DETECTION OF AND REACTION TO CYBER ATTACKS IN A CRITICAL INFRASTRUCTURES SCENARIO: THE COCKPITCI APPORACH

Donato Macone[(a)], Francesco Liberati[(a)], Andrea Simeoni[(a)], Francesco Delli Priscoli[(a)], Marco Castrucci[(a)], Stefano Panzieri[(b)], Serguei Iassinovski[(c)], Michele Minichino[(d)], Ester Ciancamerla[(d)]

[(a)]Università di Roma "Sapienza", V. Ariosto 25, Rome, 00185, Italy
[(b)]Università degli Studi Roma Tre, Via della Vasca Navale 79, Rome,00146,Italy
[(c)]Multitel ASBL, Rue Pierre& Marie Curie 2, Mons, 7000, Belgium
[(d)]ENEA,Lungotevere Thaon di Revel, 76, Rome, 00196, Italy

[(a)]{macone, liberati, asimeoni, dellipriscoli, castrucci}@dis.uniroma1.it, [(b)]panzieri@dia.uniroma3.it, [(c)]iassinovski@multitel.be, [(d)]{ester.ciancamerla, michele.minichino}@enea.it

ABSTRACT
The protection of the national infrastructures is one of the main issues for national and international security. The FP7 MICIE project has achieved promising results by developing a secure online software architecture and by sharing information on a real time basis among local risk predictors, in order to obtain accurate and synchronized predictions using shared interdependency models. However, results of MICIE project are not enough in order to quickly and effectively react to all adverse events that may occur over the System of Systems and, in particular, to face cyber attacks. The EC FP7 CockpitCI project aims to improve the resilience and the dependability of CIs through the design and the implementation of an Alerting System that provides to CI operators an efficient tool to support them: (i) in the prevention of cyber attacks and (ii) in the implementation of consequence containment strategies in case of attack.

Keywords: Critical Infrastructure protection, SCADA systems, cyber attacks countermeasures, detection and reaction strategies.

1. INTRODUCTION

The protection of the national infrastructures (i.e. the System of Systems including energy grids, transportation networks, telecommunications systems, etc., Suter and Brunner (2008)) is one of the main issues for national and international security. There are, in principle, several approaches that should be used to this end that encompass analytical (Bobbio, Bonanni, Ciancamerla, Clemente, Iacomini, Minichino, Scarlatti, Terruggia and Zendri, 2010;Bobbio, Ciancamerla, Diblasi, Iacomini, Mari, Melatti, Minichino, Scarlatti, Terruggia, Tronci and Zendri, 2009), simulative (Ciancamerla, Foglietta, Lefevre, Minichino, Lev and Shneck, 2010; Ciancamerla, Di Blasi, Foglietta, Lefevre, Minichino, Lev and Shneck, 2010) and what-if analyses (Haimes, Horowitz, Lambert, Santos, Lian and Crowther, 2005; De Porcellinis, Panzieri, Setola and Ulivi, 2008; Amin, 2002), while online approaches are less likely to emerge, due to the huge complexity. Among the others, the FP7 MICIE (Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures) project has achieved promising results by developing a secure online software architecture and by sharing information on a real time basis among local risk predictors, in order to obtain accurate and synchronized predictions using shared interdependency models (Capodieci, Foglietta, Lefevre, Oliva, Panzieri, Delli Priscoli, Castrucci, Suraci, Khadraoui, Aubert, Jiang, Spronska, Diblasi, Ciancamerla, Minichino, Setola, De Porcellinis, Lev, Shneck, Iassinovski, Simoes, Caldeira, Harpes and Aubigny, 2010). The outcome of this process is that operators receive information about the future evolution of their infrastructure with a wider perspective compared to previsions that can be generated by sector specific and isolated simulators.

While MICIE project has proved that increasing cooperation among infrastructures' owners by sharing information leads to better previsions, such an integration is not enough in order to quickly and effectively react to all adverse events that may occur over the System of Systems and, in particular, to face cyber attacks. Cyber attacks against SCADA (Supervisory Control And Data Acquisition) systems are considered extremely dangerous for CI (Critical Infrastructure) operativeness and must be addressed in a specific way. As an example, one of the most adopted attacks to a SCADA system is based on fake commands sent from the SCADA to the RTUs (Remote Terminal Unit).

In order to effectively react to a specific low level menace, there is the need to consider both the global and the local perspectives. In fact, besides obtaining a wider perspective on the state of the System of Systems, there is the need to increase the intelligence of equipment and devices that are used to influence the behaviour of the system, such as RTUs, valves, etc.

The idea to add "intelligence" to the field is not new; electro-valves for gas pipelines are available on the market that, in the case they receive a rapid sequence of open-close commands, do not perform them in order to avoid the consequence of the mechanical shock.

The CockpitCI approach, in order to overcome such catastrophic vision, aims to improve the resilience and the dependability of CIs through the design and the

implementation of an Alerting System that provides to CI operators an efficient tool to support them: (i) in the prevention of cyber attacks, and (ii) in the implementation of consequence containment strategies in case of attack.

In order to reach this goal, at low field level equipment will be provided of some kind of intelligence, allowing them to be able to perform local decisions but only in the presence of "critical" situations, i.e. those characterized by a high risk in terms of on-going cyber attack or unavailability of the communication. This approach will increase both global awareness and local decision-making capability.

2. METHODOLOGY

In the framework of giving "intelligence" to the low-level field equipment, a mandatory element to be considered is the capability of the different actuators (e.g. RTUs) to contrast cyber attacks by identifying them and operating, even in the absence of information coming from the central SCADA, in a "safe" manner. This implies to increase the "intelligence" at RTU level providing them with some form of self-healing and self-protection capabilities. However, it is important to understand that for SCADA systems currently used to monitor and control Critical Infrastructures, it is very dangerous that RTUs can perform autonomous operations or refuse to execute requested commands. To overcome such contradictory behaviour a sort of hybrid schema will be considered and developed in the CockpitCI project:

- at the level of Control Centre, the presence of an "Integrated On-line Risk Predictor" will perform an accurate situation assessment and will provide the operator with a qualitative/quantitative measurements of near future level of risk integrating data coming from the field, data coming from other infrastructures and data coming from smart detection agents monitoring possible cyber attacks.
- at field level, the schema is complemented with a smart software layer for RTUs and a detection system for the TLC (Telecommunication) network. This layer will continuously analyze the inputs and outputs of the RTU in order to prevent misuse, and will analyze the traffic on the TLC network to recognize cyber attacks.

As long as the smart layer does not receive an arming command from the SCADA, it will continue to execute commands received from the SCADA, even if there are large discrepancies between the expected commands and the ones actually received. On the other side, when the RTU is armed (i.e., there is a high risk level), the RTU may eventually neglect the received commands and actuate locally by defined ones. This implies the creation of a local vision of RTUs environment that will continuously evaluate optimal reaction strategies.

With respect to cyber attacks, CockpitCI project aims to improve resilience and dependability of CIs through the design and implementation in each CI of the CockpitCI Integrated Risk Prediction System. The main improvement addresses the detection, prevention and reaction to cyber threats. More specifically, the CockpitCI system will:

- develop and deploy smart detection agents to monitor the potential cyber threats according to the types of ICT based networks (SCADA, IP…) and types of devices that belong to such networks;
- identify, in real time, the CI functionalities impacted by the cyber attacks and assess the degradation of CI delivered services;
- broadcast an alerting message through an improved Secure Mediation Gateway at different security levels (low and high level);
- manage a strategy of containment of the possible consequences of cyber attacks at short, medium and long term.

The above-mentioned cyber threats and the assessment of consequences will be expressed in terms of risk level for a given CI of being no more able of providing its services with its target QoS (Quality of Service) in consequence of events occurring in other CIs; such a risk level will be hereinafter referred to as CI risk level. So, the CockpitCI system will be able to provide, in real time, each CI operator with a CI risk level measuring the possibility that, in the near future, he will no more be able to provide the CI services with the desired QoS in consequence of faults or cyber attacks, and from a high level point of view, the CockpitCI system will be able to provide a map of potential cyber threats on CI network.

The CockpitCI system will analyze in real time the cyber threats according to adaptive algorithms, compute the CI risk on the basis of abstract CI models (forecasting CI QoS taking indicators, accounting mutual interdependency among CIs and cyber attacks) and on a suitable set of aggregated data from raw field data, collected in real time by means of adequate interfaces.

3. DEVELOPMENT

The CockpitCI approach is based on the following concepts, models, equipment and tools:

(1) QoS prediction models. Quality of Service prediction models have the final aim of predicting the QoS delivered by interconnected SCADA and Telco networks accounting for cyber vulnerabilities and cyber attacks. The models will predict indicators of QoS delivered by the interconnected networks by adequate representation of the technological networks, their cyber vulnerabilities and adverse events, including cyber attacks (Bobbio, Bonanni, Ciancamerla, Clemente, Iacomini, Minichino, Scarlatti, Terruggia and Zendri, 2010; Bobbio, Ciancamerla, Diblasi, Iacomini, Mari, Melatti, Minichino, Scarlatti, Terruggia, Tronci and Zendri, 2009; Ciancamerla, Foglietta, Lefevre, Minichino, Lev andShneck, 2010; Ciancamerla, Di Blasi, Foglietta, Lefevre, Minichino, LevandShneck, 2010). The activity will be fed by an overview of modeling techniques and tools for cyber threats and

cyber vulnerabilities analysis of interconnected of SCADA systems and Telco Networks and SCADA systems. Prediction models will predict the attributes of readiness, reliability, security and performances of such services. Models will be built according to heterogeneous paradigms selected according to their capacity to represent the impact of adverse events (cyber threats, internal failures, network congestions and natural phenomena) on the QoS delivered by SCADA and the interconnected Telco networks. Modeling paradigms will include adequate agent based simulation, analytical dependability modeling with careful examination of scalability issues (Extended Stochastic Petri Nets, Network Reliability analyzers) discrete event simulation (based on largely known open source platforms) and Input/output modeling.

(2) The design and the implementation of the CockpitCI Detection System (detection agents plus detection adaptors). This part will include research aspects (especially in terms of smart detection agents for SCADA and Telecom network) and integration aspects (taking into account existing system). Especially, this concept will include the research aspects on traffic monitoring and attack detection, i.e. new machine learning based approaches for unusual traffic event detection will be investigated. At the end of this phase, the different approaches will be evaluated and the most suitable solution for cyber attack detection will be selected. The final objective is to design and implement a set of intelligent detection agents able to identify the cyber threats. These agents will be included in a smart architecture able to be re-oriented thanks to learning strategies.

(3) The On-Line Integrated Risk Predictor (IRP) which, on one hand, will allow to model the cyber-dependencies of CIs and the other functional dependencies, and, on the other hand, will permit to identify the potential cascading effects of cyber attacks or other adverse events using the right interdependency schemes provided by the modeling. The on-line IRP will also implement an accurate situation assessment to devise best responses to the actual threat and identify the part of risked CI network, and to broadcast relevant information to other CI and national/European authorities.

(4) The design and implementation of the CockpitCI Secure Mediation Network in the prospect of broadcasting cascade failures and cyber alerts at low and high level.

(5) The design of a CockpitCI Smart RTU Reaction System which, on the grounds of the CockpitCI On-Line Risk Predictor, will manage the strategy of containment, i.e.: (1) to block attacks, (2) to isolate infected systems, (3) to deploy tactical and operational security policies.

(6) The design and implementation of the CockpitCI SCADA adaptors to extract raw data from SCADA and Telco control rooms but also from other SCADA and Telco devices (Smart RTUs, Detection Agents, etc.)

In particular, the methodology in question will be based on the following issues:

a. To identify a typology of cyber-threats and to model the cyber-interdependencies of the composite CIs system in order to identify the right peers to communicate alert messages for each type of cyber-attacks.

b. Develop a real-time Distributed Monitoring System and Perimeter Intrusion Detection System (PIDS) able to aggregate the filtered and analyzed information of potential cyber-attacks induced on SCADA systems or telecommunication systems used to support the operation of CIs and identify the potential unsecured area of the CIs. Thanks to intelligent detection agents, the monitoring system should be able to dynamically reconfigure itself in order to focus on specific threats.

c. Create a framework to allow the community of CI owners to exchange real-time information about attacks (and tentative attacks), extending the capabilities and functionalities of the Secure Mediation Gateway and of the risk prediction tool developed in MICIE project. Issues to be considered include: (i) need to exchange information among trusted CIs, not necessarily interdependent, (ii) availability of the integrated prediction tool in each CI to calculate cascading events induced by faults and cyber attacks especially in terms of QoS of Power and Telecommunication Grid, (iii) need to develop a strategic analysis tool able to calculate the potential threat of coordinated cyber-attacks on CIs.

d. Analyze strategies for automatic real-time reaction able to better manage the corrupted portion of the grids (Telco and SCADA), able to predict the time of reconfiguring the grid to reach a defined QoS level, and able to treat the corrupted system at short, medium and long term (definition of automatic procedures of treatment).

Another fundamental aspect addressed by the CockpitCI approach is the secure exchange of information across CIs and to high level authorities (national or European). The CockpitCI system, based on Secure Mediation Gateways, will be capable to allow secure broadcasting of the information at low and high level. The use of the new Secure Mediation Network will assure that information sharing regarding CI is mediated and elaborated to support decisions and, at the same time, it takes place in an environment of trust and security. The sharing of information requires a relationship of trust such that companies and organizations know that their sensitive data are sufficiently protected.

The CockpitCI system, including detection, prediction, alert and reaction, will be conducted by means of a reference scenario. Reference scenario identifies the portion of the interconnected SCADA system and Telco network, selects services delivered to customers, evaluates their quality (in terms of continuity, readiness, performances, time response), finds the vulnerabilities in the interconnected networks

for possible cyber attacks and cyber interdependencies between networks in order to mitigate the effects of successful cyber attacks. A reference scenario is in an operational mode when the quality of the delivered services (QoS) is within a Service Level Agreement (SLA), or in a degraded mode when QoS is outside SLA as an ultimate consequence of successful cyber attacks or other adverse events.

4. PRELIMINARY RESULTS AND CONCLUSION

The accomplishment of the proposed objectives will bring noteworthy added value to specific application scenarios. In the following, the ideas, concepts and objectives presented in the previous sections have led to the definition of the following architecture of the CockpitCI system. The envisaged CockpitCI system architecture, in the case where two interdependent CIs are considered, is shown in Figure 1.

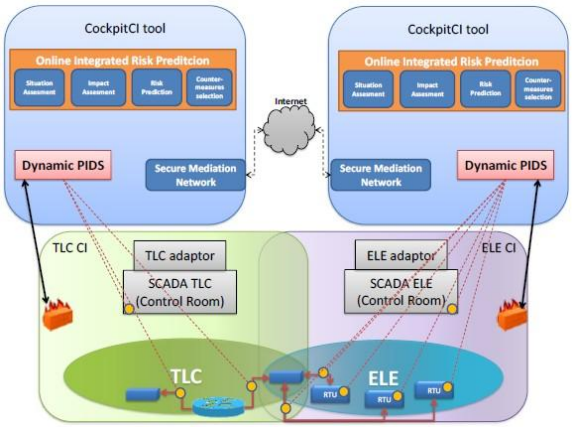

Figure 1: Envisaged CockpitCI architecture.

At the bottom of the figure, a conceptual and simplified illustration of the two CIs and of their interconnection is presented. In particular, for the sake of exposition, a telecommunication CI ("TLC" in the figure) and an electric distribution network ("ELE" in the figure) are considered. For each CI, both field elements (e.g. RTUs) and the SCADA control room ("SCADA ELE" and "SCADA TLC") are represented (the CockpitCI tool interacts both with field level devices and at control room level). Each CI has an associated CockpitCI tool. Since the CockpitCI tool must be a scalable and CI-technology independent solution, it is necessary to consider in the architecture also proper adaptors ("TLC adaptor" and "ELE adaptor" in the figure) at the interface between the CockpitCI tool and the particular CI domain. The CockpitCI tool architecture consists of three layers, namely detection layer, risk prediction layer and mediation layer.

As concerns the components lying at detection layer, they consist of (i) a centralized component, named dynamic PIDS (Perimeter Intrusion Detection System), and (ii) a set of distributed local detection agents for intrusion detection at local level (the yellow dots in the figure). The local detection agents will be able to autonomously detect and (in some cases) react to local attacks, and will provide information to distributed Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) mechanisms. Detection agents, adaptors and extensions for system components will pervade CI's field and will be placed at the most critical sources of vulnerabilities, including RTUs and the main SCADA elements. The PIDS is a centralized component which correlates and aggregates the alerts received from the detection agents. Moreover, the PIDS has the capability to detect coordinated cyber-attacks, and to dynamically deploy containment or even preventive strategies of isolation (as an example, the PIDS could respond to detected threats by changing firewalls rules in order to redefine ICT system perimeters).

Information from local detection agents is gathered by adaptors (which perform all the needed operations in terms of filtering, aggregation, translation, etc.), and sent (in a technology independent format) to a centralized on line Integrated Risk Prediction (IRP) (at the top of the figure), which performs a situation assessment, computing the risk level associated to the current state of the CI, and evaluates the impact of cyber-attacks, suggesting also possible countermeasures. The IRP performs the above-mentioned situation assessment by properly analyzing rich input information merging both local field information (coming from the local CI Detection Layer) and global/remote information about the status of linked CIs, coming from linked IRPs. Notably, the connection between the IRP and the local detection layer is bidirectional in the sense that the results of IRP elaborations can be fed-back to the detection layer (to local detection agents and PIDS) in order to improve local detection and reaction capabilities. Hence, the output of the IRP will be provided both to control room operators and to the detection layer.

The secure and reliable communication between the detection layer and the IRP is assured by a secure mediation network, which also supports the secure exchange of data between linked CIs. So doing, it is possible to combine local and global perspectives and obtain awareness at all the levels of the system. This is essential in view of the concept of interdependence, which plays a crucial role in critical infrastructures protection. Concluding, the proposed CockpitCI architecture is functional to the achievement of the general objectives explained in the previous sections, which impose innovative technological and scientific contributions in the fields of CI modeling, cyber detection, risk prediction, adaptors design, secure mediation of data and intelligence for local autonomous reaction capabilities.

REFERENCES

Amin M., 2002. Modelling and Control of Complex Interactive Networks. *IEEE Control System Magazine*, pp. 22–27.

Bobbio A., Bonanni G., Ciancamerla E., Clemente R., Iacomini A., Minichino M., Scarlatti A., Terruggia R., Zendri E., 2010. Unavailability of critical SCADA communication links interconnecting a power grid and a Telco network. *Reliability Engineering and System Safety Journal, Elsevier editor*.

Bobbio A., Ciancamerla E., Diblasi S., Iacomini A., Mari F., Melatti I., Minichino M., Scarlatti A., Terruggia R., Tronci E., Zendri E., 2009. Risk analysis via heterogeneous models of SCADA interconnecting Power Grids and Telco Networks. *CRiSIS'2009 – The Fourth International Conference on Risks and Security of Internet and Systems*, 19-22 October 2009, Toulouse, France.

Capodieci P., Foglietta C., Lefevre D., Oliva G., Panzieri S., Delli Priscoli F., Castrucci M., Suraci V., Khadraoui D., Aubert J., Jiang J., Spronska A., Diblasi S., Ciancamerla E., Minichino M., Setola R., De Porcellinis S., Lev L., Shneck Y., Iassinovski S., Simoes P., Caldeira F., Harpes C., Aubigny M., 2010. Improving Resilience of Interdependent Critical Infrastructures via an On-Line Alerting System.*Proceedings of COMPENG 2010 - Complexity in Engineering*.

Ciancamerla E., Di Blasi S., Foglietta C., Lefevre D., Minichino M., Lev L. Shneck Y., 2010. QoS of a SCADA system versus QoS of a Power distribution grid. *10th International Probabilistic Safety Assessment & Management (PSAM)*. June 7-11, 2010, Seattle, WA.

Ciancamerla E., Foglietta C., Lefevre D., Minichino M., Lev L., Shneck Y., 2010. Discrete event simulation of QoS of a SCADA system interconnecting a Power grid and a Telco network. *1st IFIP International Conference on Critical Information Infrastructure Protection, World Computer Congress 2010*. 20-23 September 2010, Brisbane, Australia.

De Porcellinis S., Panzieri S., Setola R., Ulivi G., 2008. Simulation of Heterogeneous and Interdependent Critical Infrastructures. *International Journal Critical Infrastructures (IJCIS)* Vol. 4, n. 1/2:pp. 110-128.

Haimes Y., Horowitz B., Lambert J., Santos J., Lian C., Crowther K., 2005. Inoperability Input-Output Model for Interdependent Infrastructure Sectors. *Theory and Methodology, Journal of Infrastructure Systems* Vol. 11(2):pp. 67-79.

Suter, M., Brunner, E.,2008. International CIIP Handbook 2008/2009. *Centre for Security Studies*, ETH Zurich.

AUTHORS BIOGRAPHY

Donato Macone, Ph.D student in the Department of Information, Electrical and Telecommunication Engineering (DIET) of "Sapienza" University of Rome. He graduated with Bachelor Degree in Computer Engineering in 2007 with 110/110 cum laude and graduated with Master Degree in Computer Engineering in 2009 with 110/110. His expertise covers network resource management, game theory, ontology representation, routing and load balancing strategies and algorithms, algorithms for data fusion. He participated in the MICIE project, fund within the FP7 EU ICT-SEC research programme and is still involved in TASS and CockpitCI projects, fund within FP7 EU SEC research programme, SMARTV2G project, fund within the FP7 EU ICT-GC research programme.

Francesco Liberati received the bachelor degree and master degree in automatic control engineering and systems engineering from "La Sapienza" University, Rome, Italy, in 2009 and 2011, respectively. He is currently working toward the Ph.D. degree in systems engineering at the same university. His research interests include critical infrastructures protection and the application of control systems theory to the design of local energy management systems, with applications to smart grids and electromobility.

Andrea Simeoni, Master degree in Computer Engineering, achieved in "La Sapienza" University of Rome. His research activity covers resource management and routing algorithms for future networks, cross platform development frameworks, Software Defined Networking and critical infrastructure security.

Francesco Delli Priscoli is Full Professor at the University of Rome "La Sapienza" where he holds the courses "Automatic Controls", "System Control" and "Network Control and Management I and II", and is a member of the board of directors of CRAT. His main research topics are nonlinear control and QoS/resource management procedures for mobile systems. He is the author of about 160 papers and four patents. He was/is presently responsible, at the University of Rome "La Sapienza", for 18 projects financed by the EU or by ESA dealing with resource management, service and interworking management for broadband terrestrial and satellite wireless/wired systems.

Marco Castrucci graduated in Telecommunication Engineering with 110/110 cum laude in May 2006 at the University of Rome "La Sapienza" and obtained the Ph.D. in System Engineering from University of Rome "Sapienza" in 2010. He was involved in FP6 IST 'DAIDALOS II' and 'WEIRD' projects and FP7 ICT 'OMEGA', 'MICIE', 'FI-WARE' and 'MONET' projects. He also covered WP leader position in several of the mentioned projects. His main research topics were related to the convergence among heterogeneous telecommunication technologies, the design of innovative architectures and paradigms for the Internet of the Future, and software defined networks. He is author of several publications related to its research activities. At the moment he works for Business Integration Partners, as business consultant in the public sector.

Stefano Panzieri (http://panzieri.dia.uniroma3.it) was born in Rome (Italy) on December 17th 1963. He took the Ph.D. in System Engineering in 1994 at University of Rome "La Sapienza". From 1996 he is with the University "Roma Tre" as Associate Professor. His teachings are in the field of Automatic Control, Digital Control and Process Control within the courses of Electronic, Mechanics and Computer Science, he is the coordinator of both "Automatic Laboratory" and "Robotics and Sensor Fusion Laboratory" ofDip. Informatica e Automazione. He is IEEE member and has been a member of the Working group on Critical Infrastructures of Prime Minister Council. Research interests are in the field of industrial control systems, robotics, sensor fusion and critical infrastructure protection (CIP). In the CIP field has contributed to develop a simulation model, the CISIA project, that is able to evaluate cascades of failures in a network of infrastructures, pointing out hidden interdependencies. Several published papers, in the robotics field, concern the study of iterative learning control applied to robots with elastic elements and to nonholonomic systems. In the area of mobile robots, some attention has been given to the problem of navigation in structured and unstructured environments with a special care to the problem of sensor based navigation and sensor fusion. Many techniques derived from Fuzzy Logic, Bayesian Estimation (KalmanFilltering) and Dempster-Shafer theory have been developed and applied to the problem of mapping building and vision based localisation. More recently, has been interested to the application of complex networks theory into evolutionary computation. He is author of about 100 papers, among them several experimental papers involving mobile and industrial robots.

Serguei I. Iassinovski. Graduated from Moscow Bauman State Technical University in 1985, Ph.D in applied sciences (1990), project manager and team leader at Multitel since 2007. Author of more than 70 publications in the fields of complex discrete system modelling, simulation, optimisation and real-time control, using of AI methods for complex discrete system simulation tools, Business Process Re-engineering, meta-heuristics, scheduling

Michele Minichino received his in Electronic Engineering, "summa cum laude" from University of Naples in 1978. He is coordinator of the program for Critical Infrastructure Protection (CIP) at ENEA. His research interests include risk based methodologies, qualitative and quantitative indicators, multi formalism and multi solution methods and tools for Quality of Service measures (in terms of performances, reliability and dependability) of Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) and of large interconnected CI, including power grids and telco networks at regional/national level. He has acted in the frame of several research programs, funded by Italian government and by European Union; among the most recent SHIP, ISAEUNET, SAFETUNNEL and IRRIIS EU Projects. He has been Contract Professor, at the Software Engineering Chair of the Engineering Faculty of the II University of Rome "Torvergata", for several years. He has been Contract Professor of Mainframe Operating Systems, at the High School of the Italian Ministry of Finance (ScuolaEzioVanoni). Currently, he is working on scenarios, services, heterogeneous models and tools to assist on line the operators of ICS and CI in performing emergency procedures, in the framework MICIE (Tool for systemic risk analysis and secure mediation of data across Critical Infrastructures) and CockpitCI (Cyber security on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures) EU FP7 Projects. He serves, as expert, the EU Directorate General Information Society and Media (DG INFSO) and the European Network and Information Security Agency (ENISA) on the topics of the security and resilience of ICS for CIP. He has authored and co-authored more than 70 papers for International Journals and Conferences Proceedings.

Ester Ciancamerla received her degree in Nuclear Engineering from University of Rome on 1978. Since her degree, she has been working at ENEA, as scholarship holder and researcher. In remote past, major experience has been gained dealing with system validation, software verification plans, software test methodologies, tools and environments for computer based systems in nuclear, avionics and railway fields. Her current research interest is on modeling methods and tools for dependability/survivability evaluation of networked systems. She has acted in the frame of several research programs, funded by Italian research organizations and by European Union; among the most recent SHIP, ISAEUNET, SAFETUNNEL and IRRIIS EU Projects. In SAFETUNNEL IST Project, she worked on the validation by modeling of a Tele Control System, based on a Public Mobile Network, for Alpine Road Tunnels protection. She has worked on IRRIIS (Integrated Risk Reduction of Information based Infrastructure Systems) IP – EU project, funded by FP6, to investigate risk based methodologies for vulnerability and interdependency analysis of critical infrastructures. Currently, she is working on scenarios, services, heterogeneous models and tools to assist on line the operators of the interconnected power grid and Telco network in performing emergency procedures, in the framework MICIE (Tool for systemic risk analysis and secure mediation of data across Critical Infrastructures) and CockpitCI (Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures) EU FP7 Projects. She has authored and co-authored more than 70 papers for International Journals and Conferences Proceedings.