The New Communication Network for an Internet of Everything Based Security/Safety/General Management/Visitor's Services for the Papal Basilica and Sacred Convent of Saint Francis in Assisi, Italy

Mauro Gambetti
General Custody of Sacred Convent of Saint Francis in Assisi – Minor Conventual Friars
Assisi, Italy
&
Foundation for the Basilica of Saint Francis in Assisi
Assisi, Italy

Fabio Garzia
Safety & Security Engineering Group - DICMA
SAPIENZA – University of Rome
Rome, Italy
fabio.garzia@uniroma1.it
&
General Custody of Sacred Convent of Saint Francis in Assisi – Minor Conventual Friars
Assisi, Italy
&
Foundation for the Basilica of Saint Francis in Assisi
Assisi, Italy

Francisco Jesus Vargas Bonilla
Electronic Engineering Department, School of Engineering, SISTEMIC
Universidad de Antioquia
Medellin, Colombia

Davide Ciarlariello
General Custody of Sacred Convent of Saint Francis in Assisi – Minor Conventual Friars
Assisi, Italy

Miguel A. Ferrer
Universitario para el Desarrollo Tecnológico e Innovación en Comunicaciones
Universidad de Las Palmas de Gran Canaria
Gran Canaria, Spain

Sergio Fusetti
General Custody of Sacred Convent of Saint Francis in Assisi – Minor Conventual Friars
Assisi, Italy

Mara Lombardi
Safety & Security Engineering Group - DICMA
SAPIENZA – University of Rome
Rome, Italy

Soodamani Ramalingam
Division of Electronics, Communications and Electrical Engineering, School of Engineering and Technology
University of Hertfordshire
Hatfiled, UK

Mahalingam Ramasamy
Netcon Technologies India Private Limited
Coimbatore, India

Simone Sacerdoti
General Custody of Sacred Convent of Saint Francis in Assisi – Minor Conventual Friars
Assisi, Italy

Andrea Sdringola
General Custody of Sacred Convent of Saint Francis in Assisi – Minor Conventual Friars
Assisi, Italy

Devi Thirupati
Department of Computer Applications

Bharathiar University
Coimbatore, Tamil Nadu, India

Marcos Faundez Zanuy
ESUP Tecnocampus
Pompeu Fabra University
Mataró, Spain

***Abstract*—The Papal Basilica and the Sacred Convent of St. Francis in Assisi, Italy together represent a unique and specific cultural heritage site where the mortal remains of St. Francis have been housed since 1230 AD. Millions of pilgrims and visitors from all over the world visit this site each year. In 2000 AD, together with other Franciscan sites in the surrounding area, it achieved UNESCO World Heritage status. Unique and complex cultural heritage sites, such as this, require a significant effort to ensure visitor security and safety. Along with such needs are cultural heritage preservation and protection as well as accessibility for visitors, with particular reference to visitors with disabilities, and for personnel normally present for site management, including the Friar's community. These aims can be achieved using integrated systems and innovative technologies, such as Internet of Everything (IoE) which can connect people, things (mobile terminals, smart sensors, devices, actuators; wearable devices; etc.), data/information/knowledge and particular processes. The purpose of this paper is to illustrate the methodology and show the results obtained from the study and the design of a new communication network for Internet of Everything based security/safety/general management and visitors' services of the Papal Basilica and Sacred Convent of Saint Francis in Assisi.**

Keywords—Internet of Everything, IoE, Internet of Things, IoT, IoE/IoT integrated security system, IoE/IoT Cultural Heritage security, communication network security.

I. Introduction

The Papal Basilica and the Sacred Convent of St. Francis in Assisi, Italy together represent a unique and specific cultural heritage site where the mortal remains of St. Francis have been housed since 1230 AD.

Millions of pilgrims and visitors from all over the world visit this site each year. In 2000 AD, together with other Franciscan sites in the surrounding area, it achieved UNESCO World Heritage status.

Important international events, such as those related to world peace and dialogue between religions, are organized in this site and are often attended by thousands of people.

The Papal Basilica, where unique frescos by Giotto and other famous painters are displayed, comprises three stratified structures:

- the tomb of St. Francis, located at the lower level;

978-1-5386-1585-0/17/$31.00 ©2017 IEEE

- the lower Church, whose altar is just above the tomb of St. Francis; and
- the upper Church, located above the lower Church.

Inside the Sacred Convent there is a museum, a library and sufficient space for hosting spiritual and cultural activities.

Unique and complex cultural heritage sites, such as this, require a significant effort to ensure visitor security and safety. Along with such needs are cultural heritage preservation and protection as well as accessibility for visitors, with particular reference to visitors with disabilities, and for personnel normally present for site management, including the Friar's community.

Fig. 1. Panoramic view of Assisi.

Fig. 2. Panoramic view of the Papal Basilica and the Sacred Convent of Saint Francis in Assisi.

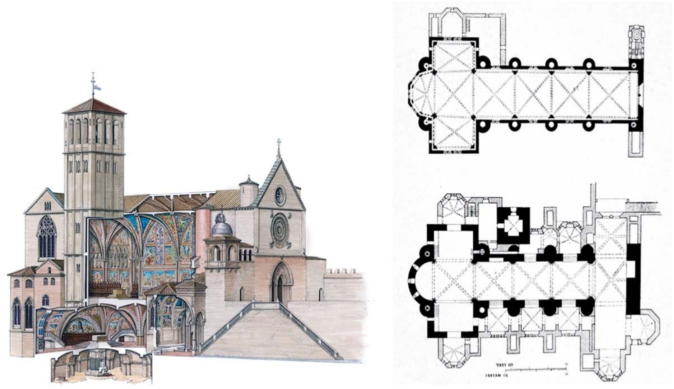


Fig. 3. View of the 3 layers of the Basilica (left) and the related plants (up-right: higher Basilica, down-right: lower Basilica)

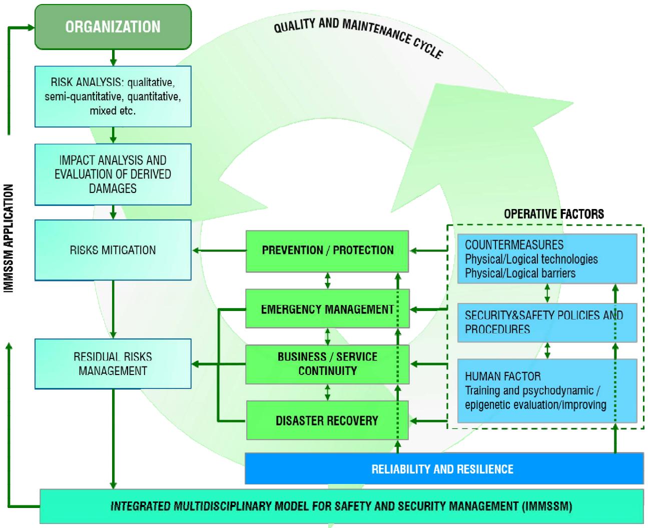
These aims can be achieved using integrated systems [1, 2] and innovative technologies, such as Internet of Everything (IoE) which can connect people, things (mobile terminals, smart sensors, devices, actuators; wearable devices; etc.), data/information/knowledge and particular processes [3, 4].

The IoE system must implement and support an integrated multidisciplinary model for security and safety management (IMMSSM) for this specific site [5].

The purpose of this paper is to illustrate the methodology and show the results obtained from the study and the design of a new communication network for Internet of Everything based security/safety/general management and visitors' services of the Papal Basilica and Sacred Convent of Saint Francis in Assisi.

II. The Integrated Multidisciplinary Model for Security and Safety Management (IMMSSM) and the Related IoE Based Integrated Technological System Framework (ITSF)

The IoE system must be able to implement and support an integrated multidisciplinary model for security and safety management (IMMSSM) [5] for the specific, peculiar and unique context, using a multidisciplinary approach whose scheme is shown in Fig.4.



ORGANIZATION
QUALITY AND MAINTENANCE CYCLE
RISK ANALYSIS: qualitative, semi-quantitative, quantitative, mixed etc.
IMPACT ANALYSIS AND EVALUATION OF DERIVED DAMAGES
IMMSSM APPLICATION
OPERATIVE FACTORS
RISKS MITIGATION
PREVENTION / PROTECTION
COUNTERMEASURES Physical/Logical technologies Physical/Logical barriers
EMERGENCY MANAGEMENT
SECURITY&SAFETY POLICIES AND PROCEDURES
RESIDUAL RISKS MANAGEMENT
BUSINESS / SERVICE CONTINUITY
HUMAN FACTOR Training and psychodynamic / epigenetic evaluation/improving
DISASTER RECOVERY
RELIABILITY AND RESILIENCE
INTEGRATED MULTIDISCIPLINARY MODEL FOR SAFETY AND SECURITY MANAGEMENT (IMMSSM)

Fig. 4. Scheme of the Integrated Multidisciplinary Model for Security and Safety Management (IMMSSM).

The IMMSSM can be implemented and supported using a proper Integrated Technological System Framework based on IoE (IoE-ITSF) which allows the full functionalities of the IMMSSM with high flexibility and modularity. In this way, it is possible to translate any eventual modification of the IMMSSM into a fast and low-cost modification of the ITSF at any time, ensuring always the best performances of IMMSSM.

The general scheme of the IoE based Integrated Technological System Framework (IoE-ITSF) is shown in Fig. 5.

Due to the presence of strong architectural restrictions, it is necessary to take particular care in the installation of wires and devices [6] and, for this reason, a proper laser scanning activity [7, 8] has already started to derive precious information that are going to be transferred in a proper BIM (Building Information Modelling) system that results to be a useful tool not only for safety and security management but also for a plenty of other goals [9].

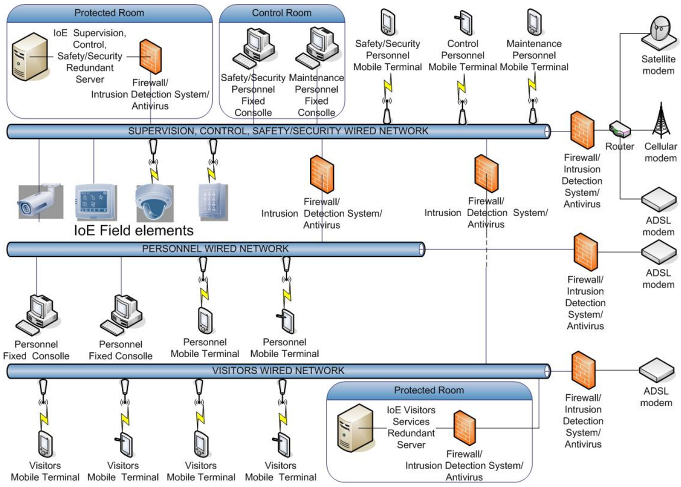

Protected Room
IoE Supervision, Control, Safety/Security Redundant Server
Firewall/ Intrusion Detection System/ Antivirus
Control Room
Safety/Security Personnel Fixed Consolle
Maintenance Personnel Fixed Consolle
Safety/Security Personnel Mobile Terminal
Control Personnel Mobile Terminal
Maintenance Personnel Mobile Terminal
Satellite modem
SUPERVISION, CONTROL, SAFETY/SECURITY WIRED NETWORK
Router
Cellular modem
Firewall/ Intrusion Detection System/ Antivirus
IoE Field elements
Firewall/ Intrusion Detection System/ Antivirus
Firewall/ Intrusion Detection System/ Antivirus
ADSL modem
PERSONNEL WIRED NETWORK
Firewall/ Intrusion Detection System/ Antivirus
ADSL modem
Personnel Fixed Consolle
Personnel Fixed Consolle
Personnel Mobile Terminal
Personnel Mobile Terminal
VISITORS WIRED NETWORK
Firewall/ Intrusion Detection System/ Antivirus
ADSL modem
Visitors Mobile Terminal
Visitors Mobile Terminal
Visitors Mobile Terminal
Visitors Mobile Terminal
Protected Room
IoE Visitors Services Redundant Server
Firewall/ Intrusion Detection System/ Antivirus

Fig. 5. Scheme of the IoE based Integrated Technological System Framework (IoE-ITSF) to support the integrated multidisciplinary model for security and safety management (IMMSSM).

III. The specific IoE based Integrated Technological System Framework (ITSF) for the considered site

Due to the specific features of the considered site and due to the need of ensuring security/safety/general management and visitors' services, a proper IoE infrastructure, characterized by a high reliability and resilience, has been designed. It is capable of providing the requested services in ordinary and critical conditions.

The goal of the IoE based integrated technological system framework (IoE-ITSF), and of the related installations and devices, is to:

- Ensure the maximum level of security and safety to people and tangible and intangible assets.
- Ensure the maximum simplicity of utilization, using local and remote automation systems.
- Ensure the maximum level of reliability, resilience and flexibility.
- Ensure the maximum reduction of energy consumption.
- Reduce, as much as possible, the maintenance costs.
- Ensure the maximum level of modularity and expandability, including actual and future IoE services, to simplify the whole management of the considered site, both in ordinary and critical/emergency situations.

The system is characterized by high modularity that allows adding, at any time, any device, element, system etc. to be integrated in the IoE system. The architecture of the system, which represents a proper fitting of the general scheme of Fig. 5 to the considered site, is shown in fig. 6.

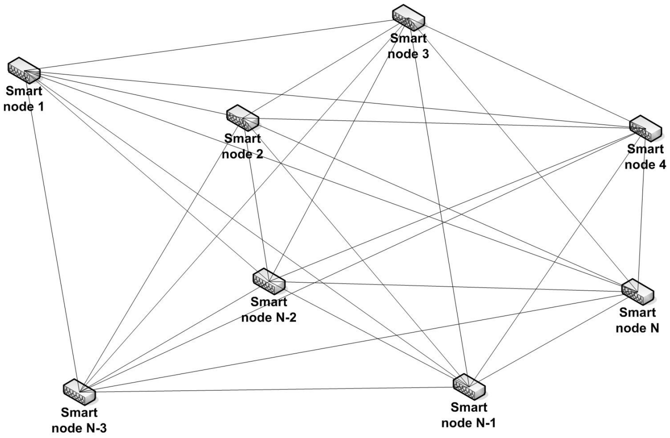


Fig. 6. The IoE based architecture of the system.

The system is based on appropriate communication smart nodes (SNs) densely connected via optical fibres so that, in case of a malfunction of one SN, only the functionality of IoE elements connected to the considered node are lost, while any communication route is rapidly recovered via the other nodes. Each SN is composed of separated devices for safety/security services, personnel services and visitors' services to ensure physical and logical separation between the different classes of services. The different wired networks serve the different Access Points that ensure Wi-Fi/IoE services to security/safety/control personnel, internal personnel and visitors, increasing the security level of the communication and the protection of the system against cyber-attacks [10].

Each SN is supported by a proper electrical back up system (UPS) that allows it to work properly even in the absence of the main electrical power. Further, each SN has a reliable and resilient communication system capable of using cellular connections that allows it to operate also in case of catastrophic events such as earthquake, fires, etc. Some of the SNs employ a proper communication device that allows it to use satellite connection, even if with reduced band width. Different kind of SNs are planned, as a function of the IoE services they must provide, mixing together the following devices/functionalities: switching, computation (node server), cellular communication, satellite communication, etc. Thanks to this flexibility, the SNs can work and communicate using also the external wireless connections, in case of a malfunction of the wired network, using a distribute intelligence scheme.

The design of the IoE-ITSF was prepared using a multidisciplinary approach, with particular care paid also to human factors and psychological aspects of safety / security / emergency and risk of both security/safety/control personnel and visitors [11], even it is not possible to illustrate them due to the limited space available.

The IoE based system, thanks to its architecture that uses wired and wireless network, can connect people (security/safety/control personnel, maintenance personnel, visitors, etc.), devices (sensors, devices and actuators, mobile terminals, wearable devices etc.), data/information/knowledge and processes, actual and futures, guaranteeing a high modularity and expandability, considering them as "IoE objects". The system can communicate with all the "IoE objects", signalling to the operators (personnel of control room, security personnel, maintenance personnel, Police, Fire Brigades, Civil Protection, Medical Staff, etc.) any dangerous or critical situation, in real time, using any kind of communication system.

A privacy-compliant app, designed for the site, can be installed by security/safety/control/management personnel and visitors on their mobile terminals directly when they arrive in the site or in advance. This app allows to access all the services planned according to the user profile (general and augmented reality information, security/safety/emergency information, positioning services useful for emergency management, VoIP/text services for ordinary, security & safety and emergency communication with the related personnel, etc.) and allows the system to consider the mobile terminals as "IoE objects" to reach the specific desired goals of the considered peculiar site. Thanks to the app, it is possible to position people using both GPS system of mobile terminals and Wi-Fi positioning capability of the system (that works correctly even in underground environments where the GPS signal is shielded or weak). In this way, it is possible to have information useful for site statistics (followed visiting routes, permanence time, etc.) and it is possible to manage emergency, communicating directly with people, if necessary, using the text and VoIP functionalities of the app.

The IoE-ITSF utilises all the countermeasures necessary to prevent cyber-attacks, using firewall / intrusion detection system / anti-viruses devices proper installed within the communication network. According to the IoE services that each SN must provide in its area, the SN itself uses a proper server, one for each class of users, so that is capable of operating in any critical condition, even in case of loss of communication, thanks to its distributed intelligence architecture. In this way, also the cybersecurity level of the architecture is improved since the IoE users data flow of the SN cannot move within the communication network without special permission, since all the upload/download communication traffic is properly checked and executed by the node server that acts as a proxy server.

IV. The Genetic Algorithm based optimization technique for communication network

Advanced techniques such as Genetic Algorithms (GAs) [12] have been used to design the wired network of the IoE integrated system to ensure a reduction of final costs and a high level of reliability and resilience of the system itself, including a correct data load balancing between the different SNs that compose the system itself.

Once given a certain site and once the risk analysis and all the other activities related to the IMMSSM [5] are done and the other IoE services are provided, it is possible to know where it is necessary/possible to install IoE field elements (IoE-FEs) such as intrusion detection sensors, video cameras, Wi-Fi Access Points for IoE-Wi-Fi services, etc. and the related data flow of each IoE-FE and where it is necessary/possible to install the smart nodes that compose the basic elements of IoE-ITSF to transmit/receive/compute all the data related to the IoE-FEs.

The problem to be solved is to find the lowest cost configuration that allows one to connect the different IoE-FEs to the SNs, distributing quite uniformly the data flow between the different SNs, without overcoming the maximum data rate of each SN that can be different each other. In this way, a high security and reliability of the network is ensured at the minimum cost.

It is now necessary to translate, in the best way, the given real optimization problem into a proper GA to obtain, in an efficient and rapid way, the required real solution.

Once the positions are selected where SNs must/can be installed, it is necessary to calculate, if exists, the cost of connection between each IoE-FE and the SNs of the system and generate the so-called *cost/connection table* (CCT) where all the IoE-FE/SNs costs are properly reported. Since some connections are not possible, due to architectural and physical restrictions that are particularly felt in already existing cultural heritage sites such as the considered one, the related situation is indicated with a X in the related position of the table. If N is the number of smart nodes and M is the number of IoE-FEs, the dimension of the CCT is equal to N x M. In table 1, an example of a general CCT is shown.

TABLE I. Example of a *cost/connection table*. $C_{(i)-(j)}$ represents the connection cost between IoE-FE i and Smart node j.

	Smart Node 1	**Smart Node 2**	**.........**	**Smart Node N-1**	**Smart Node N**
IoE-FE 1	$C_{(1)-(1)}$	$C_{(1)-(2)}$	---	$C_{(1)-(N-1)}$	$C_{(1)-(N)}$
IoE-FE 2	$C_{(2)-(1)}$	$C_{(2)-(2)}$	---	$C_{(2)-(N-1)}$	$C_{(2)-(N)}$
....	---	---	---	---	---
IoE-FE M-1	$C_{(M-1)-(1)}$	$C_{(M-1)-(2)}$	---	$C_{(M-1)-(N-1)}$	$C_{(M-1)-(N)}$
IoE-FE M	$C_{(M)-(1)}$	$C_{(M)-(2)}$	---	$C_{(M)-(N-1)}$	$C_{(M)-(N)}$

Once the CCT is derived, it is necessary to continue with the codification of the design problem in a simple and efficient genetic problem. The easier way to do this is to use a chromosome composed by a number of genes that is equal to the number M of IoE-FEs: this means that homogeneous genes compose the chromosome. Each gene, related to a specific connection IoE-FE/SN, codifies, with an integer number, the number of SN where the considered IoE-FE is connected. For this reason, the value of each gene varies between 1 and the maximum number of smart nodes N of the network that must be optimally design by the GA.

To allow the maximum efficiency of the genetic process, the IoE-FE/SN connection, represented by an integer number into each gene, is coded with a binary alphabet so that in the presence of the crossing and the mutation operations, the data can be exchanged at the inter-gene level more that at the intra-gene level. If N is the number of smart nodes that must compose the network whose IoE-FEs connections must be optimised, the minimum number of bits necessary to codify N can be demonstrated to be:

$$Int\ (log_2\ (N) +1) \tag{1}$$

In table 2 the codification of the genes and the related chromosome is shown.

TABLE II. DETAILS OF THE CODIFICATION SCHEME OF THE GENE.

	Gene	Considered variable	Variability range	Variable type	Number of Bits
Chromosome	1	Connection IoE-FE 1/smart node	1 ÷ N	Integer	Int ($\log_2$ (N) +1)
	2	Connection IoE-FE 2/smart node	1 ÷ N	Integer	Int ($\log_2$ (N) +1)
	......	......	......	......	......
	M-1	Connection IoE-FE M-1/smart node	1 ÷ N	Integer	Int ($\log_2$ (N) +1)
	M	Connection IoE-FE M/smart node	1 ÷ N	Integer	Int ($\log_2$ (N) +1)

Each chromosome, or individual I, representing a possible solution of the problem is composed by a binary string representing the M connection paths of the IoE-FEs to the considered N smart nodes. The total length of each chromosome, o individual I, is equal to M* Int ($\log_2$ (N) +1) bits.

It is now necessary to do some preliminary considerations to derive a general method that can be valid and useful in any similar cultural heritage contexts.

The fitness function f(I) (where I is the generic individual or chromosome of the population) must consider both the costs of connections and the data load of each SNs. It is therefore composed by two sub fitness functions represented by $f_C(I)$ and $f_D(I)$.

The general fitness function related to the cost $f_{CG}(I)$ for this kind of problem is represented by the sum of the costs of the different connections between the IoE-FE and the SNs:

$$f_{CG}(I)= \Sigma^{M}_{k=1} C_k \qquad (2)$$

being C_k the cost (calculated preliminary and stored in CCT) of connections represented by generic gene k of individual I. The fitness function expressed by (2) can be calculated only if the individual I represents a valid solution, otherwise it is equal to zero, since the individual I does not represent a valid solution for the considered problem.

To deal with a normalized fitness function, it is preliminary necessary to verify the maximum cost C_{max} of connection of IoE-FEs to SNs, if it exists. The normalized fitness function related to the cost $f_C(I)$ can thus be expressed as:

$$f_C(I)= \Sigma^{M}_{k=1} C_k / C_{max} \qquad (3)$$

The fitness function related to cost expressed by (3) can be calculated only if the individual I represents a valid solution, otherwise it is equal to zero, since the individual I does not represent an effective solution for the considered problem.

It is now necessary to define the fitness function related to the data load of IoE-FEs with respect to SNs.

First of all, the total data load of the generic SN_i (TDL, SN_i(I)), in normalized units, with respect to the individual I, can be defined as:

$$TDL,SN_i\ (I)= (\Sigma^{M}_{k=1}\ Data\ Load\ (IoE\text{-}FE_k)|_{SNi}(I))\ /\ (data\ load\ SN_{i,max}) \qquad (4)$$

where $Data\ Load\ (IoE\text{-}FE_k)|_{SNi}\ (I)$ is the data load of the generic IoE-FE connected to the i-th SN in the individual I and $data\ load\ SN_{i,max}$ represents the maximum data load that the i-th SN can support.

The mean data load of the SNs (MDL, SN), in normalized units, with respect to the individual I, can be defined as:

$$MDL,\ SN= (\Sigma^{N}_{k=1}\ TDL,SN_i\ (I))\ /\ (N) \qquad (5)$$

The fitness function $f_D(I)$ related to the data flow can thus be expressed as:

$$f_D(I) = (\Sigma^{N}_{k=1}\ TDL,SN_i\ (I) - MDL,SN(I))\ /\ (MDL,SN) \quad (6)$$

that is a function that is as close to zero as the data load is equally distributed through the different SNs, that is one of the goal.

The total fitness function is therefore f(I)= α f_C(I) + β f_D(I) where α and β are proper normalized parameters, variable between 0 and 1, that can be chosen at will according to the wished results.

The initial population is generated randomly and the number of individuals of populations affects the number of generations necessary to find the final optimal solution and therefore the convergence time. Once recombined and mutated the population, the fitness function of the population is calculated with the fitness function illustrated above, considering only fitting individuals. The converge test is made controlling if the difference between the mean value of fitness functions of the valid individuals belonging to the actual generation and the mean values of the last N_G generations is lesser than a certain percentage value p_{stop} selectable at will.

V. RESULTS

The GA has been tested on more than 1000 real and random sites to obtain, as much as possible, general mean results applicable to any kind of site characterized by the same peculiar features. All the results, reached with a quite rapid converge, as explained in the following, are obtained with converge test parameters N_G and p_{stop} equal to 30 and 0.25 respectively. Due to the great amount of final data obtained and to the number of results that can be extracted from this great amount of final data, only the most noteworthy results are illustrated in the following, due to the limited space available.

An important parameter to be considered to extract significant data is represented by Cost Optimization Ratio (COR) expressed by the ratio between the cost of final optimal solution of the considered problem and the maximum cost of the connections solution C_{max} of the considered problem. It is evident that COR is equal to 1 (or 100 %) if the mean number of connections N_C available between the generic IoE-FE and a generic SN is equal to 1, since there is not any degree of freedom for the optimization activity of the GA. If the mean number of connections N_C available between the generic IoE-FE and a generic SN is equal to N, this means that each IoE-FE could be connected to each SN and thus the GA can perform in the best way its optimization activity. since there is not any degree of freedom for the optimization activity of the GA.

Another important parameter to be considered to extract significant data is represented by Data Load UnBalance (DLUB) that is the difference between the maximum value of data load of a SN (expressed in percentage) and the minimum value of data load of an SN (expressed in percentage). If DLUB is equal to 1 (or 100 %), it means that in the considered solution there is almost one SN that has reached its full data load and almost one SN that has no IoE-FE connected.

In fig. 7, the Cost Optimization Ratio COR and Data Load UnBalance DLUB, expressed in percentage, as a function of mean number of available connection paths N_C between each IoE-FE and each SN is shown.

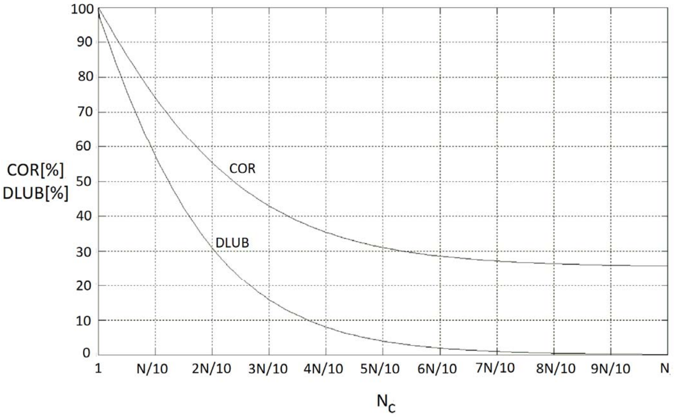


Fig. 7. Cost Optimization Ratio COR and Data Load UnBalance DLUB, expressed in percentage, as a function of mean number of available connection paths N_C between each IoE-FE and each SN.

From fig. 7 it is possible to see how the GA is capable of reaching cost reductions around 25% with respect to the maximum cost of connection of the network C_{max} when N_C increases, due to the fact that the GA has more connection paths available between IoE-FEs and SNs to perform its optimization capabilities. In the same way, the GA is capable of balancing the data load between the different SNs, reaching a perfect balancing (DLUB=0) when N_C tends to N.

The number of generations necessary to the GA to reach the final optimal solution represents a very important parameter, together with the initial population, since it gives an indication of the computation load that, once related to the computation resources available, provides an exact value of the time necessary to reach the desired final optimal solution. It has been properly studied but the related results are not shown in the following due to limited space available.

VI. Conclusions

The new communication network for Internet of Everything based security/safety/general management and visitors' services of the Papal Basilica and Sacred Convent of Saint Francis in Assisi, Italy has been illustrated.

Genetic Algorithms (GAs) have been used to design the connections between the different IoE Field Elements and the different smart nodes that comprise the network to ensure a reduction of final costs and an elevated level of reliability and resilience of the system itself, keeping, into consideration, the typical artifacts and restrictions of unique and peculiar cultural heritage sites such as the considered one.

The proposed system, together with the GAs based optimization technique, because of their flexibility, can be used in any kind of similar cultural site by means of proper adaption.

References

[1] F. Garzia, E. Sammarco, R. Cusani, “The integrated security system of the Vatican City State”, International Journal of Safety & Security Engineering, WIT Press (Southampton - UK and Boston-USA), Vol. 1, No. 1, pp. 1-17, 2011.

[2] G. Contardi, F. Garzia, R. Cusani, “The integrated security system of the Senate of the Italian Republic”, International Journal of Safety & Security Engineering, WIT Press (Southampton-UK and Boston-USA), Vol. 1, No. 3, pp. 219- 246, 2011.

[3] F. Garzia, L. Papi, “An Internet of Everything based integrated security system for smart archaeological areas”, Proc. of IEEE International Carnahan Conference on Security Technologies, Orlando (USA), pp. 64-71, 2016.

[4] F. Garzia, L. Sant'Andrea, “The Internet of Everything based integrated security system of the World War I commemorative museum of Fogliano Redipuglia in Italy”, Proc. of IEEE International Carnahan Conference on Security Technologies, Orlando (USA), pp. 56-63, 2016.

[5] F. Garzia, “An integrated multidisciplinary model for security management and related supporting integrated technological system”, Proc. of IEEE International Carnahan Conference on Security Technologies, Orlando (USA), pp. 107-114, 2016.

[6] F. Garzia, R. Cusani, "New technique for the optimization of security communication wired networks in historical buildings" Proc. of IEEE International Carnahan Conference on Security Technologies, Medellin (Colombia), pp. 116-121, 2013.

[7] F. Garzia, D. Costantino, V. Baiocchi, "Security and safety management and role of laser scanning in unique and peculiar cultural heritage sites such as the Papal Basilica and the sacred convent of St. Francis in Assisi in Italy", International Journal of Heritage Architecture, Vol. 2, No. 2, pp. 271-282, 2018.

[8] M. G. Angelini, V. Baiocchi, D. Costantino, F. Garzia, “Scan to BIM for 3D Reconstruction of the Papal Basilica of Saint Francis in Assisi in Italy, The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Volume XLII-5/W1, 2017 GEOMATICS & RESTORATION – Conservation of Cultural Heritage in the Digital Era, 22–24 May 2017, Florence, Italy, pp.47-54. doi:10.5194/isprs-archives-XLII-5-W1-47-2017.

[9] F. Garzia, M. Lombardi, "The role of BIM for Safety and Security management”, International Journal of Sustainable Development and Planning Volume 13, No. 1, pp. 49-61, 2018.

[10] F. Garzia, “Handbook of Communication Security”, WIT Press (Southampton - UK and Boston - USA), 2013.

[11] F. Borghini, F. Garzia, A. Borghini, G. Borghini, “The Psychology of Security, Emergency and Risk”, WIT Press (Southampton - UK and Boston - USA), 2016.

[12] D. E. Goldberg, “Genetic Algorithms in Search, Optimisation and Machine Learning”, Addison-Wesley, New York, 1989.