The Economy of ICT Risk Following a Bio-Inspired Model

Aurelio La Corte[1], Marialisa Scat a[2]

Department of Electrical, Electronics and Computer Science, University of Catania
A. Doria Street 6, Catania, Italy

[1]lacorte@dieei.unict.it; [2]lisa.scata@dieei.unict.it

***Abstract*- Information security stands for protecting data and information systems from unauthorized access, use, modification or destruction, to ensure the CIA requirements, confidentiality, availability and integrity. Information and communication technology world is facing with security issues due to many challenges in network architecture and communication paradigm. The design of an ICT infrastructure cannot ignore the technological and social analysis, economic aspects, and now with the sustainability. This paper analyses the safety of these systems and propose a new paradigm to manage the security through a bio-inspired approach. This model evaluates the information assets of data, using three steps, Analysis, Assessment and Management, identifying the procedures, the weaknesses and the threats. We present a security management architecture and a bio-inspired model to evaluate the risk and the probability of a probable threat, based on the failure analysis. The goal is to realize the real state of security degree of the system, acting into it in order to optimize the global safety, picking out the business strategic decisions and the economic choices, finding the perfect condition that allows combining the risk of failure, the hazard function, the risk of economic losses and information losses affecting security requirements. This approach could be applied in the future to investment models on information and communication architectures.**

Keywords- ICT; Security; Risk Analysis; Bio-Inspired; Economic Investments

I. INTRODUCTION

In recent decades we have seen extraordinary developments in communication technologies and network architectures that have produced a lot of information networks. Information is defined in [4, 5] as an important business asset. Information can be disseminate and share in many forms, and this implies a greater range of possible areas of weaknesses. In recent years, the ICT has been characterized by several challenges. The next future requires being closer to the user, simplifying the plurality of resources and interacting with social environment through user interactions experiences, convergence, ubiquity and dynamicity, which causes a social behavior that could influences the global safety. It is expected that the next generation of information systems such as next and new generation network, quantum communication networks and Interplanetary Internet, are characterized by a layer of information and communication services should be easily accessible by users in a transparent, manner. This new type of ubiquitous network will include, the social networks, wearable networks, in-body molecular communication networks, self-organizing networks, self-cognitive and cognitive radio networks. This perspective implies that every user and every object shared is a node of the networks, and it could be a social measure of influence and a communication measure. The complexity of existing systems increased complexity with the size of networks, their social, mobile, self- organized nature, the need for prediction of potential unexpected failures. Essentially, we need an information and communication system ruled by sustainable processes in terms of energy consumption, quality and security. A sort of ecosystem could guarantee efficiency, robustness and scalability. Most of the existing communication systems and next generation networks cannot be treated using the paradigms of conventional network, which are not able to support these new features. We need new paradigms to guarantee scalability, heterogeneity and complexity. These have been addressed successfully by nature. The changing nature has produced artifacts that are actually the approaches to the solution and can address many of these challenges. The biological systems are based on a small number of simple rules that produce effective models to manage cooperation models, among nodes of the network. In general, the biological processes have the intrinsic following features:

- Adaptable to evolution.
- Robust to threats and failures.

- Able to achieve complex behaviors.
- Able to learn and evolve as new conditions are applied.
- Efficient managers of resources.
- Able to self-organize into a fully distributed, resulting in a collaborative manner an efficient equilibrium.
- Able to survive in the face of harsh environmental conditions.

Today's networks are characterized by mobile nodes and social behavior. Your freedom to share and movement, increase the global knowledge of the network and of each individual, but worsen safety situation. An event of threat can stop an individual process and cause significant economic losses, and at the same time if the single node has many interactions, that event can damage also his network of nodes. The extent of interaction and influence between nodes could in fact give a measure of risk and security of the network, with the correct assessment of the dynamics and topologies. We need to evaluate every aspect to choose the right countermeasures and make appropriate investments. This requires strategic planning, refers to the type of network, the value of the information that you want to protect and entities involved. This involves writing new analysis models and new rules, as they are the possible new threats and weaknesses of the system. The goal is to provide a strategy for analyze and manage new and general that it can encompass various technologies. In [11], the subject strategy is defined as a science and art of planning which involve accurate methods. After a Section about Related Work, the paper is organized as follows: Section III is about the risk analysis with bio-inspired approach; Section IV presents the proposal of security management architecture; Section V the mathematical model bio- inspired for ICT system and in the Section VI the model that concern the economical investments on security and at last Conclusion and Future Works.

II. RELATED WORK

Information and communication technology is the study of design, implementation, support and management of information systems. Bruce Shneier (Chief Security Technology Officer of BT) gives this definition: "Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected". The idea of security cut across a broad range of research areas. In a context in which is possible to invests often on semantic search, and digitizing dematerialization, mobile communications, multimedia and pervasive technologies, cloud computing and social networking, we risk to trust the network more than we should do and we can lose control of the data for lack of knowledge of the tools that are possible to use. A strategic approach would evaluate each part of the system, the type of users, the habits of them, the environment and the context, the possible links, the assets involved, the processes, the presence of any social network that would change the dynamics of virus spread, which would become very uncontrollable. The need for security is closely tied to the value of information: this is much higher, the more we are willing to spend to protect it. For this, bringing together of different aspects, is possible to introduce in the ICT world a methodology for strategic analysis and risk management socio-economic and technological global system, as an indispensable tool for planning of a complex model of security management. A consolidated study on security degree of an ICT (Information and Communication Technology) system is still missing, but we can find many different models applied to specific architecture. Protecting information and networks infrastructures should not be considered secured of inevitable attacks, but we need to provide analysis models that could be helpful in preparation for future damages [17]. From statistical reports of 2010 there are worrying data under so many points of view [18, 19, 20, 21]. More papers like [12, 13, 14, 15] investigate about ICT applications and the new trend of it. About risk models there are many studies and survey of threats [6, 7, 8]. The similarity between biological processes and computer security problems has long been recognized and studied, over the years. Adelman, in 1987, introduced the term computer virus, inspired by biological terms, such as Spafford, with the term form of artificial life, referring to the virus, and so on. In fact there are many biological terms such us worms, virus, which have been borrowed to name computer attacks. Such usage suggests the comparison with biological diseases [22]. If we consider information systems and biological systems, they share several properties such as complexity and interactions between individuals of a population (asset of the information systems). There are many analogies between computer systems and biology, and many research studies support the idea that nodes of a network are such as the individual of a population, and the interactions between nodes as the relationship of people [23, 24, 25]. The research in this area has mostly focused on epidemiological studies of disease dissemination [7, 8, 9, 26]. The risk is similar to a disease, caused by the action of threat that takes advantage of the weaknesses. The result of the impact of this event can be distorted because of other variables, the explanatory variables, or confounding variables (confounders) used into the Cox regression model [2, 3], and are useful to detect and predict cause and effect of a threat. A broader bio-inspired analysis is the survival analysis. In some papers as [6, 7, 8] the authors develop a mathematical approach to risk management and the detection of failures requires that what types of failures should be defined. This analysis is important to estimate the expected benefit of a security investment. Everything related to business investment begins with the strategic decisions. To benefit from the investments it is essential to understand where, how and when to apply them [6, 7, 8].

III. ANALYSING THE RISK WITH BIO-INSPIRED APPROACH

The need for protection of personal profile and of personal information is increased. This need is due to the pervasive presence in the network anytime, anyway and anywhere. Communications of today favor the interconnectivity, interactions and sharing of data between users. In the future the amount of data that will form our profile in the network will continue to grow, so we need to ensure privacy, and we need to rewrite dynamically the security policies. A tool for global analysis and management could provide the paper procedure to act in the context, in which information has a certain weight that increase that information is exchanged between users. The networks are evolving towards convergence maintaining the social and mobile nature. The architecture forms a single complex, adaptive body, able to provide services and applications. In biological world, the organisms are complex bodies, they are part of a community, and they could share resources and information, and live in an interconnected environment. We propose this research paper using the concepts of biological systems that can inspire ICT models. The term virus is something that affects suddenly a computer system or a network. It could be a simple malicious code or a more complex event. In both cases the virus is the expression of a threat that exploits vulnerability. In biological and health context a disease is the result of an exploiting. A bio-virus affects a weakness of a biological entity and cause the disease. So, there is a very close similarity, well studied in many research works [6, 7, 8]. The question is how similarities, already useful to design new network infrastructure, could be useful to inspire methodologies and strategies of risk analysis and management, and security of ICT systems. Viruses and worms were not the only biological models used in investigating information security threats. If we consider the next generation information systems, they are envisioned to be characterized by an invisible and ubiquitous cloud of information and communication services, which should be easily accessible by users ensuring privacy and quality. The new networks have to face with scalability, heterogeneity and complexity which are new by-products of the challenges in ICT environments in the last few decades. They have been successfully dealt with by the nature for quite some time. The dynamics of many biological processes and laws governing the mare based on a surprisingly small number of simple generic rules that allows:

- effective collaborative;
- task allocation;
- effective resource management;
- synchronization;
- protection against pathogens;
- relative stable equilibrium state;
- adaptive to the dynamicity of environment features and circumstances;
- robust and resilient to the failures caused by internal and external agent;
- high complexity, high connectivity and extensive interaction between components/nodes/systems;
- numerous entry points;
- complex behaviours with limited set of basic rules;
- able to learn, evolve and self-organize;
- energy efficiency.

The two fields have a much stronger connection that one might expect. All these features that characterize the biological systems are due to millions of years of evolution in biology, thus we can guide ICT based on these principles. The key of drawing useful correlations between biological world and ICT world is a proper selection of topics and a right comparison.

The most important requirements for the future are:

- adaptive, pervasive, opportunistic and ubiquitous infrastructure of networks;
- large-scale networking;
- heterogeneity, coexistence, cooperation and social-friendly environment among different types of networks;
- internet of things;
- self-properties: self-organization, self-management, self-learning;
- security, quality of service and energy efficiency (e.g. Sustainability of ICT).

This paper has not the aim to find similarities between the social and biological world of ICT, but it has the aim to detect

among the similitudes, which of them is more suitable for analysis and management of safety. The similarities between the various natural processes and those strictly related to the networks have already been extensively studied [7, 9, 10]. Epidemiology is the one that is best suited to connection between biological world and ICT disciplines. As defined in [16], Epidemiology is a methodology, a technical approach to problems, a "philosophy". Epidemiology is a "different" way to study health and disease, and it is cross-science. Epidemiology is working with the clinic and preventive medicine. Making use of mathematical-statistical models, this discipline allows you to analyses the causes, spreading effect and impact of the illness. Through epidemiological analysis we acquire information about the history of the disease, we can investigate about causes and design a control process with monitoring tasks. Information assets and vulnerability associated to its, can be treated as individual of a population with weaknesses. Both are subject to threats of a different nature. We propose an analysis and management model in order to avoid that threats exploit the vulnerabilities. The epidemiology studies these mechanisms in terms of population, so it lends itself for future analysis, in the field of ICT, concern social networks and diffusion of the community behavior. The risk is the probability that a threat acts damaging a system, individual nodes or the entire network. A key role in the risk analysis is the assessment of variables that may confuse the result or the prediction. These are evaluated in the Cox Model [2, 3] and they are called "confounding variables", or "control variables" in econometrics. The explanatory variable is useful in understanding the relationship between cause and effect of a general threat and it is a variable which is used also to predict important challenges of another variable. In the next section we show the steps of the process proposed.

IV. SECURITY MANAGEMENT OF COMMUNICATION SYSTEM

A. Introduction

The proposed model in this paper shows a process of analysis divided into three stages. Each step introduces a part of assessment and analysis essential to the achievement of the ultimate management of the system. The focus of this analysis is the information exchanged. This comes in the form of information assets, which are analyzed and classified in order to identify weaknesses and spreading points of threats. The ultimate goal is to optimize the risk level of the system, making prediction about any damage, locate the appropriate action against it, and finally, manage the security of the system. Thus, based on information security management (ISMS) [4, 5], which is part of overall management system, a business risk approach is taken to establish, implement, operate, monitor, review, maintain, and improve information security. Safety management must not be understood as something purely technical and practical, but as a logical process to identify, assess and analyses the overall information system. To establish ISMS, we first need to identify the assets of the system because any activity uses the resources and information to enable the transformation of inputs into outputs. We choose a strategy model based on three steps, which are "*situation*", "*target*", and "*path*":

- Situation: The current environment of the communication system;
- Target: the strategy goal and the desired managed information system;
- Path: the method of moving from the situation to obtain the target.

B. Security Management Process

The Information Security Management process is displayed, as in Figure 1, in the form of layered architecture, where each level corresponds to a fundamental step. The level of Assessment is the first step of the process, as in Figure 2. This level includes all the procedures and processes for evaluating the general environment, in its physical components and logical components. It is characterized by three steps of evaluation and modeling:

- Environment Assessment;
- Asset Modelling;
- Vulnerabilities and Threat Taxonomy.

The information assets are the main features of the system. In the first level the aim is to evaluate each aspect related to its. This stage of model proposed allows us to classify and modeling each component, identify the process and establish the logical assets. We can understand interactions between logical parts of the system, involved in the sharing process. In this step we detect and classify also weaknesses and threats related to asset level. Then, having a full knowledge of the systems, in terms of entities, processes and assets, we can introduce in the second level the statistical analysis [9, 10] that applied to ICT, allows us to evaluate distribution over time of system failures. The failure time analysis identify the times when the system is damaged due to the action of a threat. Many failures events could increase the risk of the system, because the outlooks of attack worsen. For this reason, an action should be carried out for monitoring the risk level. This level may also remain stable, despite having a series of failures events over time, in that knowledge of the causes and detection of the damage already imply an awareness of system security. Sometimes we do not know the origin of certain events or we do not understand to which vulnerability they are related, or they happen after the end of observation period. We call these events "censored data" and can provoke an

increase of risk degree. So the risk could rise even in the absence of failure events. The target of this analysis is to calculate the extent quantitative and qualitative risk, in order to understand the state and the degree of security of our system by studying the statistics of failure. As in Figure 3, there are two steps for the Failure Analysis, the first is Failure Data Definition, and the second is Failure Time Distribution. About the Risk Analysis, the model has the aim to calculate three functions, Failure Function, Survivor Function and Hazard Function. After the two levels of analysis, the ultimate goal is to have a clear vision of how to manage the security of the system. The phase of management is another step in our stack case. This phase, as in the Figure 4, allows us to evaluate the countermeasures and all actions to protect the environment, the appropriate policies. At this stage we acquire the know-how, can decide the economic investments, have the tools needed to make an assessment of the degree of safety of the system, and we can make the prediction of the main events, or which fall under the general statistics.

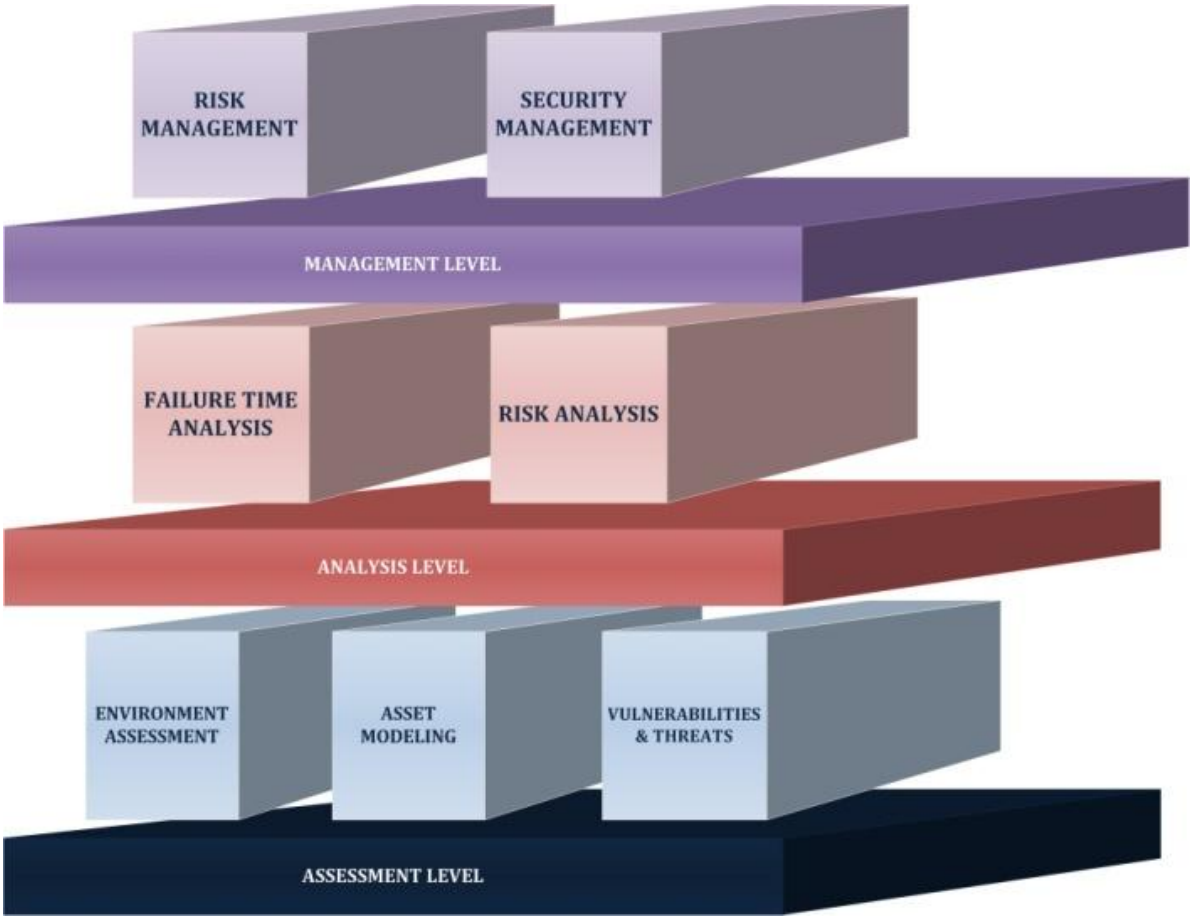

Fig. 1 Information Security Management Architecture

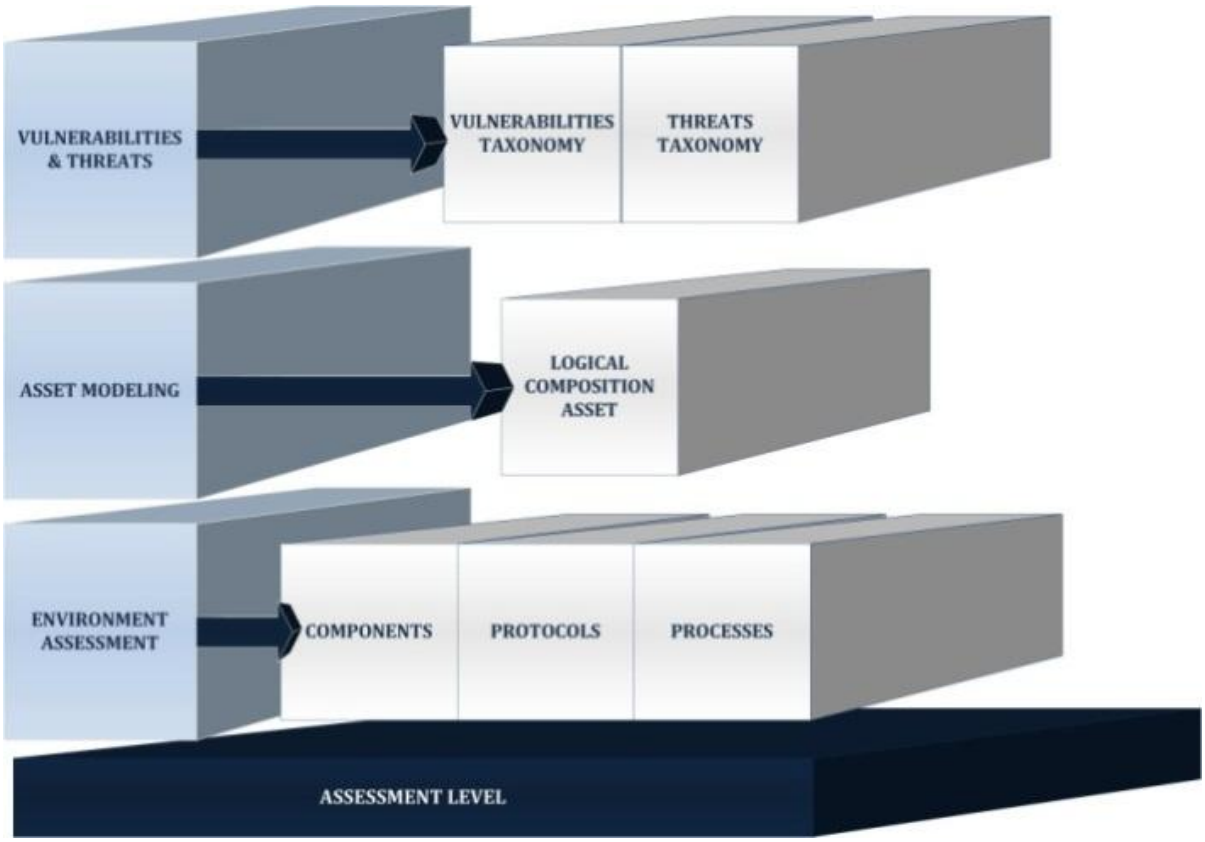

Fig. 2 Assessment Level

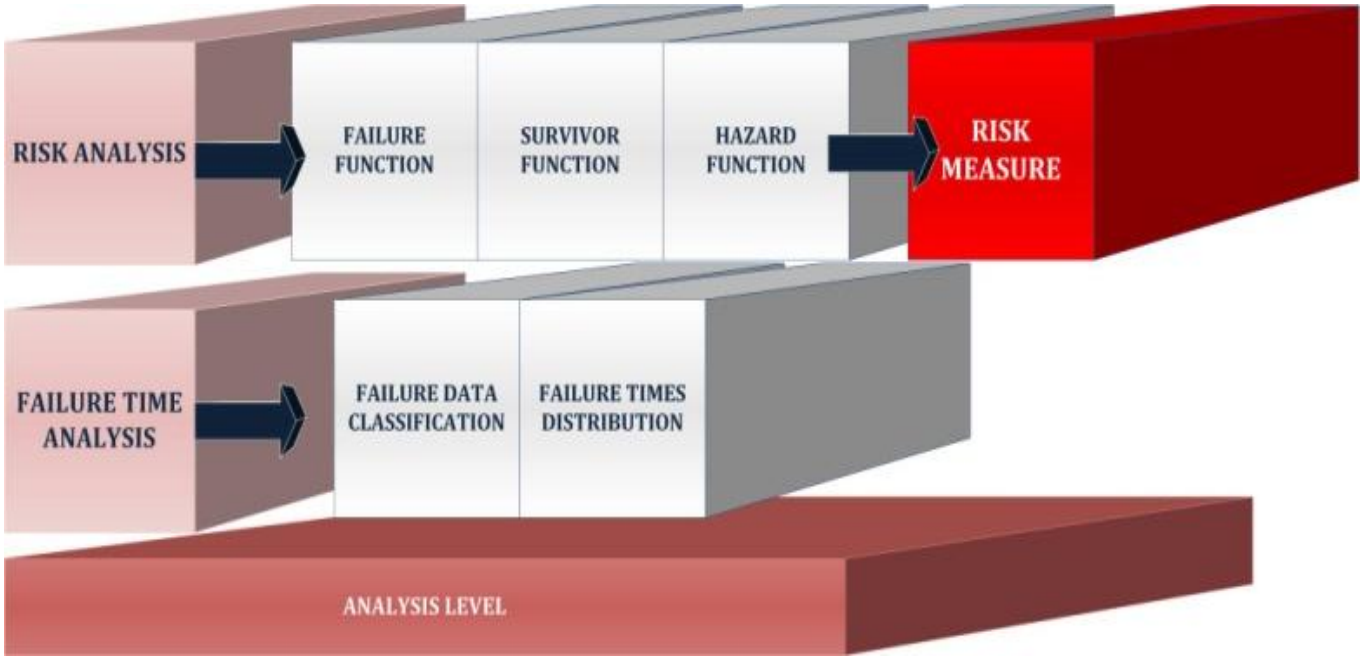

Fig. 3 Analysis Level

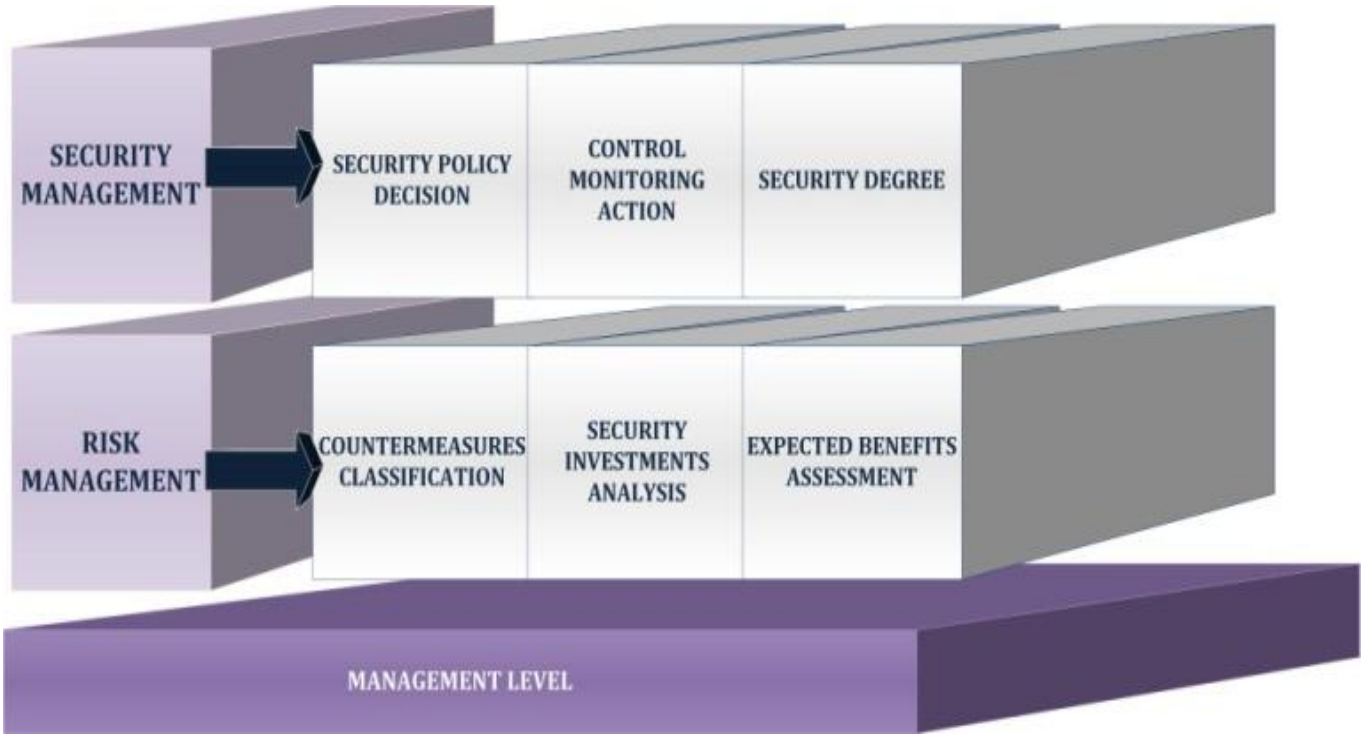

Fig. 4 Management Level

V. BIO-INSPIRED MODEL FOR FAILURE ANALYSIS ON ICT

The model proposed in this paper has as main purpose to evaluate not the best practice, that the most satisfactory for the system in question. To assess what decisions taken regarding investments in security, it is good to consider every aspect, otherwise left to chance, while remaining idea that does not exist a fully safe, so any procedure, estimate the most probable events, and the impacts that ensue. This model suggests a procedure, to introduce in security evaluation, a step-by-step strategic decision process. The historical data about damages and requirements are needed to understand the system, a procedure is needed to assess where, when and how make investments to safe it. In [6, 8] the authors develop a mathematical approach to risk management to help the economic evaluation of investments. They try to quantify security, seen as the inverse of risk. The failure happens when there is a compromising of confidentiality, availability and integrity of data. We can define different type of assets inside the system. Some of its can communicate with external network and have numerous access points which can result weak to several threats. The failures are classified on the basis of the assets that are involved, in order to evaluate all aspects. The safety requirements rule investments on the basis of failures time analysis and the importance we place on privacy. There will be parts of the system that must be taken safer than others, because manage information which high value. So, detection of failures requires that we decide what type of damages we want to avoid and on what kind of data we want to invest. The failure time distribution, for this reason, must assign a weight to information shared following the approach presented in [27]. Following the failure time analysis and epidemiology definitions and methodology we pull out these parameters:

- Frequency: $F(t)$
- Distributions on: $F_a(t), F_p(t), F_s(t)$
- Determinants: $H(z, \delta_1), H(th, \delta_2)$
- Health/Disease: S_{dICT} is function of $F(t)$
- Populations: assets of the systems
- Social Relations: processes and interaction between communication nodes
- Epidemic Risk: Risk propagation through ICT systems.

So, if T is a non-negative failure time random variable, $F(t)$ and $S(t)$, as in (1), are respectively, failure time distribution and survival distribution in an homogeneous population as explained in [8] for discrete and continuous distribution. Then the Hazard Function as in (2) is:

$$F(t) = P_r(T < t) \qquad S(t) = P_r(T \geq t)$$

$$H(t) = -logS(t)$$

VI. SECURITY DEGREE AND ECONOMICAL INVESTMENTS

The importance of security is directly proportional to the value of information in any ICT system. Who decides to invest in safety should be able to tell if the planned expense of the infrastructure improvement, such as protection of assets of the system is needed. They should also be able to assess, in advance, the expected benefits, from this investment for proper strategic planning. The value of information increases significantly if it shared and exchanged through nodes of networks and ICT systems. Different systems and nodes can interact in many ways through different means. Thus, to design a security infrastructure a properly assessment of the importance degree of the investment in security is necessary. Thus, we can define the "Information Value" of an ICT system that is function of three parameters:

$$V_{ICT} = f(C, S, E)$$

C= Information Constant of the System.

S= Sharing Variable of a Communication Process.

E= Environment Variable of the System.

C is a parameter referred to the information itself, the starting value of the information packets. *S* is added when this information is shared, and finally E is the context variable of the environment and of the interactions involved through system. If we consider two systems we have the following equations:

$$V_1^{\,0} = C_1^{\,0} + E_1$$

$$V_2^{\,0} = C_2^{\,0} + E_2$$

Then, the first system becomes the source of sharing. It exchanges a quantity of information with the second system, involving certain assets and communication processes to share different types of data, so at t_1:

$$V_1 = V_0^{\,1} + S_{12}(t)$$

$$V_2 = V_2^{\,1} + S_{12}(t)$$

S_{12} is the sharing variable of this communication between these two system:

$$S_{12} = \gamma_{12} C_1 + \mu_{12} E_1 + \beta_{12} E_2$$

It depends on three factors:

- Information constant of the source of sharing that is weighted by a value, which we call the sharing fraction.
- The environment variables of the two systems that are weighted by two constant, μ_{12} and β_{12}. These constants depend on the assets and processes involved.

In the time interval of the interaction, the value of information shared grows according to this trend, depending on S_{12} .

$$V_{s12} = S_{12} t$$

Therefore, we define I_s as the "*Importance Security Factor*". This factor is an essential parameter for all ICT systems. It allows for evaluation of the importance of the strategic planning of security for the entire system. It allows for evaluation of the importance of the strategic planning of security for the entire system. For a generic system, i, that wants to share and communicate with a generic system, j, the Important Security Factor is a function of sharing variable S_{ij} .

Thus, for the first system of our example:

$$I_{S1} = f(S_{1j}) \quad with\, j = 2, \ldots, n$$

$$S_{1j} = \gamma_{1j} C_1 + \mu_{1j} E_1 + \beta_{1j} E_2$$

$$I_{S1} = a_{12}\, S_{12} + a_{13}\, S_{13} + \cdots + a_{1j}\, S_{1j} + \cdots + a_{1n}\, S_{1n}$$

The Importance Security Factor is the linear combination of S_{1j}, and a_{1j}, depends on the weakness of the system and the threats.

$$a_{1j} = th + w$$

If S_D is the "*Security Degree*" of the system we can say that:

$$I_{Si} \propto \frac{1}{S_D}$$

$$S_D \propto \frac{1}{RISK}$$

The security decisions are generally taken outside of the initial strategic plan, or they are not suitable to the systems. In many cases the security actions are made after damage occurs when a network threat successfully exploits a vulnerability of the system. A security investment does not stem only from a statistical assessment of threats and vulnerability through taxonomy, r from the subsequent action that is taken as the result of an attack that has already happened, but from the entire analysis of the architecture, assets, processes and interactions with other systems. To benefit from investments it is essential to understand where, how and when apply them. The Security Investment in a strategic plan of security of an ICT system is proportional to the Risk degree and the Importance Security Factor, which is the inverse of the Security degree of the system:

$$SEC_{INV} \propto \frac{Risk \cdot I_S}{S_D}$$

In this way we can demonstrate that to decide the optimal investment we must address three issues:

- Assessment of I_S;
- Risk Analysis to estimate the Risk Degree of the system;
- Assessment of the Security Degree of the system through the analysis of existing countermeasures, policy, strategies.

Following the steps of the proposed architecture in the previous section and the bio-inspired approach, we can summarize four steps which can be identified to design security plan with that approach:

- Identification, Assessment, Analysis of similarities and analogies among biological system and information systems;
- Classification of Methodologies, Positive Aspects and Drawbacks;
- Selection of Macro areas of Interest;
- Understanding of biological models;
- Design and Engineering of Bio-Inspired Approach.

Following this methodology we can estimate the security degree. The security degree is a function of $F(t)$ and $S(t)$ and it is the inverse of H(t). With S_{dICT} security degree and $R_{ICT}(t)$ the risk measure:

$$S_{dICT} = R_{ICT}(t)^{-1}$$

R is the function of $F(t)$, Explanatory Variable and Threat. Following the Cox Model [2] [3], $H(z, \delta_1), H(th, \delta_2)$, identify respectively the vectors of explanatory variables and threats weighted on the coefficient δ_1, δ_2 as in:

$$R_{ICT}(t) = \gamma F_s(t) H(z, \delta_1) H(th, \delta_2)$$

Thus, before investing the money, it is necessary to make appropriate assessment. Resuming the previous definitions and equations and following the bio-inspired approach, we can consider the system in two different cases, with and without investment, and evaluate it with hazard function.

The hazard function is defined as:

$$h(t) = \frac{number\ of\ assets\ experiencing\ a\ failure\ in\ interval\ beginning\ at\ t}{(number\ of\ assets\ surviving\ at\ time\ t) \cdot (interval\ width)}$$

Thus, we have that:

$$h_1(t) is\ the\ hazard\ function\ with\ security\ investment$$

$$h_0(t) is\ the\ hazard\ function\ without\ security\ investment$$

We can relate the two quantities through the following relationship:

$$h_1(t) = k \cdot h_0(t)$$

k is the Hazard Ratio.

If we decide to invest on security with an investment i, the benefits that we expect to have are:

$$E_{NB}[i] = p_0 L^I - p_i L^{II} - i$$

Where $p_0$and p_i are respectively the loss probability for the system and the loss probability after we invested. L is the Loss function and a positive value of $E_{NB}[i]$ means that the investment has made benefits.

The Loss function for an ICT system is:

$$L = L_{inf} + L_E$$

where L_{inf} is the loss of information in terms of security requirements, that are confidentiality, availability and integrity and L_E is the economic loss cause from the attack.

Thus, we have that:

$$E_{NB}[i] = p_0(L^I_{INF} + L^I_E) - p_i(L^{II}_{INF} + L^{II}_E) - i$$

If we consider the Hazard Ratio, by hypothesis, k:

$$k = \frac{p_i L^{II}}{p_0 L^I}$$

We identify two conditions to have a good performance in terms of security after investment:

- $E_{NB}[i] > 0$
- $k < 1$

The first condition ensure the positive benefits after the investment i, the second condition ensure that the risk, after i, is less the risk before it.

$$E_{NB}[i] = p_0 L^I (1 - k - i)$$

Thus, the perfect condition is:

$$k + i < 1$$

This condition allows combining the risk of failure, the hazard function, the risk of economic losses and information losses affecting security requirements. Investment has to follow the approach proposed in the previous sections, and it is function of the decisions making during each phase of the Information Security Management Architecture:

$$I = f(Assessment, Analysis, Management)$$

The investment has to follow the system security requirements and has to comprise the evaluation of the importance of the vulnerability and the probable breach. Many times the investment is not done for vulnerability with a great risk and with a low probability, but sometimes, especially some companies decide to invest in security for real and probable vulnerability with medium risk but high probability of breach. Making decisions concerning investments in information security, his approach requires calculation of net benefits expected to result from the economic strategy of security management linked to the information system analysis and assessment. Investment does not stem only from a statistical evaluation of threats and vulnerabilities, or from a next action, as a result of an attack already happened, but from the study of the entire system.

VII. CONCLUSIONS

The proposed approach allow to present a new model and new strategy to investigate about threats, predict and detect

failures, protect information assets, assess risk and manage security. The approach is based on social, bio-inspired and economic features. It considers every aspect of the system and the currency in order to manage security. The bi-inspired strategy helps us to apply methods of analysis and evaluation, proper to the clinical world, such as epidemiology. At the same time the social approach, that we are going to develop in the future works, allow us to evaluate the importance of relationship and interactions, in which information is exchanged. The economic approach serves us to give a justification for investment spending to secure our ICT environment. In this model, we face the problem of security, for the purpose of economic investment as appropriate. We want to address as future works, the social aspects of security based on interactions, which on the one hand encourage the sharing and the growth of knowledge, then anticipate and keep users informed of damages to the network, on the other hand favor the diffusion of threats. The next future, for further works, issues that will rule the new generation network are classified in three topics, Security, Quality and Energy consumption. To understand how an information and communication system could add value to guarantee good performance of every systems in terms of these three issues or how improve ICT system itself based on the estimate of risk, quality and energy consumption, both questions are open problems. The key aim is to have a social community of networks, smart and sustainable, that shares information and knowledge in a secure way, focusing on energy consumption issues, maintaining the work of the network more efficient, balancing costs of investments and expected benefits. This will result in significant challenges for communication and information provision, based on required scalability, efficiency in forwarding, heterogeneity re-configurability, security and dynamicity. In this context the need is to find an optimal set of rules and method, to implement and develop technologies to guarantee security, quality and energy consumption and awareness of these issues, to allow the future of ICT also in term of green sustainability.

REFERENCES

[1] B. Shneier, Architecture of privacy, IEEE Computer Society, Security and Privacy, 2009.

[2] D. Roxbee Cox and D. Oakes, Analysis of Survival data, CHAPMAN & HALL/CRC, 1984.

[3] D. Roxbee Cox, Regression Models and life-tables, Journal of the Royal Society, Series B (Methodological), vol. 34, No. 2, 1972.

[4] International Standard ISO/IEC 17799:2005, Information Technology Security techniques. Code of Practice for information security management, 2nd edition.

[5] International Standard ISO/IEC 27001, Information Technology Security techniques. Information Security management System-Requirements.

[6] J. C. H. Ryan and D. J. Ryan, Performance Metrics for Information security Risk management, IEEE Computer Society, Security and Privacy, 2008.

[7] J. C. H. Ryan and D. J. Ryan, Biological System and models in information Security, Proceedings of the 12th Colloquium for Information System Security Education, University of Texas, Dallas, 2008.

[8] J. C. H. Ryan and D. J. Ryan, Expected benefits of information security investments, Computer and Security, ScienceDirect, www.sciencedirect.com, 2006.

[9] J. M. Lachin, Biostatistical Methods: The Assessment of Relative Risks, John Wiley & Sons, New York, 2000.

[10] J. D. Kalbfleish and R. L. Prentice, The Statistical Analysis of Failure-Time Data, 2nd edition, Wiley, 2002.

[11] V. Leveque, Information Security: A Strategic Approach, IEEE Computer Society, J. Wiley and Sons, 2006.

[12] R. Lenz and M. Reichert, IT Support for Healthcare Processes, in Business Process Management, 2005.

[13] L. Willcocks, W. Currie, and S. Jackson, "Radical Re-Engineering and information Systems: evidence from UK public Services, in Fifth European Conference in information Systems. Cork, 1997.

[14] M. Buckley, H. Kershner, K. Shindler, C. Alphonce, and J. Braswell, Benefits of using Socially Relevant projects in computer Science and Engineering Education, in SIGCSE, 2004.

[15] R. Heeks, ICT4D 2.0: The Next phase of Applying ICT for International Development, Computer, 2008.

[16] W. H. Murray, "The application of epidemiology to computer viruses", Computer & Security, vol. 7, issue 2, 1988.

[17] M.T. Dlamini, J.H.P. Eloff, and M.M. Eloff, Information security: The moving target. Computers & Security, 2009.

[18] Lizzie Coles-Kemp and Yee-Lin Lai. Privacy on the internet: attitudes and behaviours, 2010.

[19] Microsoft. Microsoft security intelligence report, 2010.

[20] Cisco. Cisco annual security report, 2010.

[21] Yury Namestnikov. Information security threats in the first quarter of 2010, 2010.

[22] Falko Dressler and Ozgur B. Akan. A survey on bio-inspired networking. Elsevier, Computer Networks, 54(6):881- 900, 2010.

[23] Vasileios Pappas Michael Meisel and Lixia Zhang. A taxonomy biologically inspired research in computer networking. Elsevier Computer Networks, 54(6): 901-916, 2010.

[24] M. Wang and T. Suda. The bio-networking architecture: A biologically inspired approach to the design of scalable, adaptive, and survivable/available network applications. IEEE Symposium on Applications and the Internet (SAINT), pages 43-53, 2001.

[25] H. Wada C. Lee and J. Suzuki. Towards a biologically-inspired architecture for self-regulatory and evolvable network applications.

Advances in Bio-Inspired Information Systems in Computational Intelligence (SCI), Springer, 69:25, 2007.

[26] Stephan Kitchovitch and Pietro Lio. Risk perception and disease spread on social networks. International Conference on Computational Science, 1(1):2339- 2348, 2010.

[27] A. La Corte, M. Scatà A process approach to manage the security of the communication system with risk analysis based on epidemiological model. Fifth International Conference on Systems and Networks Communications, 2010.

Aurelio La Corte was born in Catania, Italy, in 1961. He received the degree in electrical engineering from the University of Catania in 1988, and the PhD in Electronic Engineering and Computer Science in 1994. From 1994 he is at the University of Catania. He is an associate professor in Telecommunication Engineering. His scientific interests include digital signal processing, distributed systems, network and QoS management techniques, risk analysis of ICT systems, bio-inspired models for information security, protocols and architecture for integrated communications. He has authored or co-authored about sixty research papers, published in international journals and conference proceedings.

MarialisaScatà was born in Siracusa, Italy, in 1981. She received her B.S. and M.S. degrees in Telecommunication Engineering, from Department of Electrical, Electronics and Computer Science Engineering, University of Catania, Catania, Italy. She holds a PhD in Computer Science and Telecommunication Engineering at the same department, under the guidance of Prof. Aurelio La Corte, in 2012 (PhD Thesis Security Analysis of ICT Systems based on Bio-Inspired Model). She made an internship at Computer Laboratory, Department of Computer Science, University of Cambridge (UK), under the supervision of Prof. PietroLiò, in 2011. Currently she works at DIEEI, Faculty of Engineering, University of Catania. Her current research interests include bio-inspired, heuristics, social risk perception, bio-diversity, risk and security analysis, ICT, social networks and social behavior. She has authored or co-authored research papers, published in international journals and conference proceedings.