---|---|---|---|
| 1. External space around the site | HIGH | NEGLIGIBLE | HIGH |
| 2. Entrance hall | MODERATE | NEGLIGIBLE | HIGH |
| 3. Ticket office | SEVERE | MODERATE | HIGH |
| 4. Coffee shop | HIGH | NEGLIGIBLE | HIGH |
| 5. Toilets | NEGLIGIBLE | NEGLIGIBLE | MODERATE |
| 6. Shop | HIGH | NEGLIGIBLE | HIGH |
| 7. Luggage depot | HIGH | HIGH | HIGH |
| 8. Internal exhibit room(i) | LIMITED | LIMITED | SEVERE |
| 9. Work of art(j) of the exhibit room(i) | SEVERE | SEVERE | SEVERE |
| 10. Offices | MODERATE | MODERATE | HIGH |
| 11. Warehouse | SEVERE | SEVERE | SEVERE |
| 12. Control room | SEVERE | SEVERE | SEVERE |
| 13. Data centre | SEVERE | SEVERE | SEVERE |
| 14. Main electrical power room | LIMITED | LIMITED | SEVERE |
| 15. Generator set | NEGLIGIBLE | NEGLIGIBLE | SEVERE |
| 16. Uninterruptible power supply | NEGLIGIBLE | NEGLIGIBLE | SEVERE |
| 17. Air conditioning central device | NEGLIGIBLE | NEGLIGIBLE | HIGH |
| 18. External electrical power delivery point | LIMITED | NEGLIGIBLE | SEVERE |
| 19. External data network delivery point | MODERATE | NEGLIGIBLE | HIGH |
| 20. Central radio transmitter | LIMITED | LIMITED | SEVERE |

| Target | Actual level of performance (day) | Actual level of performance (night) | Requested level of performance |
|---|---|---|---|
| 1. External space around the site | 4 | 1 | 4 |
| 2. Entrance hall | 3 | 1 | 4 |
| 3. Ticket office | 5 | 3 | 4 |
| 4. Coffee shop | 4 | 1 | 4 |
| 5. Toilets | 1 | 1 | 3 |
| 6. Shop | 4 | 1 | 4 |
| 7. Luggage depot | 4 | 4 | 4 |
| 8. Internal exhibit room(i) | 2 | 2 | 5 |
| 9. Work of art(j) of the exhibit room(i) | 5 | 5 | 5 |
| 10. Offices | 3 | 3 | 4 |
| 11. Warehouse | 5 | 5 | 5 |
| 12. Control room | 5 | 5 | 5 |
| 13. Data centre | 5 | 5 | 5 |
| 14. Main electrical power room | 2 | 2 | 5 |
| 15. Generator set | 1 | 1 | 5 |
| 16. Uninterruptible power supply | 1 | 1 | 5 |
| 17. Air conditioning central device | 1 | 1 | 4 |
| 18. External electrical power delivery point | 2 | 1 | 5 |
| 19. External data network delivery point | 3 | 1 | 4 |
| 20. Central radio transmitter | 2 | 2 | 5 |

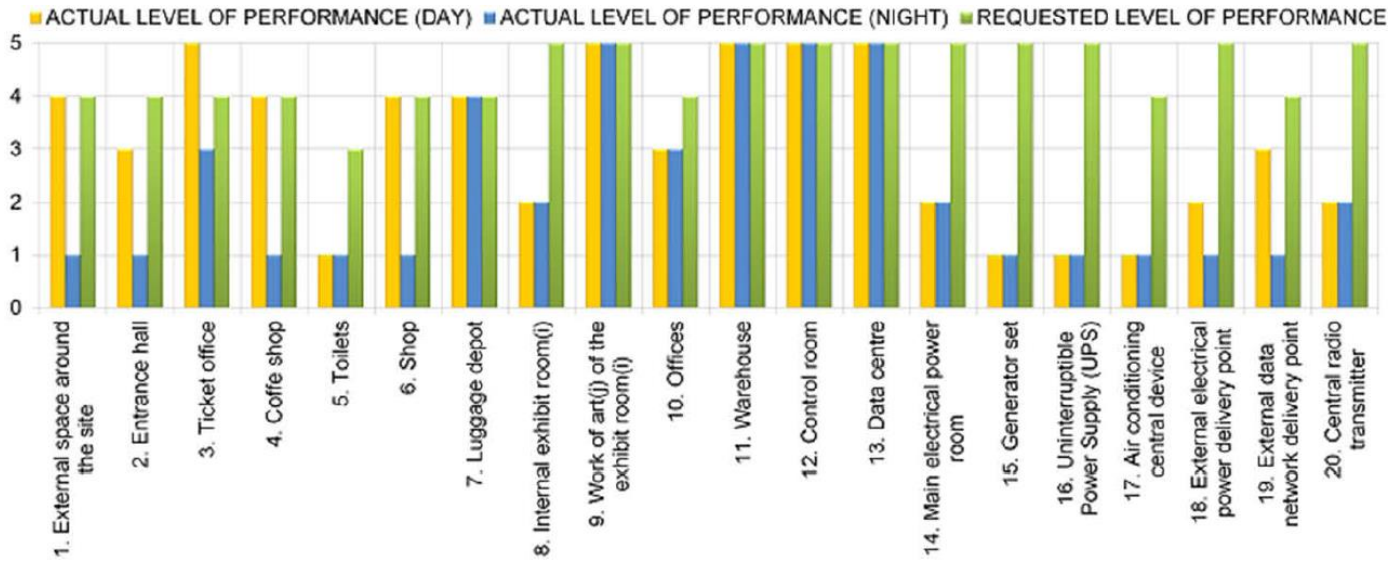


**Figure 1.** Histogram graph of the attained results

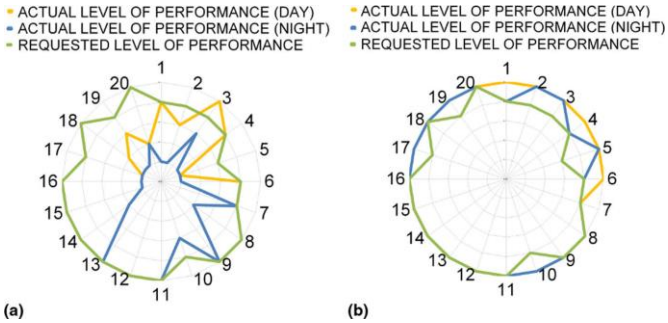


**Figure 2.** Radar graph of the obtained results: before (a) and after (b) adding further protections

All the needed information to make an opening analysis have been acquired utilizing opensource data accessible on the Internet. In this way, also using the results of Table 2, it has been feasible to create the interaction matrix impact on targets - threats for the considered place whose results are illustrated in Table 3, where the mean values of every objective are rounded to the upper integer to utilize a cautionary approach.

It is now possible to proceed with the calculation following the different steps illustrated previously, remembering that mean values of every objective of Table 3 are considered as the related TF and they embody the estimated damage and the correlated requested level of performance in Table 4, after appropriate mathematical transformation through Table 1 and IS. The results of Table 4 are shown in Figures 1 and 2a.

Figures 1 and 2(a) show that, excluding targets 7, 9, 11, 12, and 13, targets are classified with an actual level of performance (similarly across the day and the night or only across one of them) that are lesser than the demanded level of performance. In certain situations, the night decrease depends on the lack or the lessening of security personnel equipped with radiocommunication devices. This indicates that there is a need to increase the number of levels of security shields, adding one or more for each of them.

It can be solved by adding, for instance, a fitting intrusion detection system, thermal camera, motion detection, video analysis, or another sort of protection.

If proper reinforcement shields are added, it is conceivable to check, reiterating the calculation procedure, if the improved actual level of protection (similarly in the day and in the night) reaches, or in some circumstances surpasses, the demanded level of protection, ensuring the fitting security shielding of each target of the considered museum. Adding, for example, thermal camera (TC) to target 1; TC and intrusion detection (ID) to target 2; ID to targets 3 and 4; ID and security personnel (SP) to target 5; ID to target 6; TC to target 8; ID to target 10; access control (AC) to targets 14, 15, and 16; AC and ID to target 17; TC and ID to targets 18 and 19; and AC to target 20, it is possible to verify, reiterating again the computation procedure, that now all targets are properly shielded and in some cases over shielded - thanks to the cumulative effect of the added protections, as shown in Figure 2(b).

Similar results can be obtained using different combinations of additional protections, always considering appropriately the cost/benefit ratio.

## 3. THE GAS-BASED TECHNIQUE TO OPTIMIZE RISK REDUCTION COUNTERMEASURES

From what we have seen so far, it is evident how the process of finding the best countermeasures to apply, always optimizing costs, when the number of targets to be protected or the number of countermeasures that can be used start to be very large, can represent a problem of difficult resolution.

Due to the nonlinear nature of the problem, GAs [21-23] can be used, translating the problem to be solved in a proper way. The GAs encode each parameter of the problem to be optimized into a proper sequence (where the alphabet utilized is generally binary) named a gene and combine the different genes to form a chromosome. A suitable set of chromosomes, named a population, undergoes the Darwinian processes of natural selection, mating and mutation, creating new generations, until it achieves the final optimal solution under the selective pressure of the chosen fitness function. Terminologies related to GAs are: Population - a subset of possible solutions; Chromosomes - one of the solutions in the population; Gene - an element in the chromosome; Fitness Function - a function utilizing a precise input to reach an improved output; and Genetic operators - the best individuals mate to reproduce an offspring that is better than the parents. Genetic operators are employed to modify the genetic

composition of the next generation.

Initially, it is necessary to identify the possible levels of protection that can or want to be used to protect the various targets. Subsequently, it is necessary to evaluate their cost C and the related PFD. The information related to the costs $C_{i,j}$ of the various protections $P_i$ on the different targets $T_j$ are stored in a proper array named cost of protections (CP) of dimensions $N_P \times N_T$, where $N_P$ is the number of protections and $N_T$ is the number of targets, while the information related to the PFD of the layers of protection are stored in a proper array PFDP whose dimension is $N_P \times 1$. An example of CP array is shown in Table 5.

Risks and TF, deriving from application of SRACHS, are stored in proper arrays named R and TF, respectively, of dimensions $N_T \times 1$ each, where NT is the number of targets.

The information related to the applicability $A_{i,j}$ of the various protections Pi on the different targets $T_j$ are stored in a proper array named applicability of protections on targets (APT) of dimensions $N_P \times N_T$, where NP is the number of protections. This array is composed by binary values, where a binary 1 in the position $A_{i,j}$ indicates that the protection Pi is applicable to target $T_j$, while it is not applicable for a binary value equal to 0.

In this context, it is also important to consider that a possible protection can be useful for protecting multiple targets. A possible example is represented by video surveillance that protects the environment and, at the same time, also the works of art contained in it, if the latter have been considered among the targets. The same considerations apply to access control at the entrance of an environment containing works of art or other possible targets. For this reason, the information related to the interaction $IPT_{i,j,k}$ of the protection Pi on the target $T_j$ with the other target $T_k$ is stored in a proper array named interaction of protections on targets (IPT) of dimensions $N_P \times N_T \times N_T$, where $N_P$ is the number of protections and NT is the number of targets. This array is composed by percentage values, variable between 0% and 100%, where the value in the position $IPT_{i,j,k}$ indicates the percentage of protection ensured to target Tk by protection $P_i$ applied to target $T_j$. For computation reasons explained later, the value of $IPT_{i,j,k}$ is set to zero when $j=k$ as the related information of protection Pi on the target $T_j$ with the same target $T_j$ is already stored in the PFDP array.

**Table 5.** Example of a cost of protections array (CP). $C_{i,j}$ embodies the cost of the protection *I* for the target *j*

| Protection | Target (1) | Target (2) | ... | Target ($N_T$-1) | Target ($N_T$) |
|---|---|---|---|---|---|
| P(1) | $C_{1,1}$ | $C_{1,2}$ | ... | $C_{1,NT-1}$ | $C_{1,NT}$ |
| P(2) | $C_{2,1}$ | $C_{2,2}$ | ... | $C_{2,NT-1}$ | $C_{2,NT}$ |
| … | ... | ... | ... | ... | ... |
| P($N_P$-1) | $C_{NP-1,1}$ | $C_{NP-1,2}$ | ... | $C_{NP-1,NT-1}$ | $C_{NP-1,NT}$ |
| P($N_P$) | $C_{NP,1}$ | $C_{NP,2}$ | ... | $C_{NP,NT-1}$ | $C_{NP,NT}$ |

**Table 6.** Encoding scheme of the generic gene '*j*'

| Gene '*j*' (components) | Considered variable | Variability interval | Kind of variable | Number of bits |
|---|---|---|---|---|
| 1 | Protection P1 on target Tj | 0÷1 | Binary | 1 |
| 2 | Protection P2 on target Tj | 0÷1 | Binary | 1 |
| ... | ... | ... | ... | 1 |
| NP − 1 | Protection PNP−1 on target Tj | 0÷1 | Binary | 1 |
| NP | Protection PNP on target Tj | 0÷1 | Binary | 1 |

It is now possible to define the data structure of the chromosome that is composed of a number of genes which is identical to the number of targets NT. Every gene, associated with protections on a precise target, is encoded as a series of binary numbers indicating if the considered protections are active on the considered target (binary 1) or not (binary 0). The number of elements that compose each gene is therefore equal to $N_P$. In Table 6, the encoding of the generic gene *j* is indicated, where *j* is variable between 1 and $N_T$ and $T_j$ is the generic target *j*. Every chromosome, or individual I, representing a potential solution of the problem, is comprised of a binary string, which represents the possible protections P on the targets *T*. The overall length of each chromosome, or individual I of the population, is equivalent to $N_P \times N_T$. The general fitness function $f(I)$ (where *I* represents the generic individual or chromosome of the population) for this kind of problem is composed by two components representing the cost and the risk reduction, respectively, and embodied by:

$$f(I) = \operatorname{argmin}\left\{ \alpha \left[ \sum_{i=1}^{N_T} \sum_{j=1}^{N_P} I_{i,j} * C_{i,j} \right] / C_{MAX} + \right.$$
$$\left. + \beta \left\{ \sum_{i=1}^{N_T} \left[ TF_i - \log\left( \sum_{j=1}^{N_P} I_{i,j} * PFD_{i,j} + \sum_{m=1}^{N_T} \sum_{n=1}^{N_P} I_{m,n} * PFD_{m,n} * IPT_{m,n,j} \right) \right] \right\} / R_{MAX} \right\} \quad (3)$$

where $I_{i,j}$ is the binary value of element '*i*' of gene '*j*' of individual *I*; $C_{i,j}$ is the cost of protection $P_i$, on the target $T_j$; $TF_i$ is the target factor associated to target $T_i$; $PFD_{i,j}$ is the probability of failure on demand of protection Pi, on the target $T_j$; $IPT_{m,n,i}$ is the interaction of the protection Pm on the target Tn with the other target $T_i$; $C_{MAX}$ is the cost of all the protections applied to all targets; $R_{MAX}$ is the level of risk evaluated for all the targets without any protection. As it is possible to see from Eq. (3), $I_{i,j}$ is present in all the terms of it as it is related to the presence or less of protections on targets represented by the generic individual *I* of population to be optimized. Further, the second part of Eq. (3) related to risk

reduction is composed by the first part related to direct protections on the targets and by the second part related to interaction of protections of targets on the other targets. $\alpha$ and $\beta$ are two parameters that vary between 0 and 1, where $\beta$=1-$\alpha$, so that it is possible to give more importance to the first term (reduction of cost, when $\alpha$ tends to 1) or to the second term (reduction of level of risk of targets, when $\alpha$ tends to 0) or to both of them (when $\alpha \approx 0.5$).

The fitness function represented by Eq. (3) can be computed only if the individual I represents an effective solution, which means that the different protections of the different targets represented by it can be really appliable: this is verified by means of the array named applicability of APT. If this does not happen, it is forced to be equal to 0, as the individual I does not correspond to an effective solution for the considered problem. Further, the fitness function represents a multi-optimization problem (two objects function - cost and risk). Consequently, the multi-objective optimization leads to a Pareto front [24] of the optimal solutions, for each value of $\alpha$ in the interval 0÷1, which is illustrated in the following.

The initial population is produced randomly. Once the population is recombined and mutated, the fitness function of the population is computed with the fitness function expressed by Eq. (3), considering only fitting individuals $I$ of the population. The convergence evaluation is done, estimating if the difference between the mean value of fitness functions of the acceptable individuals belonging to the actual generation and the mean values of the last $N_G$ generations is smaller than a definite percentage rate $p_{stop}$ that can be selected.

The GA has been tested on more than 500 real and random situations using a proper software code developed with Python [25], to obtain, as much as possible, general mean results valid to any sort of site. All of the results, achieved with quite fast converge, as described in the following, are attained with converge test parameters $N_G$ and $p_{stop}$ equal to 40 and 0.3, respectively. Further, the simulations were made considering a one-point crossover function characterized by a probability variable between 0.6 and 0.8, a mutation probability variable between 0.01 and 0.1 and different values of $\alpha$ variable in the interval 0÷0.25. Due to the huge amount of ultimate data attained and to the number of results that can be obtained from this huge amount of data, only the most considerable results are shown in the following, due to the limited space available. A significant parameter to be considered in obtaining noteworthy data is embodied by $IPT_{mean}$ that is the mean value of IPT. If this value is equal to 0, it means that every protection shields only every specific target. On the contrary, if it is equal to 1, it means that every protection of each specific target is able to protect all the other targets. The value of $IPT_{mean}$ depends on the kind of protections chosen to protect the targets of the considered site. An example of protection capable of increasing the value of $IPT_{mean}$ is represented by video surveillance that can be used, in certain zones and in certain situations, to protect more targets at the same time. It is evident that the greater $IPT_{mean}$ and the greater the GA chance of optimization, as will be shown in the following.

Another important parameter is represented by the cost ratio (CR), represented by the ratio between the cost of the protections offered by optimal individual I and the cost of all the protections applied to all targets $C_{MAX}$. It is evident that the greater CR and the greater the GA chance of optimization, as will be shown in the following.

It is also evident that if all the possible protections are utilized, and if the related calculation shown previously allows it, the total risk, embodied by the sum of all considered risks Ri, is reduced at the minimum level (i.e., a reduction value of 100%), while if no protections are utilized, the total risk remains at the maximum level (i.e., a reduction value of 0%). The total risk reduction (TRR), expressed as a percentage, can represent a valuable parameter to evaluate the optimization skills of the considered GA.

The TRR, expressed as a percentage, as a function of CR, for different values of $IPT_{mean}$ is shown in Figure 3. As it is possible to see from Figure 3, the GA is capable of usefully increasing the TRR (and therefore reduce the total risk) as a function of both CR and I $IPT_{mean}$, as expected. It is evident that, as CR increases, more protections can be utilized by GA for risk reduction, and the curves grow, according to different profiles, as a function of $IPT_{mean}$. It is also evident that the greater the $IPT_{mean}$ and the greater the GA chance of optimization. In fact, when $IPT_{mean}$ tends to 1 (maximum value reachable), each protection tends to shield every target and this allows the GA to achieve its maximum optimization capabilities, reaching TRR of 100% with investment ratio equal to about 0.45. When $IPT_{mean}$ tends to 0 (minimum theoretical value reachable), each protection can shield only one target and this does not allow the GA to best perform its optimization capabilities, reaching a TRR of 100% with CR equal to about 0.88. Anyway, even in this worst case, the GA is capable of guaranteeing a reduction of CR.

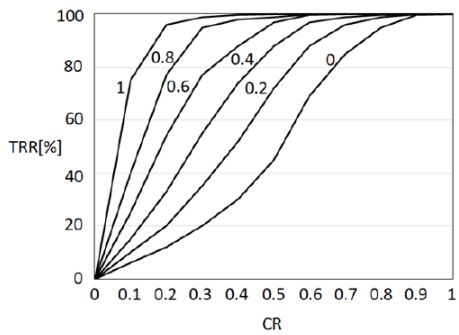


**Figure 3.** TRR, expressed as a percentage, as a function of CR, for different values of $IPT_{mean}$

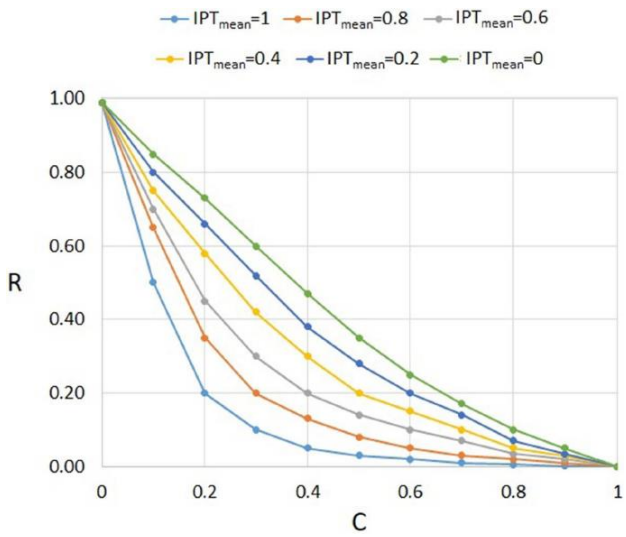


**Figure 4.** Pareto front of the optimal solutions for α varying in the interval 0÷1, for different values for different values of $IPT_{mean}$ (upper left side are the values obtained when $\alpha$ tends to 1, while lower right side are the values obtained when α tends to 0)

Regarding the multi-optimization features of fitness function represented by Eq. (3) (two object functions, cost C and risk R), the multi-objective optimization leads to a Pareto front of the optimal solutions. This aspect has been studied, as indicated previously, for each value of $\alpha$ in the interval 0÷1, and the results are illustrated in Figure 4.

The different curves of Figure 4 are related to different Pareto fronts obtained for different values of $IPT_{mean}$, since, as already illustrated previously, the greater the $IPT_{mean}$ and the greater the GA possibility of optimization.

As it is possible to see from Figure 4, when $\alpha$ tends to 1 (upper left side of Figure 4), that is the reduction of cost C is predominant with respect to the reduction of risk R in Eq. (3), the values of Pareto fronts provide values of risk R greater than 0.5, since, due to superior importance given to the economic resources and the consequent lesser importance given to the protections applicable for risk lessening, the GA is not driven at guaranteeing a great reduction of risk R.

On the contrary, when $\alpha$ tends to 0 (lower right side of Figure 4), that is the reduction of risk R is predominant with respect to the reduction of cost C in Eq. (3), the values of Pareto fronts provide values of risk R smaller than 0.1, since, due to lesser importance given to the economic resources available and the consequent greater importance given to the protections applicable for risk lessening, the GA is driven to guarantee a great reduction of risk R.

When $\alpha \approx 0.5$ (central part of Figure 4), that is the reduction of risk R has more or less the same importance of the reduction of cost C in Eq. (3), the values of Pareto fronts provide values of risk R variable between 0.6 and 0.1. The different values obtained for risk depends on different values of $IPT_{mean}$ since, as already illustrated, the greater the $IPT_{mean}$ and the greater the GA capability of optimizing the considered problem.

The number of generations required for the GA to achieve the final optimal solution embodies a very important parameter, together with the initial population, as it provides an indication of the calculation charge that, once associated to the processing resources available, delivers a precise information regarding the time needed to reach the wanted final optimal solution. This aspect has been analysed jointly with other aspects, but the findings cannot be shown due to the limited space available.

Anyway, the applied GA, thanks to its specific features, has proven to be able to scope the final optimal solutions, even in the worst cases, with a rather reduced number of generations and a rather reduced number of individuals of population, offering the wanted solution in a rapid and effective mode, even in the presence of limited processing resources.

## 4. CONCLUSIONS

A new security risk assessment method for cultural heritage sites (SRACHS) has been presented, illustrating as a case study, without any loss of its wide-ranging pertinency, its application to a museum. Further, a suitable GAs-based method to optimize risk reduction countermeasures has been presented.

The proposed security risk assessment method permits of achieving, in a rather quick and effective manner, the exact amount of security defences (intrusion detection system, access control, video surveillance, communication devices, security personnel, etc.) that a chosen cultural heritage site requires and the linked attributes which depend on the probable targets that might be attacked, as it occurred in a plenty of real contexts where it was used.

It also avoids of overestimating the risks as in the situation of forecasting needless protective countermeasures that sometimes cannot be required, thus reducing the related extra expenses, as properly demonstrated by the GAs-based methodology to optimize risk reduction countermeasures illustrated in this paper.

Further, the GAs-based methodology has demonstrated all its strength in this context, as it allows of optimizing cost/benefit ratio of necessary countermeasures as a function of risks assessed, letting chose in a proper range variable between minimum cost or maximum risk reduction. It also allows to consider the protective effect that a certain countermeasure related to a given target extends on the other targets, thus ensuring a higher degree of its optimizing capabilities.

The outcomes produced by the proposed combined method (risk assessment + GA) allow of finding results characterized by an optimal cost/benefit ratio.

## REFERENCES


[1] Garzia, F., Sammarco, E., Cusani, R. (2011). The integrated security system of the Vatican City State. International Journal of Safety and Security Engineering, 1(1): 1-17. https://doi.org/10.2495/SAFE-V1-N1-1-17

[2] Garzia, F. (2018). Implementing an Internet of Everything system in the archaeological area of Quintili's Villa in the Ancient Appia route park in Rome. WIT Transactions on the Built Environment, 174: 261-272. https://doi.org/10.2495/SAFE170241

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

[4] Broder, J.F., Tucker, G. (2011). Risk Analysis and the Security Survey. Elsevier.

[5] Norman, T.L. (2010). Risk Analysis and Security Countermeasure Selection. CRC Press.

[6] CCI/ICC and ICCROM (2016). The ABC Method, A risk management approach to the preservation of cultural heritage. Canadian Conservation Institute.

[7] Runhovde, S.R. (2021). Risking munch. The art of balancing accessibility and security in museums. Journal of Risk Research, 24(9): 1113-1126. https://doi.org/10.1080/13669877.2020.1801810

[8] Atkinson, C., Yates, D., Brooke, N. (2020). 'Now that you mention it, museums probably are a target': Museums, terrorism and security in the United Kingdom. Museum Management and Curatorship, 35(2): 109-124. https://doi.org/10.1080/09647775.2019.1683881

[9] Bülow, A.E. (2010). Collection management using preservation risk assessment. Journal of the Institute of Conservation, 33(1): 65-78. https://doi.org/10.1080/19455220903509960

[10] Pinheiro, A.C., Macedo, M.F. (2009). Risk assessment: A comparative study of archive storage rooms. Journal of Cultural Heritage, 10(3): 428-434. https://doi.org/10.1016/j.culher.2008.10.005

[11] Brokerhof, A.W., Bülow, A.E. (2016). The QuiskScan-A quick risk scan to identify value and hazards in a collection. Journal of the Institute of Conservation, 39(1): 18-28. https://doi.org/10.1080/19455224.2016.1152280

[12] Waller, R. (2004). Cultural property risk analysis model:

Development and application to preventive conservation at the Canadian Museum of Nature. APT Bulletin: The Journal of Preservation Technology, 35(4): 57. https://doi.org/10.2307/4126423
[13] Elkin, L. K., Nunan, E., Fenkart-Froeschl, D. (2013). The "collections risk management" program at the American Museum of Natural History. Collections, 9(1): 125-137. https://doi.org/10.1177/155019061300900111
[14] Lee, K., Castles, D. (2013). Collections risk assessment at the Royal BC Museum and Archives. Collections, 9(1): 9-27. https://doi.org/10.1177/155019061300900103
[15] Southward, J., Thorwald, H., Muething, G., Waller, R. (2013). Collections risk assessment at the Denver Museum of Nature & Science. Collections, 9(1): 71-92. https://doi.org/10.1177/155019061300900107
[16] Garzia, F., Lombardi, M., Fargnoli, M., Ramalingam, S. (2018). Psa-lopa-a novel method for physical security risk analysis based on layers of protection analysis. In 2018 International Carnahan Conference on Security Technology (ICCST), Montreal, QC, Canada, pp. 1-5. https://doi.org/10.1109/CCST.2018.8585593
[17] Garzia, F., Sammarco, E. (2020). New risk analysis methodology for religious buildings. WIT Transactions on Engineering Sciences, 129: 215-227. https://doi.org/10.2495/RISK200191
[18] Garzia, F. (2021). Novel risk assessment methodology for cultural heritage sites. WIT Transactions on The Built Environment, 203: 149-160 https://doi.org/10.2495/STR210131
[19] Willey, R.J. (2014). Layer of protection analysis. Procedia Engineering, 84: 12-22. https://doi.org/10.1016/j.proeng.2014.10.405
[20] Borghini, F., Garzia, F., Borghini, A., Borghini, G. (2016). The Psychology of Security, Emergency and Risk. WIT Press.
[21] Goldberg, D.E., Deb, K. (1991). Foundations of Genetic Algorithms. Morgan Kaufmann.
[22] Mitchell, M. (1992). An introduction to genetic algorithms. The MIT Press.
[23] Eiben, A.E., Smith, J.E. (2015). Introduction to Evolutionary Computation. Springer.
[24] Jahan, A., Edwards, K.L., Bahraminasab, M. (2013). Multi-Criteria Decision Analysis. Elsevier.
[25] Python, Python Software Foundation. (2002). www.python.org/