SAFETY AND SECURITY MANAGEMENT THROUGH AN INTEGRATED MULTIDISCIPLINARY MODEL AND RELATED INTEGRATED TECHNOLOGICAL FRAMEWORK

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

ABSTRACT

The purpose of this paper is to illustrate a multidisciplinary model for safety and security management (IMMSSM) which can be implemented by means of a suitable Integrated Technological System Framework (ITSF) that can be based on Internet of Things (IoT)/Internet of Everything (IoE), showing also the significant role played by the integration of the elements that compose the model itself, thanks to a proper genetic algorithm studied for the specific context.

Keywords: safety management, security management, Internet of Things, Internet of Everything, Genetic Algorithms, IoE/IoT integrated system.

1 INTRODUCTION

Safety and Security management (SSM) represents a substantial and powerful instrument for the prevention of incidental events (fires, floods, hurricanes, earthquakes, etc.) and/or voluntary attacks (vandalism, thefts, espionage, 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 essential 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.

Due to the never-ending growth of new hazards and threats, SSM requires constant updating using more and more powerful and flexible tools which must be properly integrated via a multidisciplinary method, bearing in mind even financial features which must heightened considering a cost/benefit point of view.

Integrated technological systems [1]–[5], represent resourceful elements to produce answers capable of aiding SSM in a practical way, even from budgets optimization point of view.

Due to this cause, it is required to exploit a wide-range approach which allows for the realization of an integrated multidisciplinary model for safety and security management (IMMSSM) [6], which can be implemented by means of a fitting Integrated Technological System Framework (ITSF) that can be based on Internet of Things (IoT)/Internet of Everything (IoE), considering also the big data aspect. [7], [10].

To realise an effective IMMSSM, it is necessary to enhance the offered tools from the cost/benefit point of view.

This aim represents an arduous task because of the reduced funds generally available. For this reason, it is necessary to use them in a very efficient way, attaining the maximum

WIT Transactions on The Built Environment, Vol 174, © 2018 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE170261

reduction of risks due to different threats and the best management of residual risks using emergency management, service/business continuity and disaster management.

From this point of view, a proper genetic algorithm (GA) [11]–[13], has been studied and developed and its optimization features within the considered problem are shown, deepening results and advantages.

The purpose of this paper is to illustrate a multidisciplinary model for safety and security management (IMMSSM) and related ITSF, even based on IoT/IoE, showing also the significant role played by the integration of the elements that compose the model itself, thanks to a proper genetic algorithm studied for the specific context.

2 THE INTEGRATED MULTIDISCIPLINARY 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. Therefore, risk R can 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. Therefore, the risk R can be defined as:

$$R = f\,(P, D), \tag{1}$$

where f (*) is a proper function that depends on the considered situation, P represents the probability of the risk, variable between 0 and 1, and D represents the damage that can be defined according to a selected reference range, as a function of the considered organization. We suppose the damage D to be variable between 0 and 10 in the considered context, without 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 happens 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:

1. response phase;
2. recovery phase;
3. continuity phase;

according to the kind of actions and activities that are necessary.

It is evident that 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.

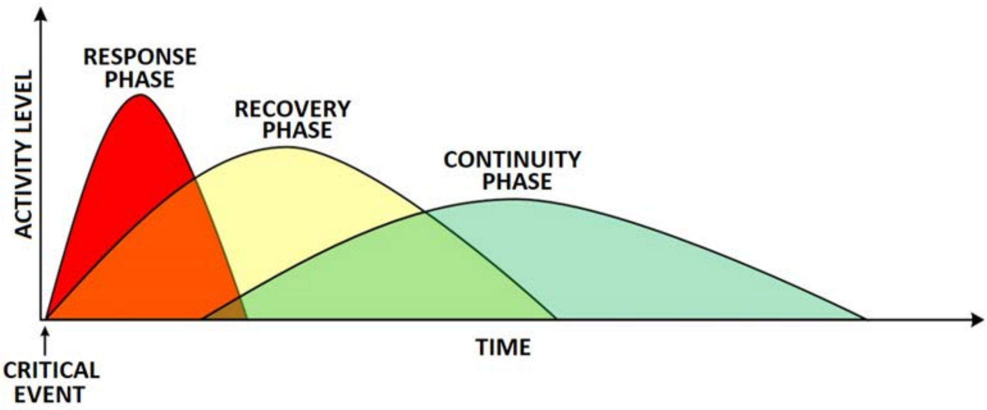

Figure 1: Activity level as a function of time of the different activities necessary to manage a critical event.

This situation is illustrated in Fig. 1.

Any critical event can provoke a partial or total interruption of the functionality of a given organization. Using proper prevention and protection countermeasures and proper activities to manage the residual risk, illustrated in the following, it is possible to reduce the interruption time. It is evident that if a short interruption time is necessary, due to the needs 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. 2.

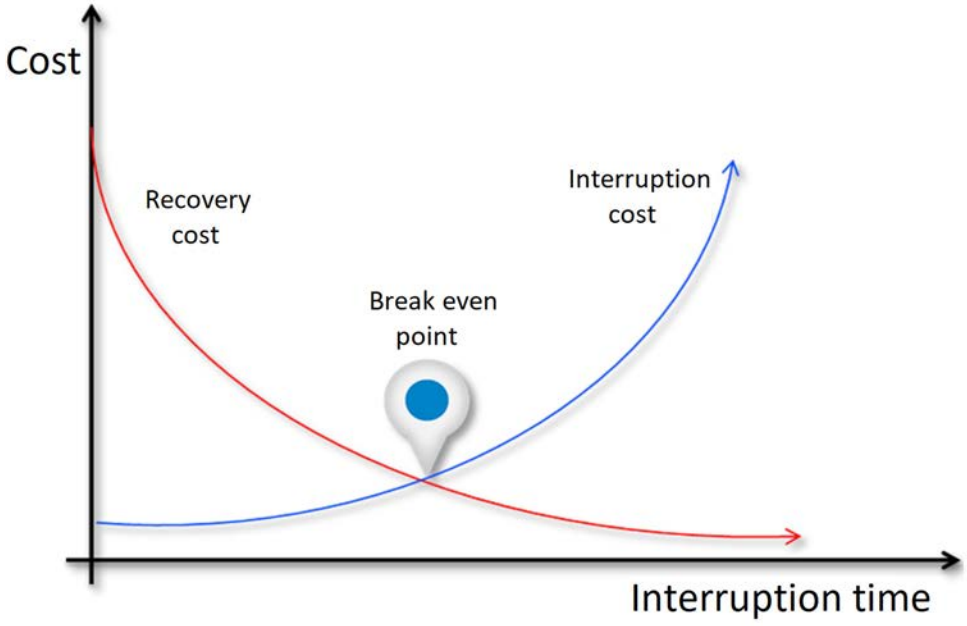

Figure 2: Costs as a function of interruption time.

On the other side, the interruption cost increases with the time, according to a behaviour that depends of the specific organization. The crossing point between the recovery cost curve and the interruption cost curve allows to individuate the break-even point that represents the balance point between the cost necessary to recover the situation and the cost due to the interruption, giving also the optimal interruption time and the optimal investment necessary.

Operative tools 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], [14], security and 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 factors and resources is fundamental to obtain the best performance by personnel and people, training them and using a proper psychodynamic/epigenetic – evaluation/improving [15]. It is also very important to evaluate human error for an efficient SSM using the most proper method such as ASEP (Accident Sequence Evaluation Program), HEART (Human Error Assessment Reduction Technique), APJ (Absolute Probability Judgment), ATHEANA (A Technique for Human Event Analysis), HRMS (Human Reliability Management System), JHEDI (Justified Human Error Data Information) etc. according to the considered situation [16].

Risk analysis [17]–[21] is a fundamental tool to evaluate the threats regarding an organization and it can be divided into distinct groups, represented by: qualitative, semi-quantitative, quantitative, and mixed including human factor.

Qualitative risk analysis is useful in doing a general and preliminary overview of the threats of an organization but it does not provide quantitative results that are fundamental to do the correct choices. Anyway, it represents a valid method to synthetize the risk scenario to be illustrated even to not skilled people. The main techniques for qualitative risk analysis are represented by: vulnerability array, interaction array, V^2 array, threats array, FMEA (Failure Mode Event Analysis), etc.

Quantitative risk analysis is fundamental in giving the exact values of different threats. It can be a very complex and expensive process, due to the elevated number of activities which are necessary to do it in an effective way. The main techniques for quantitative risk analysis are represented by: ETA (Event Tree Analysis), FTA (Fault Tree Analysis), etc.

Semi-quantitative risk analysis represents an intermediate analysis positioned between qualitative and quantitative analysis. It tries to reach a good trade-off between both of them. A commonly used method of this group is represented by AZHOP (HAZard and Operability analysis) but there are plenty of others.

Mixed risk analysis including human factor joins different techniques. The most commonly used methods are represented by LOPA (Layer of Protection Analysis) but there are plenty of others.

Once individuated and quantified 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 fundamental elements that must be kept operative to guarantee that the organization could work. From this point of view, it is important to consider three important parameters represented by: MTD (Maximum Tolerable Downtime), RTO (Recovery Time Objective), RPO (Recovery Point Objective) that provide a quantitative evaluation regarding the above elements which is necessary to perform a correct impact analysis.

Risk mitigation is done using 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 suitable way. In fact, it is important to operate in a very efficient and precise way as soon as the emergency happens otherwise it could be no more possible to recover the initial conditions and the consequences could be more dangerous.

Business and service continuity focus about what is necessary to recover between functionalities, processes and activities which are considered critical for the correct 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 of system, data, infrastructure even if this represent a quite limited approach since disaster can be caused from a plenty of reasons.

It is evident, from what illustrated above, that not only the above elements of residual risk management must be strongly linked but also all the elements of SSM, including OTs, must be linked together to obtain performing and efficient results. For this reason, a suitable integrated multidisciplinary model for safety and security management (IMMSSM) has been studied [6], representing a general model valuable for most organizations that, in the present paper, is furtherly studied and deepened. The scheme of IMMSSM is shown in Fig. 3.

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, as shown below, thus assuring the finest employment of the IMMSSM at lowest rate with respect to the wanted objectives.

All the elements of the IMMSSM showed above interrelate reciprocally: if there is a variation in one of them, such as a new threat to face, the related variation of risk analysis generates an unavoidable adjustment in all the other elements, since the model is strictly correlated.

Other fundamental elements that must be considered for OTs, emergency management, business /service continuity and disaster recovery, are represented by reliability and resilience, as illustrated in Fig. 3.

The IMMSSM needs of an Integrated Technological System Framework (ITSF) for its sustenance and for the actuation of all the strategies and procedures, due to the assortment of features, analyses and measures which must be considered in normal and critical circumstances.

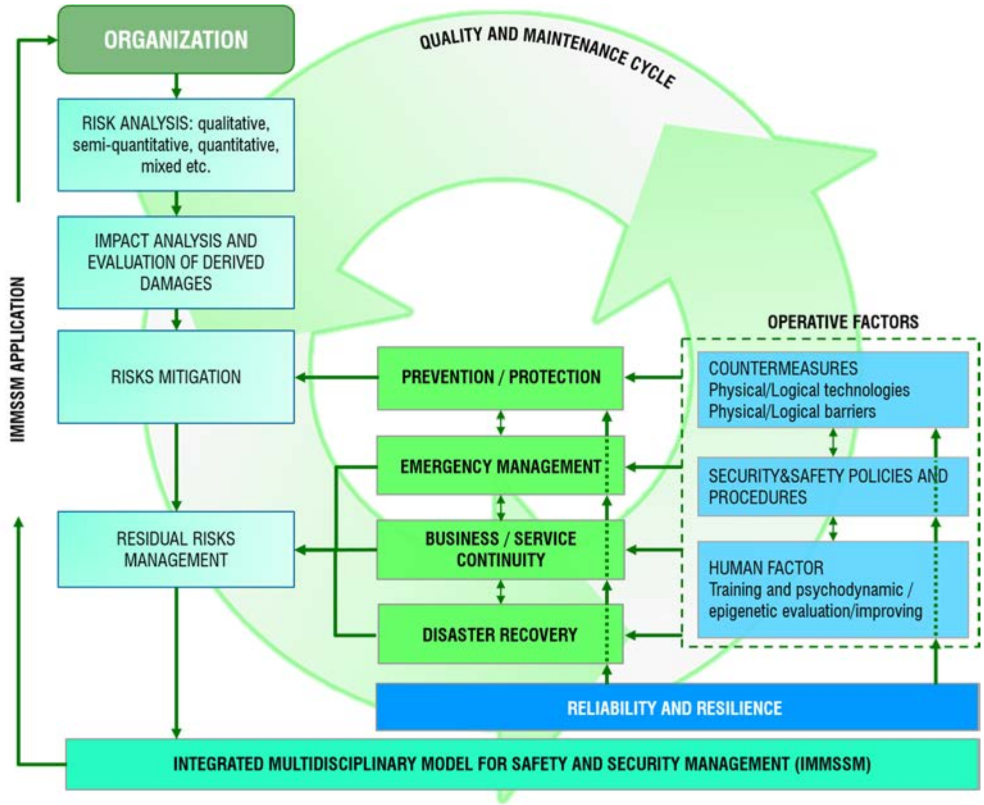
ORGANIZATION
QUALITY AND MAINTENANCE CYCLE
RISK ANALYSIS: qualitative, semi-quantitative, quantitative, mixed etc.
IMPACT ANALYSIS AND EVALUATION OF DERIVED DAMAGES
RISKS MITIGATION
RESIDUAL RISKS MANAGEMENT
IMMSSM APPLICATION
PREVENTION / PROTECTION
EMERGENCY MANAGEMENT
BUSINESS / SERVICE CONTINUITY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

Figure 3: Scheme of the Integrated Multidisciplinary Model for Safety and Security Management (IMMSSM). *(Source: Sostituire figura.)*

The IMMSSM and the related supporting ITSF must consider also analysis, planning and management of the maintenance and quality, as well as the initial realization cost and annual cost.

To create a performing IMMSSM, it is required to improve the use of OTs from a cost/benefit point of view, as shown in the following, 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 are demonstrated in the following.

3 THE INTEGRATED TECHNOLOGICAL SYSTEM FRAMEWORK

To support the IMMSSM, it is strongly recommended the use of a fitting Integrated Technological System Framework based on Internet of Everything (IoE-ITSF). In this way, it is possible to warrant all the objects of the IMMSSM in a flexible and modular way, to translate, at any time, any necessary tuning of the IMMSSM into a rapid and cheap modification of the correlated IoE-ITSF.

This target can be achieved by means of integrated systems [1]–[5] and advanced technologies such as Internet of Everything (IoE) where people, things (mobile terminals,

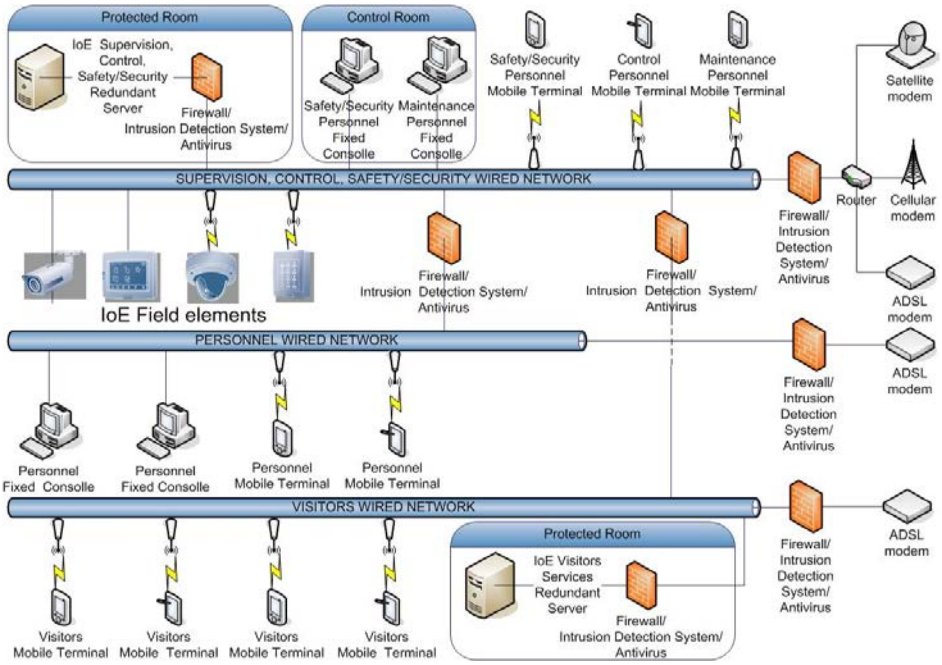
Protected Room
IoE Supervision, Control, Safety/Security Redundant Server
Firewall/ Intrusion Detection System/ Antivirus
Control Room
Safety/Security Personnel Fixed Consolle
Maintenance Personnel Fixed Consolle
Safety/Security Personnel Mobile Terminal
Control Personnel Mobile Terminal
Maintenance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

Figure 4: Scheme of the Integrated Technological System Framework based on Internet of Everything (IoE-ITSF) to support the Integrated Multidisciplinary Model for Safety and Security Management (IMMSSM).

devices, actuators, smart sensors, wearable devices, etc.), data/information/knowledge and procedures are properly connected to attain the required targets [7]–[10]. The general scheme of the proposed IoE-ITSF is shown in Fig. 4.

The IoE-ITSF is characterized by a high modularity which allows for the integration, at any time and in flexible way, of any sort of component which requests to be unified in the IoE system.

The proposed IoE-ITSF is planned to be a widespread framework useful for the most organizations where can be external visitor's. For this reason, the networks used to provide supervision, control and safety/security services, internal personnel services and visitor's services are suitably separated from the physical and logical points of view for security reason [14].

The IoE-ITSF can interconnect all the "IoE objects", providing 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 type of communication means, when any unsafe or risky situation takes place. [14].

It is evident that IoE-ITSF deals with a huge amount of data and, for this reason, it uses proper big data and data analytics techniques to ensure always its best performances [8].

4 IMPROVING FEATURES FOR THE IMPLEMENTATION OF THE INTEGRATED MULTIDISCIPLINARY MODEL FOR SAFETY AND SECURITY MANAGEMENT

To set up an efficient IMMSSM, suitable for a given organization, it is essential to select and integrate the available operative tools (OTs), considering their improving features, such as integrability, which is the scope of the paper.

Generally, due to the funds availability limitation, this goal can be difficult to be realised in the most of contexts. For this reason, it is essential the use of funds in an efficient way so that can be achieved the maximum reduction of damages depending on different threats and the best management of residual risks by means of emergency management, service/business continuity and disaster management.

The considered problem is typically nonlinear, multi-parameters and multi-goals and has already been resolved by means Genetic Algorithms (GAs) [11]–[13], without considering improving features of OTs, such as integrability. In the following, after briefly illustrating the general optimization method, due to the limited space available, the improving feature of integrability of OTs are studied and the related results are illustrated.

The already studied Genetic Algorithms (GAs) [6], has demonstrated to be able of optimizing the use of the operative tools (OTs) available and allows to set up a resourceful IMMSSM for the considered context characterized by an optimal cost/benefit ratio.

Once individuated and evaluated all the threats by means of risk analysis, and all the available OTs, together with the relative realization cost and annual maintenance costs (to contemplate their total cost of the useful life cycle), the GA can find the best mixture of OTs, using only the available ones, which can be used to guarantee the maximum reduction of total risk, respecting the available budget [6].

The process starts with a preliminary and detailed analysis which permits to generate a group of arrays which contain all the information necessary for the GA to run its optimization duty [6]. The arrays are represented by RA (Risks Array), P (Probability Array), D (Damage Array), CM (Countermeasures Array), Procedures Array (PR), Human Factor Array (HF), EM (Emergency Management Array), BSC (Business and Service Continuity), DR.

A suitable fitness function leads the evolution of the individuals of the GA to reach the ultimate whished optimization target. Due to the limited space available, the GA is not illustrated in the following. Anyway, the GA has been tested on more than 800 real and random situations, to get general mean results which can be applicable in any type of context. All the results are got with quite quick converge. Due to the limited space available, only the remarkable results are showed in the following.

A substantial parameter in this type of problem is represented by the mean OT flexibility $\mathrm{MOT}_{\mathrm{flexibility}}$, represented by the mean value, extended over all the OTs, of the number of risks of the P, D, EM, BSC, DR arrays where each OT is used, and the total number of risks of the same arrays. The $\mathrm{MOT}_{\mathrm{flexibility}}$ synthetizes the mean flexibility of OTs and can vary between 1 (all OTs can be used for any activities) and 0 (not any OT can be used for any activities, that is a not real situation). For example, CCTV represents a very flexible OT since it can be applied both to reduce the probability and the damage of a given risk but can be also be advantageous for emergency management, business and service continuity and for disaster recovery. Further, CCTV is characterized by a great integrability, that represents the improving factor which is desired to be studied in the following. It is clear that, the greater $\mathrm{MOT}_{\mathrm{flexibility}}$ and the greater the GA possibility of optimization, as will be shown in the following.

An additional and significant parameter is represented by the investment ratio IR, which is the ratio between the investment cost, represented by the sum of the realization cost and the annual cost, and the total cost of OTs. The IR can therefore vary between 1 (all OTs are used for any activity since the investment permits it) and 0 (not any OT can be used for any activity, since the investment does not permit it, which is an unreal situation). It is clear that the greater IR and the greater the GA possibility of optimization, as will be shown in the following.

In this part, the contribute of integrability of OTs is not considered, to study properly its efficient role in the following, demonstrating all its improving features.

It is also evident that if all the possible OTs (without considering their integrability which is the goal of this study and whose role is studied later) are used, the total risk, characterised by the sum of all considered risks, is reduced at the initially minimum planned level (that is a reduction value equal to 100%) while if not any OT is used, the total risk remains at the initially maximum planned level (that is a reduction value equal to 0%). The total risk reduction (RR) represents an appropriate parameter to quantify the optimization skills of the GA.

The total risk reduction RR, expressed in percentage form, as a function of investment ratio IR, for different values of $MOT_{flexibility.}$, is shown in Fig. 5.

Fig.5 shows how the GA can efficiently reduce the RR as a function of both IR and $MOT_{flexibility,}$ as estimated [6]. If IR increases, more OTs can be used by GA for risk reduction, and the curves grow, according to different profiles, as a function of $MOT_{flexibility.}$

The greater the $MOT_{flexibility}$ and the greater the possibility of GA to perform its optimization tasks. If $MOT_{flexibility}$ tends to 1 (maximum value reachable), the OTs can be used in most activities and this allows the GA to perform its maximum optimization tasks, achieving a total risk reduction of 100% with investment ratio equal to about 0.4. If $MOT_{flexibility}$ tends to 0 (minimum theoretical reachable value), the OTs cannot be used in most activities and this does not permit the GA to best perform its optimization abilities, achieving a total risk reduction of 100% with investment ratio IR equal to about 0.9. Even in this worst case, anyway, the GA can ensure a decrease of IR. In Fig. 5, it is not considered the situation $MOT_{flexibility} = 0$ since this situation is unreal. For this reason, only the situation when $MOT_{flexibility} = 0.001$ is considered, as lower values of $MOT_{flexibility}$ tend to produce curves that are practically superimposed to this last curve.

From the results of the previous research illustrated synthetically above, it is evident that the more the $MOT_{flexibility}$ is close to one and the more the final solution is characterized by a final solution which is extremely efficient from the cost/benefit point of view [6].

It is now important to investigate the role of improving features of OTs, such as integrability, to verify if and how it is capable of contributing in an efficient way, under all the points of view, to the safety and security management, which represents the scope of the paper.

As demonstrated in the following, the percentage of OTs that can be integrated into the IoE system (OTI) can increase the $MOT_{flexibility}$, optimizing the cost/benefit ratio of the final solutions for safety and security management.

A substantial parameter to validate the effect of OTI is represented by the $MOT_{flexibility}$, since it greatly impacts the GA ability of attaining the desired target in an effective way, as shown in Fig. 5.

To verify the improving features of OTI, the above GA simulations were repeated, varying OTI from 0 (none OTs can be integrated within the system) to 100% (all the OTs can be integrated in the system) and the $MOT_{flexibility}$ has been calculated as a function of OTI (expressed in percentage). In Fig. 6, the $MOT_{flexibility}$ as a function of the percentage of OTs that can be integrated into the IoE system (OTI), for different values of initial $MOT_{flexibility}$ (0.001, 0.2, 0.4, 0.6, 0.8) is shown.

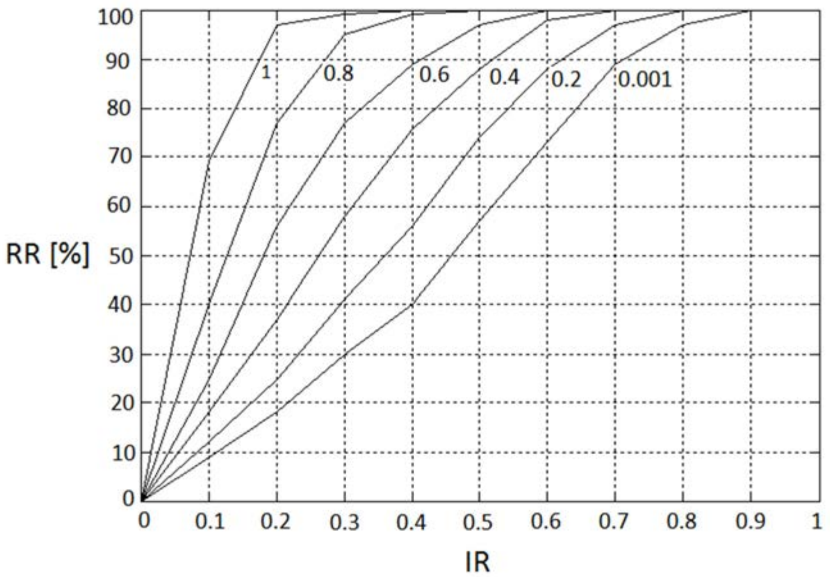

Figure 5: Total risk reduction (%) as a function of number of investment ratio IR for different values of $MOT_{flexibility}$.

As it is possible to see from Fig.6, the increase of the percentage of OTs that can be integrated into the IoE system (OTI) increases the $MOT_{flexibility,}$ for any kind of initial value of $MOT_{flexibility}$.

Since the RR illustrated in Fig. 5 has been considered for 4 significant values of $MOT_{flexibility}$ (0.001, 0.2, 0.4, 0.6, 0.8), the same was made in Fig. 6.

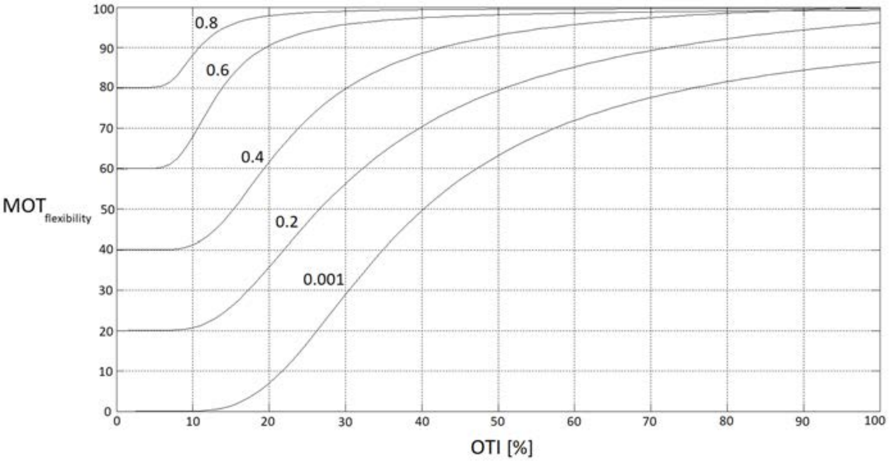

Figure 6: $MOT_{flexibility}$ as a function of the percentage of OTs that can be integrated into the IoE system (OTI), for different values of initial $MOT_{flexibility}$ (0.001, 0.2, 0.4, 0.6, 0.8).

Results shown in Fig. 6 reveal that when the percentage of integrated OTs is null (OTI=0 %) the $\mathrm{MOT}_{\mathrm{flexibility}}$ remains obviously the same for the 4 considered initial values (0.001, 0.2, 0.4, 0.6, 0.8). As soon as the percentage of integrated OTs increases, due to increase of their performances depending on the mutual interaction, the $\mathrm{MOT}_{\mathrm{flexibility}}$ augments in a substantial way for lower initial values of the $\mathrm{MOT}_{\mathrm{flexibility}}$ itself (0.001) and in a less significant way for greater initial values of the $\mathrm{MOT}_{\mathrm{flexibility}}$ itself (0.8).

When all OTs are fully integrated (OTI=100%) the $\mathrm{MOT}_{\mathrm{flexibility}}$ reaches the maximum level for the 4 considered initial values (0.001, 0.2, 0.4, 0.6, 0.8). In particular, for greater initial values of $\mathrm{MOT}_{\mathrm{flexibility}}$, it is possible to reach a final value of $\mathrm{MOT}_{\mathrm{flexibility}}$ close to 1 (maximum level of flexibility of OTs which permits to achieve the minimum level of risk with the lowest possible cost) even with a quite reduce value of OTI.

Anyway, it is possible to see that the $\mathrm{MOT}_{\mathrm{flexibility}}$ increases in a more significant way for lower initial values of itself, showing the importance of integration of OT into the IoE system.

The above quantitative results demonstrate how the percentage of OTs that are integrated into the IoE system represents a vital need to create an efficient IMMSSM from the cost/benefit point of view.

5 CONCLUSIONS

A multidisciplinary model for safety and security management and the related integrated technological system framework based on IoT/IoE has been illustrated, studying also the significant role played by the integration of the elements (operative tools or OTs) that compose the model itself, thanks to a proper genetic algorithm studied for the specific context.

The quantitative results that have been attained demonstrate the valuable importance of integration of the operative tools of the model that can be properly achieved thanks to integrated technological systems based on IoT/IoE.

REFERENCES

[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, *Proceedings of the Fifty Annual IEEE International Carnahan Conference on Security Technology*, pp. 107–114, 2016.

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

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

[9] Garzia, F. & Papi, L., An Internet of Everything based integrated security system for smart archaeological areas, *Proceedings of the Fifty Annual IEEE International Carnahan Conference on Security Technology*, pp. 64–71, 2016.

[10] Garzia, F. & Sant 'Andrea, L., The Internet of Everything Based Integrated Security System of World War I Commemorative Museum of Fogliano Redipuglia in Italy, *Proceedings of the Fifty Annual IEEE International Carnahan Conference on Security Technology*, pp. 56–63, 2016.

[11] Goldberg, D.E., *Genetic Algorithms in Search, Optimisation and Machine Learning*, Addison-Wesley, 1989.

[12] Goldberg, D.E. & Deb, K., *Foundations of Genetic Algorithms*, Morgan Kaufmann, 1991.

[13] Holland, J.H., Genetic algorithms, *Scientific American*, pp. 66–72, 1992.

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

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

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

[17] Lombardi, M., Guarascio, M. & Rossi, G., The management of uncertainty: Model for evaluation of human error probability in railway system, *American Journal of Applied Sciences*, **11**(3), pp. 381–390, 2013.

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

[19] Guarascio, M., Lombardi, M. & Massi, F, Risk Analysis in handling and storage of petroleum products, *American Journal of Applied Sciences*, **10**(9), pp. 965–978, 2013.

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

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