Improving Resilience of Interdependent Critical Infrastructures via an on-line Alerting System

P. Capodieci
Selex COM
paolo.capodieci@selex-comms.com

S. Diblasi, E. Ciancamerla, M. Minichino
Enea
minichino@casaccia.enea.it

C. Foglietta, D. Lefevre, G. Oliva, S. Panzieri
University Roma Tre of Rome
panzieri@uniroma3.it

R. Setola, S. De Porcellinis
University Campus Bio-Medico of Rome
r.setola@unicampus.it

F. Delli Priscoli, M. Castrucci, V. Suraci
Crat Consortium
castrucci@dis.uniroma1.it

L. Lev, Y. Shneck
Israel Electric Corp
adara@iec.co.il

D. Khadraoui, J. Aubert
CRP Henri Tudor
jocelyn.aubert@tudor.lu

S. Iassinovski
Multitel
serguei.iassinovski@multitel.be

J. Jiang
University of Bradford
j.jiang1@bradford.ac.uk

P. Simoes, F. Caldeira
University of Coimbra
micie-dei@dei.uc.pt

A. Spronska
PIAP
aspronska@piap.pl

C. Harpes, M. Aubigny
Itrust
aubigny@itrust.lu

Abstract— **This paper illustrates the activities under development within the FP7 EU MICIE project. The project is devoted to design and implement an on-line alerting system, able to evaluate, in real time, the level of risk of interdependent Critical Infrastructures (CIs). Such a risk is generated by undesired events and by the high level of interconnection of the different infrastructures. Heterogeneous models are under development to perform short term predictions of the Quality of Service (QoS) of each CI according to the QoS of the others, to the level of interdependency among the Infrastructures, and according to the undesired events identified in the reference scenario.**

I. The MICIE project

The EU FP7 MICIE project (whose extended title is "Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures" - see the project website for detailed information http://www.micie.eu), has the main aim to design and implement the so-called MICIE *on-line* alerting system; in particular, whenever any undesired event occurs, the MICIE alerting system will support the CI operators in the different control rooms, providing a real time combined risk level indicator. This combined risk level will be defined as the ability level of the CI to provide its own services with a target Quality of Service according to the degradation of its own QoS and of the QoS of interdependent CIs, due to undesired events. In the MICIE framework, the QoS has to be assessed both from a functional point of view (i.e. in terms of availability, reliability...) and from a security point of view (i.e. in terms of confidentiality, integrity, accountability...). The alarm conditions will be evaluated by means of a distributed on-line prediction tool, based on properly designed abstract CI models. These models will be fed with aggregated metadata coming from the field of each CI. A particular effort will be done to identify and formalize proper metadata suitable for describing CI status. The provided models will also be used *off-line*, in order to evaluate the level of interdependency existing among different CIs and to identify the most vulnerable elements of the resulting System of Systems. MICIE alerting system will also include a proper communication infrastructure, namely *Secure Mediation Gateway* (SMGW), aimed to retrieve from each CI all the information required for the real-time risk prediction; moreover, the system will allow the information sharing in a highly available and secure framework. A portion of the electrical and telecommunication infrastructures of

978-0-7695-3974-4/10 $26.00 © 2010 IEEE
DOI 10.1109/COMPENG.2010.28

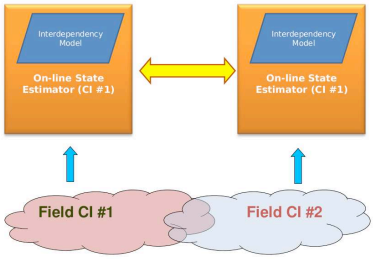

Fig. 1. Decentralized risk prediction tool

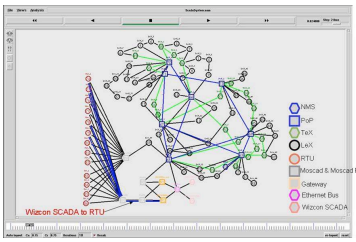

Fig. 2. A snapshot of the NS2 model of interconnected networks underlining rerouting and performance calculations of FISR.

Israel, both managed by IEC, is considered as a test-bed for the on-line alerting system.

II. Critical Infrastructure Modeling

Heterogeneous (stochastic versus deterministic, agent based, dynamic simulation, etc.) models are under development, with the aim of investigating the short term prediction of the *Quality of Services* (QoS) delivered by different Critical Infrastructures. Models are based on the underlying interconnected networks that cooperate for service delivery and on possible undesired events.We are currently investigating how a possible degradation of the QoS of SCADA (expressed in terms service connectivity, reliability, rerouting, time response, operability level) affects the quality of power supply provided by the power grid operator to power grid customers (expressed in terms of duration and number of interruptions). Within this aim, the Power Grid *Fault Isolation and Reconfiguration Service* (FISR), performed by SCADA, throughout its operator, is a particularly critical service. FISR detects and isolates grid outages, then restores the grid in order to re-energize grid customers. The interconnected networks, which underline the delivery of FISR service (SCADA system, Telecommunication network and power distribution grid) have been identified (in terms of topologies, functionalities, performances, rerouting and failure behaviors, interconnections at physical, geographic and logical layers) and represented with multiple techniques, such as the *Mixed Holistic Reductionistic* (MHR) approach [1] and heterogeneous models based on *NS2* simulator and other network analysis tools [2]. The aim is the short term prediction of QoS of FISR by means of its *static* and *dynamic* indicators, computed under normal and critical operation (when possible undesired events occur). *Static* QoS indicators, such as connectivity and availability, depend upon failure and repair behavior of networks elements. They are computed by means of analytical methods (we resort to the *Weighted Network Reliability Analyzer*, an Academic tool) and by the integration of the different topologies in a simulative perspective (i.e with the MHR approach); a close cooperation with the stakeholders and experts is required in order to provide a unitary vision of the overall System of Systems. *Dynamic* QoS indicators [3,4], such as packet round trip time, node throughput and packet dynamical paths, node operability level, depend upon network congestion and routing policies other than on failure and repair activities. They are computed by simulation schemas (we adopted, among the others, MHR modeling framework and *NS2 network simulator*, an open source tool). Figure 2 shows a snapshot of the NS2 model of interconnected networks used to investigate rerouting and performance indicators of FISR.. The Static and Dynamic indicators are then composed to compute the response time of Fault Isolation and System Restoration (FISR) service. Widely adopted reliability indices for power distribution grids, such as CAIDI (Customer Average Interruption Duration), SAIDI (System Average Interruption Duration) and SAIFI (System Average frequency Interruption), are used to quantify the impact of the QoS of FISR on the Quality of Service of the Power grid supply to utility customers.

III. Online Risk Prediction Tool

The definition of a centralized state estimator requires that such tool have the complete knowledge of the status of every infrastructure and their parts; such requirement is not easy to satisfy, due to the huge amount of data that must be taken into account and because of the obvious security aspects related to the disclosure of critical information. A more feasible compromise may be a decentralized, yet synchronized, scenario; from such a perspective, each control center can be equipped with a *global* model of the overall System of Systems (see Figure 1). Obviously the tool inside each infrastructure directly receives only the data originated within such infrastructure. Moreover, the different tools must be interconnected. The main issue is then the synchronization of such models; a first step has been done in [5], in the case of linear distributed interdependency estimators with complete information sharing. In our opinion, the easiest way to grant the consistency of the overall state estimated by the different distributed tools is to equip every system with a common general model, although each specific domain receives only a subset of the inputs. Hence, in the proposed framework, every tool has *exactly* the same model of the overall System of Systems (see Figure 1). To this end we adopted the Mixed Holistic Reductionistic Approach, taking advantage of the CISIA simulation framework, which allows to manage into a single framework heterogeneous models, with the desired level of granularity.

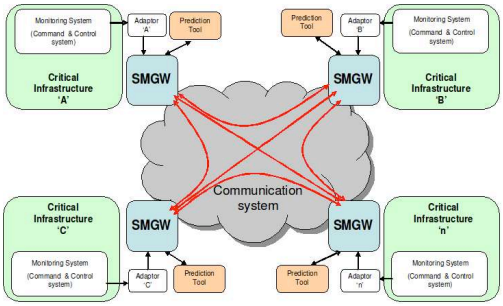

Fig. 3. MICIE overall system architecture

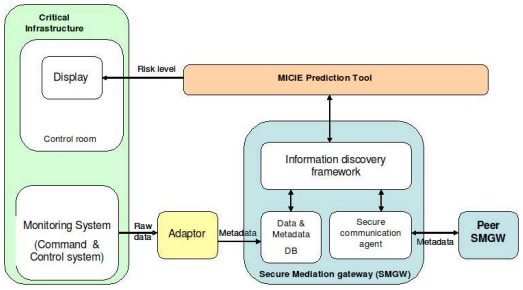

Fig. 4. MICIE system attested in a CI

IV. Secure Mediation Gateway

In order to allow a real-time exchange of information among different and heterogeneous CIs, a communication infrastructure have to be deployed. The key element of this communication infrastructure is the so-called *Secure Mediation Gateway* (SMGW). The whole communication system thus consists of a set of SMGWs (one for each CI in the system). Each SMGW can be used by the prediction tool to retrieve all the information necessary to perform the real-time risk prediction. In fact, the main tasks performed by the SMGW are: (i) to collect information about the local CI (i.e. the CI where the SMGW is located); (ii) to retrieve information about the other interdependent CIs in the system; (iii) to send information about the local CI to remote CIs; (iv) to provide all the collected information to the prediction tool. Figure 3 shows, at high level, the overall MICIE system architecture. The SMGW is designed in a CI-independent way; a specific adaptor is used to interconnect each CI monitoring system with the corresponding SMGW. SMGW implements a content discovery framework that enables the dynamic discovery of information in the whole information system, realized connecting different SMGWs. In addition, specific security requirements (i.e. confidentiality, integrity, availability, non repudiation and auditability/traceability) are considered in the design of the communication system, due to the sensitive nature of the exchanged information. Each local SMGW will have also to manage the potential communication breakdown with remote CIs by performing an rescue information recovery policy (e.g. thanks to a neighboring information sharing procedure). Figure 4 illustrates how the MICIE system can be interfaced with the CI where the SMGW is located.

V. On-line Alerting System validation and conclusions

In order to validate the effectiveness of the MICIE approach, a reference scenario composed of a portion of the electric power grid managed by the IEC (the Israel electric distribution firm) with its telecommunication network was considered. Specifically, the reference scenario includes:(I) A portion of a MV power grid at 22 KVgrid; (II) A portion of communication network, including passive (i.e. fiber optics) and active (i.e. VHF radio interfaces, Remote Terminal Units (RTU) and 22KV SCADA control center); (III) SCADA and NMS systems for control and management of the above networks; (IV) A portion of HV power grid at 160 KV. The project can be split into two subsequent phases: a *off-line* and a *on-line* phase. The *off-line* phase is devoted to the analysis of the reference scenario by means of a set of uncorrelated, heterogeneous software tools and simulators.Starting with the knowledge acquired during the above phase, and considering also a close cooperation with the stakeholders, the *on-line* phase consists of the definition of a shared interdependency model and the implementation of an online, distributed interdependency estimator. The resulting estimator will be able to provide a short term prediction of the state of the overall system. Moreover, it will also warn operators about future threats, taking advantage of its wider perspective; in fact, due to the sharing of information among the infrastructures, the MICIE tool will provide useful information that could not be obtained otherwise. Actually a first set of heterogeneous models has been developed in order to perform offline simulations and 'what if' analyses; a preliminary on-line framework is under development.

Acknowledge

This work has been supported by the EU IST project MICIE FP7-ICT-225353/2008

References

[1] S. De Porcellinis, G. Oliva, S. Panzieri and R.o Setola, A Holistic-Reductionistic Approach for Modeling Interdependencies, Critical Infrastructure Protection III, M. Papa and S. Shenoi eds., Springer, pp. 215-227, 2009.

[2] A. Bobbio, E. Ciancamerla, S. Diblasi, A. Iacomini, F. Mari, I. Melatti, M. Minichino, A. Scarlatti, R. Terruggia, E. Tronci, E. Zendri, Risk analysis via heterogeneous models of SCADA interconnecting Power Grids and Telco Networks, CRiSIS 2009 - Int. Conf. on Risks and Security of Internet and Systems, 2009.

[3] G. Bonanni, E. Ciancamerla, Clemente, A. Iacomini, A. Scarlatti, E. Zendri, R. Terruggia, Exploiting stochastic indicators of interdependent infrastructures: the service availability of interconnected networks, Proc. of the European Safety and Reliability Conference, 2008.

[4] G. Bonanni, E. Ciancamerla, M. Clemente, A. Iacomini, A. Scarlatti, E. Zendri, A. Bobbio, R. Terruggia, Availability and QoS Analysis of Interconnected Networks, Poster session at 5th International Service Availability Symposium, 2008

[5] A. Gasparri, G. Oliva and S. Panzieri, On the distributed synchronization of on-line IIM Interdependency Models, Proc. of the 7th IEEE International Conference on Industrial Informatics (INDIN), Cardiff (UK), June, 2009.