INTEGRATED MULTIDISCIPLINARY APPROACH FOR SAFETY & SECURITY MANAGEMENT: THE CASE STUDY OF PAPAL BASILICA AND SACRED CONVENT OF SAINT FRANCIS IN ASSISI, ITALY

Fabio Garzia
Safety & Security Engineering Group – DICMA, SAPIENZA – University of Rome, Italy
Wessex Institute of Technology, Southampton, UK
European Academy of Sciences and Arts, Salzburg, Austria
Foundation for the Basilica of Saint Francis in Assisi, Assisi, Italy
fabio.garzia@uniroma1.it

Abstract:
The purpose of this paper is to illustrate an integrated multidisciplinary approach for safety and security management. It is based on a general Integrated Multidisciplinary Model for Safety and Security Management (IMMSSM) supported by an Integrated Technological System Framework (ITSF) that can be based on Internet of Things (IoT) / Internet of Everything (IoE). It can be adopted in most situations and has already produced interesting results, both from a theoretical and practical point of view, in safety & security management, and even from a cost/benefit point of view, in different existing organizations which have started to adopt the IMMSM and have started to modify their already existing technological systems to support it through the above mentioned ITSF. In particular, the case study of the Papal Basilica and Sacred Convent of Saint Francis in Assisi in Italy is shown.

Key words:
Safety management, security management, Internet of Things, Internet of Everything, IoE/IoT integrated system.

1 Introduction

Safety and Security management (SSM) represents a vital and powerful tool for the prevention of incidental events (fires, floods, hurricanes, earthquakes, etc.) and/or voluntary attacks (vandalism, thefts, espionage, terrorism, etc.) against people and tangible and intangible resources as well as for their protection when incidental events and/or voluntary attacks take place in any sort of organization.

It is also very important to mitigate an incidental event (safety) and/or a voluntary attack (security) during the initial phase and during the subsequent phases, using fundamentals tools represented by emergency management, business/service continuity and disaster recovery.

Because of the constant growth of new hazards and threats, SSM requires constant updating using more and more powerful and flexible tools which have to be integrated using a proper multidisciplinary approach, considering also economical aspects from the cost / benefit point of view.

Integrated technological systems [1 – 5] represent resourceful elements of generating responses which can aid SSM in an effective way, even from budgets optimization point of view.

For this reason, it is necessary to exploit an integrated multidisciplinary approach for safety and security management which joins together modelization [6, 7] and a suitable Integrated Technological System Framework (ITSF) that can be based on Internet of Things (IoT) / Internet of Everything (IoE), considering also the big data aspect [8 -12] which represents the purpose of this paper, showing also the case study of the Papal Basilica and Sacred Convent of Saint Francis in Assisi, Italy.

2 Integrated multidisciplinary approach for safety & security management

The considerend approach joins together modelization and a suitable Integrated Technological System Framework (ITSF) that can be based on Internet of Things (IoT) / Internet of Everything (IoE).

In the following, a proper general model and a general ITSF capable of supporting are shown.

2.1 The general model for safety and security management

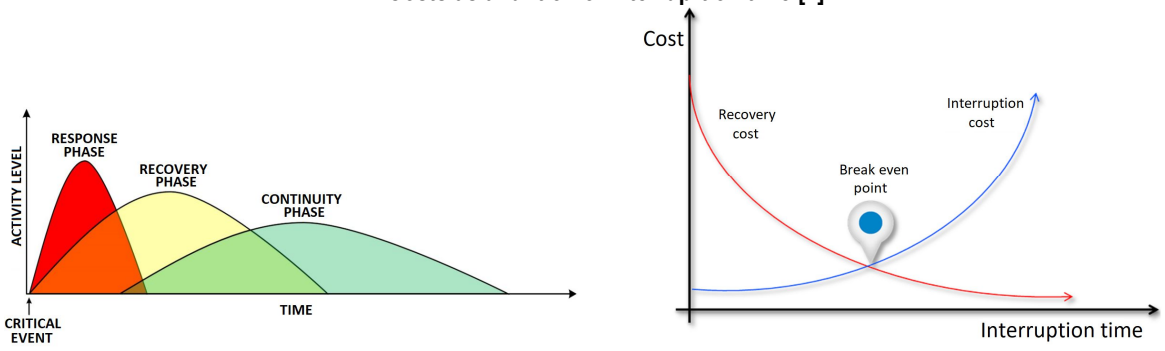
Since safety and security deal with risks, it is fundamental to provide a general description of it for our purposes. Risk R can therefore be defined as the probability P of a quantifiable damage, injury, liability, loss, or any kind of undesired occurrence (briefly designated as damage D which depends on the considered situation) that is generated by external or internal vulnerabilities. The risk R can therefore be defined as:

$$R = f(P, D) \quad (1)$$

where f (*) is a proper function which depends on the considered situation, P represents the probability of the risk, variable between 0 and 1, and D represents the damage which can be defined according to a selected reference range, as a function of the considered organization. The damage D is supposed to be variable between 0 and 10 in the considered context, without any loss of generality and to preserve a general approach.

The proposed integrated multidisciplinary model for safety and security management (IMMSSM) joins all the elements necessary to deal with risks such as risk analysis, impact analysis, risk mitigation and residual risk management such as emergency management (EM), business/service continuity (BSC), and disaster management (DM), considering the associated operative tools (OTs), as shown in the following. When a critical event takes place despite of all the prevention countermeasures necessary to reduce its probability and the protection countermeasures necessary to reduce its damage, a plenty of activities must be done to manage the critical event and to return to the initial condition, if possible. All the necessary activities can be divided into 3 main phases represented by response phase, recovery phase and continuity phase according to the kind of actions and activities that are necessary. The level of these activities varies according to the considered phase both from intensity point of view and from the time duration point of view. The response phase represents the activities that must be done immediately to face the critical event, avoiding greater damages. The recovery phase represents the activities that must be done, even overlapped to the previous phase, to start to recover from the critical event. The continuity phase represents the activities that must be done, even overlapped to the previous phases, to restore the initial condition, before than the critical event. This situation is illustrated in Fig. 1a.

Figure 1: (a) Activity level as a funtion of the time of the different activities necessary to manage a critical event. (b) Costs as a funtion of interruprtion time [7].



Any critical event can generate a partial or total interruption of the functionality of a considered organization. From this point of view, it is possible to reduce the interruption time using proper prevention and protection countermeasures and proper activities to manage the residual risk, illustrated in the following. If a reduced interruption time is needed, due to the requirements of the considered

organization, a noticeable investment is necessary to set up all the necessary countermeasures. The recovery cost decreases with the tolerable interruption time since less efforts are needed. This situation is illustrated in Fig. 1b. On the other side, the interruption cost growths with the time, according to a behaviour that depends of the considered organization. The crossing point between the recovery cost curve and the interruption cost curve lets individuate the break-even point which represents the balance point between the cost necessary to recover the situation and the cost due to the interruption, individuating the optimal interruption time and the optimal investment necessary.

Operative tools (OTs) are represented by all the elements that can be used for SSM, properly integrated and supported from a ITSF. They can be divided into countermeasures (CM) [1– 5, 13], security & safety policies and procedures (PR), and human factor and resources (HF). Countermeasures are represented by physical/logical technology (physical: intrusion detection, access control, video surveillance, fire detection, dangerous gas detection etc.; logical: intrusion detection systems, anti-viruses, etc.) and physical/logical barriers (physical: fences, armoured doors, armoured glasses, fire extinguisher etc.; logical: firewalls, etc.). Human factor and resources are fundamental to obtain the best performance by personnel and people, training them and using a proper psychodynamic/ epigenetic - evaluation/improving [14]. It is also very important to evaluate human error for an efficient SSM using the most proper method according to the considered situation [15].

Risk analysis [16 – 17] represents an essential tool to evaluate the threats concerning an organization and it can be divided into distinct groups, represented by: qualitative, semi-quantitative, quantitative, and mixed including human factor.

Once individuated and measured all the risks of the considered organization, it is necessary to evaluate the impact that those risks can produce over the organization itself, identifying all the essential elements which must be kept operative to ensure that the organization could work. From this point of view, it is important to contemplate three important parameters represented by: MTD (Maximum Tolerable Downtime), RTO (Recovery Time Objective), RPO (Recovery Point Objective) which provide a quantitative evaluation concerning the above elements that is necessary to achieve a precise impact analysis.

Risk mitigation is done by means of all the necessary OTs to reduce the probability of each risk (prevention activities) and/or damage of each risk (protection activities). There are four main strategies for risk mitigation, represented by: risk acceptance (the risk is accepted since the mitigation activity is too expensive with respect to the damage produced by the risk), risk avoidance (any risk is reduced at the minimum level without any care to of costs), risk limitation (that is the most common strategy since it reduces the exposition considering only a sub-set of actions. It joins risk acceptance and risk avoidance), risk transference (the risk is transferred to third parties available at accepting it).

Residual risk management can be made using emergency management, service/business continuity and disaster management that can and must be strongly integrated to avoid malfunctioning of residual risk management.

Emergency management is extremely important to manage critical situations according to what is planned in the safety and security procedures and policies, using OTs in a proper way. In fact, it is important to work in a very well-organized and accurate way as soon as the emergency takes place otherwise it could be no more possible to recover the original conditions and the consequences could be more hazardous.

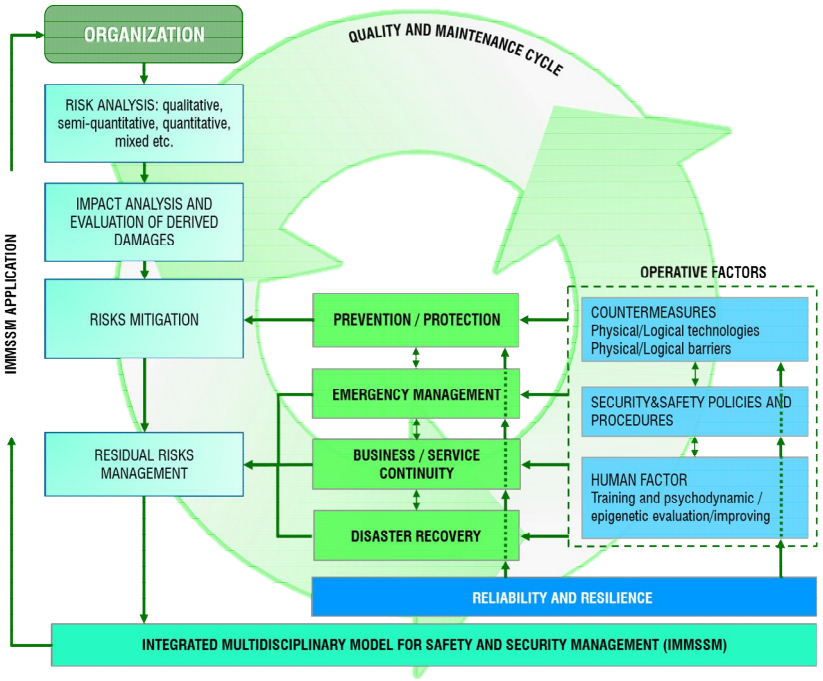
Business and service continuity concentrate about what is required to recover regarding functionalities, processes and activities which are considered critical for the exact operativity of the considered organization. They can be divided into the typical phases of plan, do, check, improve.

Disaster recovery is represented by the technological, management and logistic elements necessary to recover the operativity of an organization, focusing mainly on system, data, infrastructure even if this represent a quite limited approach since disaster can be produced from a plenty of motives.

From what illustrated above, not only the above elements of residual risk management must be strongly connected but also all the elements of SSM, including OTs, must be connected to attain

resourceful results. For this reason, a suitable integrated multidisciplinary model for safety and security management (IMMSSM) has been studied [6, 7]. It represents a general model valid for most organizations and its scheme is shown in Fig. 2.

Figure 2: Scheme of the Integrated Multidisciplinary model for Safety and Security Management (IMMSSM) [6, 7]



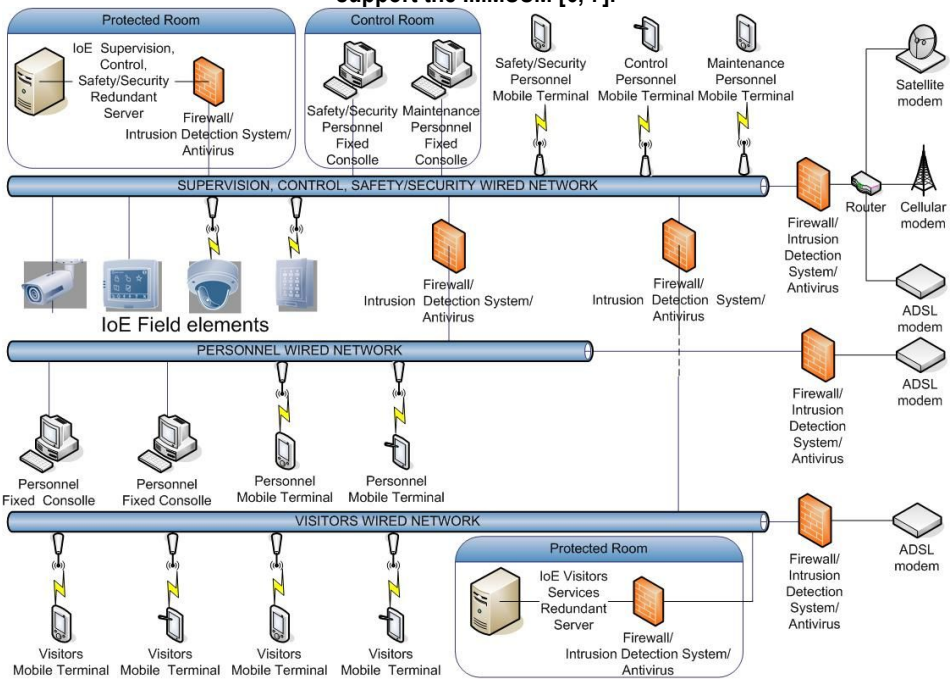
An appropriate Integrated Technological System Framework (ITSF), aided by a proper optimization procedure for the use of OTs from the cost/benefit point of view, can reduce the general risk of the organization at minimum cost, thus assuring the finest employment of the IMMSSM at lowest rate with respect to the wanted objectives. All the elements of the IMMSSM mutually interact. This means that if there is a variation in one of them, such as a new threat to face, the related variation of risk analysis generates an inevitable tuning in all the other elements. It is also necessary to consider other essential elements represented by reliability and resilience for OTs, emergency management, business /service continuity and disaster recovery, as shown in Fig.2. The IMMSSM requests an Integrated Technological System Framework (ITSF) for its support and for the implementation of all the policies and procedures, due to the mixture of features, analyses and measures which must be considered in normal and critical situations. The IMMSSM and the related supporting ITSF must also consider analysis, planning and management of the maintenance and quality, as well as the initial realization cost and annual cost. To create a suitable IMMSSM, it is essential to evaluate the use of OTs from a cost/benefit point of view, considering not only the cost of initial execution but also the annual costs. From this point of view, the great advantages deriving by the integrability of OTs in the above IMMSSM and related ITSF have been demonstrated [7].

2.2 The integrated technological system framework based on IoT/IoE

A suitable and fitting Integrated Technological System Framework based on Internet of Everything (IoE-ITSF) is strongly recommended to support the IMMSSM. In this way, it is possible to warrant all the objects of the IMMSSM to be integrated in a flexible and modular way, to translate, at any time, any necessary tuning of the IMMSSM into a quick and inexpensive adjustment of the associated IoE-ITSF. This goal can be realised using integrated systems [1– 5] and innovative technologies such as Internet of Everything (IoE) where people, things (mobile terminals, devices, actuators, smart sensors, wearable devices, etc.), data/information/knowledge and procedures are suitably associated to accomplish the required targets [8- 12]. The IoE-ITSF is characterized by a high modularity which allows

for the integration, at any time and in flexible way, of any type of element which needs to be incorporated in the IoE system. Its general scheme is shown in Fig. 3.

Figure 3: Scheme of the Integrated Technological System Framework based on Internet of Everything (IoE-ITSF) to support the IMMSSM [6, 7].



The proposed IoE-ITSF is planned to be a widespread framework useful for the most organizations where external visitors can also be present. For this reason, the networks used to provide supervision, control and safety/security services, internal personnel services and visitor's services are appropriately separated from the physical and logical points of view for security reason [13]. The IoE-ITSF can interconnect all the 'IoE objects', generating a proper signalling to the operators (personnel in the control room, security personnel, safety personnel, maintenance personnel, Police, Fire Brigades, Civil Protection, Medical staff, etc.), in real time, via any sort of communication channel, when any dangerous or risky situation happens [13]. Due to its nature, the IoE-ITSF deals with a massive amount of data and, for this reason, it uses proper big data and data analytics techniques to guarantee always its best performances [9]. The IoE-ITSF illustrated before has demonstrated to be a powerful tool to ensure a high flexibility for OTs that can be supported and integrated, with a reduced cost, by the IoE-ITSF itself, guaranteeing considerable cost reductions thanks to the integration capability of the system with respect to the OTs [6, 7]. This is the reason for which the IoE-ITSF has shown itself to be extremely useful not only for IMMSSM but also for its optimal implementation, from the cost/benefit point of view, thanks to its positive influence on OTs. For this cause, some existing organizations have started an implementation program of IMMSSM and of the related IoE-ITSF, modifying, gradually, their already existing integrated systems [1-5].

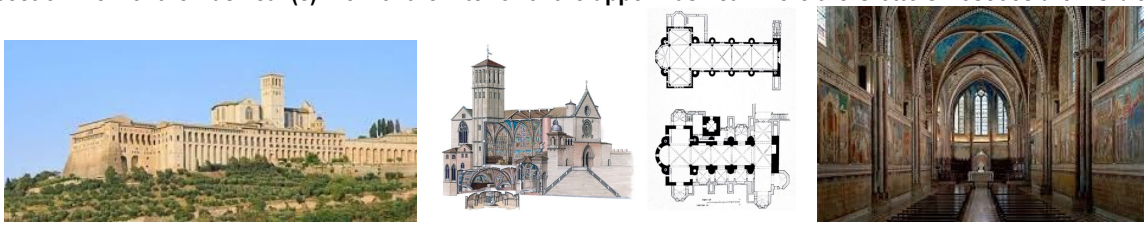
3 The case study of the Papal Basilica and Sacred Convent of Saint Francis in Assisi

The Papal Basilica and the Sacred Convent of Saint Francis in Assisi in Italy represent an exceptional cultural heritage site where the mortal remains of Saint Francis are housed since 1230 A.D.

Each year, millions of pilgrims and visitors from all over the world visit this site each which, from 2000 A.D., together with other Franciscan sites in the surrounding and the entire Assisi town, have been appointed as World Heritage by UNESCO. The Papal Basilica, where unique frescoes by Giotto and other famous painters are present, is composed by three layered assemblies: the tomb or crypt of Saint Francis, located at the lower level; the lower Basilica, whose altar is just above the tomb of Saint

Francis; the upper Basilica, located above the lower Basilica. Inside the Sacred Convent there is a museum, a library and sufficient space for hosting spiritual and cultural activities. Inimitable and composite cultural heritage sites, such as the considered one, necessitate a noteworthy effort to guarantee security and safety of visitors. Along with such needs are cultural heritage preservation and protection as well as accessibility for visitors, with reference to visitors with disabilities, and for personnel normally present for site management, including the Friar's community. From this point of view, it is necessary to consider other important aspects such as energy management, maintenance management and a plenty of other aspects that must be managed in a well-organized way, by means of a suitable proper integrated technological system. These goals can be reached using the above integrated multidisciplinary approach properly adapted for the considered site.

Figure 4: (a) Panoramic view of the Papal Basilica and the Sacred Convent of Saint Francis in Assisi. (b) Schematic section view of the Basilica. (c) View of the interior of the upper Basilica where the Giotto's frescoes are visible.

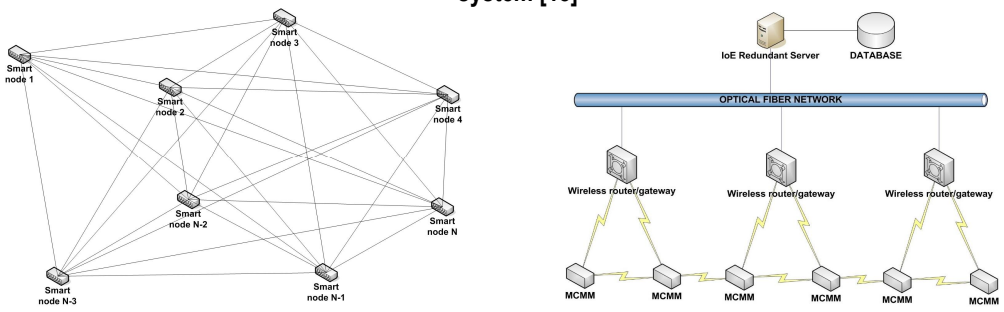


(a) (b) (c)

3.1 Development of the model, design of the IoE-ITSF system and first results obtained

Different actions have been carried out and are still going on both sequentially and in parallel, as a function of the available resources, always considering the final goal. Thus, a set of preliminary and essential series of multi-disciplinary activities formulated as set up of the IMMSSM and subsystems of the IoE system are considered [18]. Due to multi-disciplinary work that have been done and that is going on, an international group started working locally and remotely.

Figure 5: (a) Architecture of the IoE system backbone network. (b) Architecture of the microclimate monitoring system [18]



(a) (b)

First of all, the introductory activities required to set up the IMMSSM have started, included the other actions necessary to study and design the Site Management System (SMS), for the specific site, based on IoE (SMS-IoE), as well as a new communication network which is vital to ensure that all the information needed for the strategic IoE services could be supported with the required level of security, safety, reliability and resilience, granting the required confidentiality, availability and integrity. From this point of view, a proper Genetic Algorithm (GA) based technique has been studied and tested to design the connections between the different IoE Field Elements and the different smart nodes that compose the network (Fig. 5a) to guarantee a decrease of final costs and an elevated level of reliability and resilience of the system itself, considering the typical artefacts and restrictions of an inimitable cultural heritage site such as the considered one.

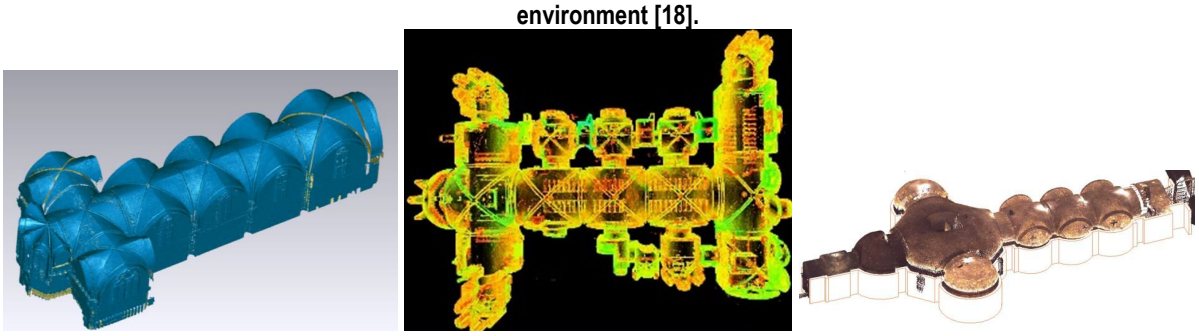
Due to the need of acquiring all the necessary information to be shared locally and remotely, a proper laser scanning activity of the Papal Basilica and of the Tomb (Figures 6) has been done. This is

aimed at obtaining a 3D model of it that is going to be rendered into a Building Information Modelling (BIM) and to utilize a flexible tool for all the needed activities, including safety and security management [19]. This action is essential due to the presence of strong architectural restrictions, which involves taking care in the installation of wires and devices.

At the same time, a proper study and analysis regarding human factor was done and it is still on-going. It regards the psychological aspects of the ordinary signalling and all the IoE services provided both to visitors and to personnel normally present for site management, including the Friar's community. It is aimed at improving the value and the effectiveness of the IoE services themselves and of those inside the site. These activities require the use of suitable tools for opinion mining of social networks to collect feedback from visitors on perceived safety/security versus real safety/security [14].

Another parallel activity is related to an experimental microclimate monitoring system (MMS) of the Papal Basilica, based on apt microclimate monitoring modules (MCMM), has been studied and realized and its architecture is shown in Fig. 5b. The MMS are aimed at controlling the microclimate parameters to avoid of reaching critical conditions which could trigger harmful processes of the unique frescos of the Basilica.

Figure 6: (a) Meshing upper Basilica. (b) Point cloud of lower Basilica. (c) Tomb point cloud represented in Revit environment [18].



(a) (b) (c)

Other activities are dedicated to new and suitable IoT/IoE services for the considered site (such as people counting subsystem), including Augmented Reality (AR) and Virtual Reality (VR) intended at improving the visiting experience of the visitors; biometric solutions for the considered site, with particular care to the privacy aspects; fluid dynamic analysis of the interior of the site to improve the quality of air with regards to people wellness and pictures preservation plus further activities related to the energy management/optimization/preservation and renewable energy; cybersecurity aspects of the IoE system; Big Data, security analytics for Big Data infrastructure, machine learning techniques for the site etc., with the purposes of attainment, step by step and with the contribute of all the people and subjects that are working on it, the desired goals.

4 Conclusions

In this work an integrated multidisciplinary approach for safety and security management which joins together modelization and a suitable Integrated Technological System Framework (ITSF) that can be based on Internet of Things (IoT) / Internet of Everything (IoE), has been illustrated.

The IoE-ITSF has demonstrated to be a powerful tool to ensure a high flexibility for OTs that can be supported and integrated, with a reduced cost, by the IoE-ITSF itself, guaranteeing considerable cost reductions thanks. For this reason, some existing organizations have started an implementation program of IMMSSM and of the related IoE-ITSF, modifying, gradually, their already existing integrated systems. The case study of the Papal Basilica and Sacred Convent of Saint Francis in Assisi in Italy, which represents and always-going-on project that is opened to future solutions and contribution by anybody, with the intention of improving constantly the services which can be provided, is demonstrating, until now, the same advantages using the approach illustrated in the paper.

5 Bibliography

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

[2] Contardi, G., Garzia, F. & Cusani, R., The integrated security system of the Senate of the Italian Republic, *International Journal of Safety & Security Engineering*, 1(3), pp. 219- 246, 2011.

[3] Garzia, F. & Cusani, R., The integrated safety / security / communication system of the Gran Sasso mountain in Italy, *International Journal of Safety & Security Engineering,* 2(1), pp. 13-39, 2012.

[4] Garzia, F. & Cusani, R., The safety/security/communication wireless LAN of the underground Gran Sasso mountain national laboratories of the Italian Institute of Nuclear Physics, *International Journal of Safety & Security Engineering,* 2(3), pp. 209-226, 2012.

[5] Garzia, F., Sammarco, E. & Cusani, R., Vehicle/people access control system for security management in ports, *International Journal of Safety & Security Engineering*, 2(4), pp. 351-367, 2012.

[6] Garzia, F. "An Integrated Multidisciplinary Model for Security Management – Optimized Implementation Technique and Related Supporting Technological System Framework", *Proc. of IEEE International Carnahan Conference on Security Technology*, Orlando (USA), pp. 107-114, 2016.

[7] Garzia, F., Lombardi, M., "Safety and security management through an integrated multidisciplinary model and related integrated technological framework", *SAFE 2017 – WIT Transactions on The Built Environment*, Vol. 174, pp. 285-296, 2017.

[8] Di Martino, B., Li, K. C., Yang, L., T., Esposito, A., Internet of Everything: Algorithms, Methodologies, Technologies and Perspectives (Internet of Things), *Springer*, 2017.

[9] Kleppmann, M., Designing Data-Intensive Applications, *O'Reilly Media*, 2017.

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

[11] Garzia, F. & Sant'Andrea, L., The Internet of Everything Based Integrated Security System of World War I Commemorative Museum of Fogliano Redipuglia in Italy", *Proc. of IEEE International Carnahan Conference on Security Technology*, Orlando (USA), pp. 56-63, 2016.

[12] 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", *SAFE 2017 – WIT Transactions on The Built Environment, Vol 174, pp.261-272, 2017.*

[13] Garzia, F., Handbook of Communication Security, *WIT Press*, 2013.

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

[15] Spurgin, A. J., Human Reliability Assessment – Theory and Practice, *CRC Press*, 2009.

[16] Guarascio, M., Lombardi, M., Rossi, G. & Sciarra, G., Risk analysis and acceptability criteria, *WIT Transactions on the Built Environment*, 94, pp.131-138, 2007.

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

[18] Gambetti, M., Garzia, F., Baiocchi, V., Vargas Bonilla, F. J., Borghini, F., Ciarlariello, D., Chakaveh, S., Costantino, D., Culla, A., Cusani, R., Ferrer, M. A., Fusetti, S., Kodl, J., Livatino, S., Lombardi, M., Marsella, S., Peng, J., Smejkal, V., Ramalingam, S., Ramasamy, M., Sacerdoti, S., Sdringola, A., Thirupati, D., Faundez Zanuy, M., "The Internet of Everything System for the Papal Basilica and Sacred Convent of Saint Francis in Assisi, Italy*", Proceedings of WEF (World Engineering Forum) - Safeguarding Humankind's Heritage, The Great Challenge for Engineers*, Rome (Italy), 2017.

[19] Garzia, F., Lombardi, M., "The role of BIM for Safety and Security management", *Int. J. Sus. Dev. Plann.*, Vol. 13, No. 1, pp. 49-61, 2018.