An Alerting System for Interdependent Critical Infrastructures

P. Simões¹, P. Capodieci², M. Minicino³, E. Ciancamerla³, S. Panzieri⁴, M. Castrucci⁵, L. Lev⁶
¹ CISUC - DEI, University of Coimbra, Portugal
² Selex Communications S.p.A., Italy
³ ENEA, Italy
⁴ Università di Roma Tre, Italy
⁵ University of Rome – La Sapienza, Italy
⁶ Israel Electric Corp., Israel
psimoes@dei.uc.pt
paulo.capodieci@selex-comms.com
michele.minichino@enea.it
ciancamerlae@enea.it
panzieri@uniroma3.it
castrucci@dis.uniroma1.it
leonid.lev@iec.co.il

Abstract:
In the last few years we have witnessed a strong interest in the protection of Critical Infrastructures (CIs) such as power distribution networks, power plants, refineries, water distribution, transportation systems, hospitals and telecommunication networks. Despite their relevance for public safety and security, these infrastructures are highly exposed to a large number of threats, including natural hazards, component failures, criminal actions and terrorism.

Several research projects address this topic. Many of them focus on building CI simulators for preventive analysis of system vulnerabilities, while others try to proactively strengthen partial sections of the CIs (such as fault tolerant components or secure control networks). Nevertheless, despite their positive results, those projects seldom provide mechanisms to assess, in real time, the risk level associated with each of the services provided by the addressed CI. Moreover, they do not take into account the high level of interdependency between heterogeneous CIs (power distribution failures, for instance, have a direct impact on telecommunication networks, which also affect other critical infrastructures and so on) or, when they do, they have to make compromises at the level of scalability, performance, or privacy of sensitive information.

In this paper we present a CI alerting system that takes a step further, when compared to those approaches, by estimating in real time the risk level associated with each service provided by the CI (i.e. the current likelihood of service degradation or service shutdown induced on a given CI by “undesired” events occurred in that CI and/or in other interdependent CIs).

Keywords: Critical Infrastructure Protection, Online Alerting Systems, CI Interdependence

1. Introduction

By their own nature, Critical Infrastructures have always been potentially weak points, exposed to a number of safety and security threats. Nevertheless, current CIs are more vulnerable than ever, as the need for efficiency and economic optimization pushes for increasingly complex systems with narrower safety margins, more complex technology and higher interdependency with external entities.

In this sense Critical Infrastructure sectors do not exist alone but interact each other, implying that CI protection must be addressed in cross sector and cross border perspectives, since an impact occurring on one infrastructure (e.g. an unexpected fault) propagates on one or more other interdependent infrastructures across CI interdependency trees such as the one depicted in Figure 1. This increases the risk of catastrophic failures, triggered by intentional attacks, accidents or simple malfunctions.

There is now a wide recognition of those risks, materialized in public initiatives such as the well-known Critical Infrastructure Protection (CIP) Program, launched in 1998 by the US government, and the European Programme for Critical Infrastructure Protection (EPCIP 2006). Such initiatives resulted in increase public awareness, better industry practices and a large number of research activities.
In order to counterbalance the risks induced by increasing complexity, a significant part of those research activities focused on intrinsic robustness, security and resiliency, addressing topics such as better industrial control networks, fault-tolerant design, redundancy of key components, more secure information systems and less vulnerable IT components.

Another line of research addresses risk analysis, with the development of risk assessment models able to preventively identify critical risks. Nevertheless, in general the currently available risk analysis mechanisms do not accurately handle the interdependency between interconnected CIs, at least when performing real-time risk estimation.

One of the reasons for this relates with the specialization of risk models. In order to tackle with the complexity of the target CI, those risk models are usually specialized in a specific type of infrastructure (e.g. power distribution networks; information systems), failing to capture finely tuned interdependencies between heterogeneous CIs.

Another reason relates with the lack of proper mechanisms for sharing, in real time, the risk knowledge between interconnected CIs. Without those mechanisms the operator of a given CI has no real-time visibility on the risk level associated with contracted services such as power or communication lines. Failures in those externally contracted services become fully unpredictable, thus compromising the accuracy of the CI risk models.

In this paper we present the MICIE Alerting System, which provides a set of solutions to specifically incorporate CI interdependencies in an online risk assessment framework. This alerting system is a core component of the MICIE FP7 Project (MICIE 2010) and is in line with the European initiative to establish a Critical Infrastructure Warning Information Network – CIWIN.

The rest of this paper is organized as follows. In Section 2 we discuss related work. The key components of the MICIE Alerting System are presented in Section 3. Section 4 analyses the relation between this alerting system and European initiatives such as EPCIP and CIWIN. Section 5 discusses the MICIE framework in the context of a simple reference scenario and Section 6 concludes the paper.

2. Related Work

The increasing interdependency of Critical Infrastructures is a well-known problem. Seminal work such as (Rinaldi 2001) identifies multiple dimensions of interdependency – including physical interdependency (e.g. a coal-fired power plant and the rail network used to transport the coal to the plant); geographic interdependency; cyber interdependency and logical interdependency – as well as multiple levels of interdependency.

Several researchers have studied these interdependencies (Svendsen 2007) and proposed their incorporation in CI risk models (Haimes 2001; Rigole 2006; Pederson 2006; Tolone 2008), but in general those models have not proven suitable for application in real time risk estimation systems, due to a number of reasons, such as scalability, performance and the need to preserve the security of the sensitive internal information kept by each CI.

More recently the IRRIS European project (Balducelli 2008) has taken a few steps towards on-line risk prediction tools able to incorporate CI interdependencies, studying multiple approaches to data sharing across CIs, interdependency modeling and risk estimators. In order to allow for communication between heterogeneous CIs using incompatible applications the IRRIS architecture
features a set of adaptation applications (the so-called Middleware Improved Technology) for fast exchange of information about the state of interrelated CIs.

The MICIE alerting system we describe in this paper is largely built on the lessons learned during the IRRIS Project, and represents one of the first attempts to effectively build from scratch a complete framework providing on-line risk estimation for multiple interdependent Critical Infrastructures whilst preserving the autonomy, privacy and security of each CI.

3. The MICIE Alerting System

The MICIE Alerting System is a distributed tool that identifies, in real time, the level of possible threats induced on a given Critical Infrastructure (CI) by undesired events happened in the same CI and/or in other interdependent CIs. This alerting system is based in three key components:

- CI risk models that are able to take into account both the specialized characteristics of each type of infrastructure and generic interdependencies between heterogeneous CIs.
- Risk prediction tools that make use of such risk models to assess the risk level of the services provided by a given CI, based on the status of its components and the current risk levels associated with the services the CI receives from other (interdependent) CIs. The MICIE framework assumes there is at least one risk prediction tool per CI, fed by monitoring of its internal components and metadata provided by interconnected CIs.
- And Secure Mediation Gateways (SMGW) that gather status information from internal CI components and also exchange metadata with interconnected CIs in order to get/provide the current risk-levels associated with services received from/provided to interrelated CIs. The MICIE framework assumes there is at least one mediation gateway per CI, feeding the risk prediction tool.

Figure 2 depicts the high-level architecture of the MICIE framework, highlighting the role of the risk prediction tools – based on the already mentioned risk models – and the secure mediation gateways. In order to deal with the specificities of each type of CI the architecture also includes specialized adapters, which translate the system-specific data collected by the CI monitoring systems into metadata more suitable for generic risk models and information exchange with (possibly heterogeneous) interconnected Critical Infrastructures.

The system is designed with real-time risk estimation in mind, but the risk prediction tools might also be used off-line, for instance to assess the impact of specific system components, to simulate the effects of emergency recovery plans or to identify critical interdependency points.

Figure 2: MICIE High-Level Architecture.
3.1 Risk Models, Ontologies and Risk Prediction Tools

Interdependencies between Critical Infrastructures might be expressed as services – a given CI provides one or more services to another CI. The same applies for relations between internal components of the CI: a specific component provides services to other components. In this sense, the notion of Quality of Service (QoS) can be used to express the risk of QoS degradation associated with a specific service – either internal or external. According to the nature of the service QoS might relate with service continuity, service performance, service capacity, etc. Furthermore, QoS degradation may be graceful (for instance a communication network might become slower but still usable) or correspond to complete service failures.

MICIE makes use of heterogeneous models (stochastic versus deterministic, agent based, dynamic simulation) to perform short-term predictions of the QoS of the CIs according to the involved services, the interdependency networks and the system status. The specific suitability of each model obviously depends on the nature of the target CI, making it possible to select for each CI the most appropriate models. Nevertheless, in order to harmonize the risk prediction of each CI, it is also necessary to identify the key semantic elements for the description of the CI status common to heterogeneous CIs. Those common semantic elements – which include qualitative and quantitative metrics and QoS indicators collected by CI monitoring platforms – are organized in CI-independent metadata, used to feed the CI risk prediction tool and also the risk prediction tools of peer CIs (see Figure 2).

In order to synchronize the risk prediction tools of interrelated CIs a common risk model is used: the Mixed Holistic-Reductionistic (MHR) model (De Porcellinis 2009; Panzieri 2009). The MHR model (Figure 3) allows a common approach across the multiple (and heterogeneous) Critical Infrastructures but does not require a centralized or strongly coupled approach – clearly undesirable due to scalability, performance and security. Each CI uses the MHR model to estimate the risk levels of the services it provides, based on its own monitoring data – which the adaptor converts from CI-specific raw data to commonly understood metadata – and on the metadata received from peer CIs and related with the services it receives from those CIs. This makes it possible to have a global model distributed across multiple risk prediction tools (and therefore multiple CIs) whilst preserving synchronization (Gasparri 2009) and protecting the sensitive internal information from each CI (internal dependencies and current system status).

![Figure 3: Mixed Holistic-Reductionistic Modeling.](image)

3.2 Adaptors

The role of the Adaptors is to retrieve information from the CI-specific monitoring systems, to filter this information and to convert it into metadata in accordance to the generic ontologies and data formats used by the SMGW and the prediction tool. Each CI may have one or multiple adapters, according to the nature and number of monitoring and control systems it uses to feed the SMGW.
Figure 4 illustrates an adaptor that converts raw data from an electricity-related utility that uses an industrial control application (named Wizcon) based on the OPC protocol (OPC 2010). Based on the raw OPC data and the specific knowledge of the targeted CI the adaptor translates CI status information into XML-based metadata based on the common, CI-independent format used by the SMGW. If the utility decides to change its industrial control platform all it needs to do – from the point of view of the MICIE Alerting System – is to replace the adapter. Furthermore, in order to reduce the costs associated with the development of new adaptors, their structure is modular so that most of the components of CI-specific Adaptors remain technology independent.

![Figure 4: OPC Adapter for Electricity-related CIs.](image)

3.3 Secure Mediation Gateways

Figure 5 shows how the SMGW integrates into the MICIE framework. The Information Discovery Framework collects and stores metadata from the local CI-dependent adaptors as well as from peer interconnected SMGWs. This data feeds the local Risk Prediction Tool, whose output is used by the CI operators to take preventive or corrective measures in response to risk events. Selected sections of the stored metadata – somehow related to services provided to other CIs – might also be made available to peer SMGWs.

![Figure 5: SMGW role in the MICIE Framework.](image)

Figure 6 presents the architecture of the SMGW. Access to stored data is controlled by the SMGW Manager, which is based on the extensive use of policy-based access control to control both internal access (local operators and local components) and the access from peer CIs. There is also an auditing module that logs all accesses to sensitive information for future audits. A deeper discussion on these modules is available in (Caldeira 2010).
Communication between peer CIs is based on secure web services. In order to preserve sensitive information the metadata made available to each peer SMGW is usually restricted, based on the set of services (i.e. interdependency links) effectively provided to that peer SMGW. Within this restricted data set, peer SMGWs have multiple access models: periodic pools, subscription services, threshold alarms, etc.

4. Relation with European Initiatives – EPCIP and ECWIN

The European Council of June 2004 asked the European Commission (EC) to prepare an overall strategy to protect critical infrastructures. On 20 October 2004 the EC endorsed a “Communication on Critical Infrastructure Protection in the Fight Against Terrorism” which conveys suggestions on what could enhance European prevention, preparedness and response to terrorist attacks involving Critical Infrastructures.

The Council conclusions on “Prevention, Preparedness and Response to Terrorist Attacks” and the “EU Solidarity Programme on the Consequences of Terrorist Threats and Attacks”, adopted by the Council in December 2004, endorsed the intention of the Commission to develop the already mentioned EPCIP, where the CIWIN plays a key role as an enlarged CI warning network.

In November 2005, the Commission adopted a Green Paper on the European Programme for Critical Infrastructure Protection, which provided policy options on how the Commission could establish EPCIP and CIWIN.

A number of research projects have already been funded in the context of EPCIP. Most of these projects focus on the study of the protection of specific types of CI, i.e., security assessment of dams, security of industrial installations, bio-safety and bio-security management standards for laboratories, water infrastructures protection, security of airport structures, etc. In general, the scope of these projects does not encompass the study of frameworks for adequate exchange of information between interrelated CIs.

In this sense, MICIE complements those projects, addressing the mechanisms needed to implement in the future an important part of the CIWIN infrastructure. As it is described in the EC Green Paper and in the call for tenders, the CIWIN should be a network/rapid alert system, established by the Commission to assist Member States and owners and operators of CI to exchange information on shared threats, vulnerabilities and appropriate measures and strategies to mitigate risk in support of CI protection.
In the long term, the CIWIN could be envisaged to link all relevant CI owners and operators in each Member State through national contact points. Data would then be channeled through this national contact points, which would be connected to the Commission and thereby to all other Member States.

Three options are possible for the development of the CIWIN:

- The CIWIN may consist of a forum limited to the exchange of CIP ideas and best practices, in support of CI owners and operators.
- The CIWIN may become a Rapid Alert System linking Member States with the Commission.
- Or the CIWIN may become a multi-level system composed of two distinct functions: a Rapid Alert System and a forum for the exchange of CIP ideas.

In this context, the MICIE framework provides an alerting system that complements the services offered by the CIWIN. While the CIWIN is focused on the exchange of information and alarms between CIs organized in a centralized hierarchy (as information is collected by national contact points and the EC) the MICIE framework goes a step further, providing fully decentralized, CI-to-CI fast communication mechanisms, along with a set of tools for adequate data exchange between directly interdependent CIs – including common semantics, secure communication channels and data integrity mechanisms.

Other differences between the proposed alerting system and the CIWIN relate with the information exchange model. In the MICIE framework the exchange of information between interrelated CIs is continuous – in order to enable the prediction of risk levels – and occurs even in the absence of contingent alarms. Besides, this communication is more dynamic, making use of information discovery, filtering and composition tools making it possible to flexibly adjust the information exchange (specifically exchanged data, status refresh rates, level of detail, etc.) according to the circumstances.

The comparison between the MICIE Alerting System and the European CIWIN also applies to its North-American counterpart, the CWIN (Critical Infrastructure Warning Information Network) endorsed by the US Department of Homeland Security. In spite of minor differences between the CIWIN and the CWIN, they have similar functionalities and a similar centralized hierarchy.

5. The MICIE Framework in the Context of a Simple Reference Scenario

In this Section we discuss some of the key components of the MICIE framework in the context of a very simple Reference Scenario that encompasses a small portion of an electricity distribution network and an interdependent telecommunications network. A more extensive discussion of this scenario and its application to a number of risk analysis models may be found in (Capodieci 2009). The planned validation work – to be carried out in the final phase of the project – will also include more complex scenarios, provided by Israel Electric Corporation and including multiple CIs.

5.1 Reference Scenario

The reference scenario encompasses two distinct CIs:

- ELE: a portion of an electricity distribution network, including a Medium Voltage (MV) power grid at 22 KV and a High Voltage (HV) power grid at 160 KV, as well as the SCADA systems that control this network and Remote Terminal Units for remote operations.
- TLC: a portion of a telecommunications network with fiber and radio links that is used, among other applications, for the control of the above mentioned electricity distribution network. This network is administrated using specialized Network Management Systems.

In addition to these two components, the scenario also includes support services such as emergency power supplies, cooling systems, etc.).

5.2 MHR-Based Online Risk Prediction

As already mentioned, one of the difficulties involved in the inclusion of CI interdependency in on-line risk models relates with the need to avoid centralized systems – due to scalability, performance and data integrity reasons – whilst still allowing for some level of synchronization between different CIs.

Figure 7 illustrates how the MHR Model (De Porcellinis 2009; Panzieri 2009) might model such a Reference Scenario, allowing for a distributed and loosely coupled risk prediction tool (one risk prediction tool per CI, in this case) while still incorporating and synchronizing the interdependencies
between Critical Infrastructures. While each CI only sees its portion of the global model and only has access to status information directly related with that portion (its own monitoring data and the status data provided by peer CIs) the whole system behaves like a global risk prediction tool. 

![Decentralized Risk Prediction Tool](image_url)

**Figure 7**: Decentralized Risk Prediction Tool.

6. Conclusion

In this paper we presented an overview of the key components of the MICIE Alerting System. This alerting system represents one of the first attempts to effectively create on-line risk prediction tools able to incorporate, in real-time, the risk levels associated with the Quality of the Service provided by interconnected Critical Infrastructures.

The MICIE Alerting System complements public initiatives such as CWIN and CIWIN with a fast, lightweight and direct CI-to-CI communication framework, which is used not only whenever anomalies are detected but also during normal operation, proactively monitoring the risk of service degradation.

In addition to the use of multiple models for off-line interdependency analysis, the MICIE framework makes extensive use of MHR models in its risk prediction tools, in order to keep a decentralized and loosely coupled – yet synchronized – risk prediction tool.

Acknowledgments

This research work has been carried out in the context of the MICIE Project, partially funded by the EU with the contract FP7-ICT-225353/2008. The authors would also like to thank all the project partners for their precious input.

References


Capodieci, P. at al. (2009), “From heterogeneous modeling and analysis to an on line prediction tool to improve QoS of interdependent networks”, Proceedings of Electricity 2009 (The Annual Conference of the Society of Electrical and Electronic Engineers in Israel), Tel-Aviv, Israel.


MICIE (2010), MICIE Project Website (online), http://www.micie.eu

OPC (2010), Open Connectivity Foundation Website (online), http://www.opcfoundation.org


