

# Secure Mediation Gateway Architecture Enabling the Communication Among Critical Infrastructures

Filipe CALDEIRA<sup>1 4</sup>, Marco CASTRUCCI<sup>2</sup>, Matthieu AUBIGNY<sup>3</sup>, Donato MACONE<sup>2</sup>, Edmundo MONTEIRO<sup>1</sup>, Francisco RENTE<sup>1</sup>, Paulo SIMÕES<sup>1</sup>,  
Vincenzo SURACI<sup>2</sup>

<sup>1</sup>Universidade de Coimbra - CISUC, Pinhal de Marrocos, Coimbra, 3030-290, Portugal

Email: [fmanuel,edmundo, frente, psimoes]@dei.uc.pt

<sup>2</sup>Università di Roma "Sapienza" V. Ariosto 25, Rome, 00185, Italy

Email: [castrucci, macone, suraci]@dis.uniroma1.it

<sup>3</sup>Itrust Consulting, 18 Steekaul, L-6831 Berbourg, Luxembourg

Email: aubigny@itrust.lu

<sup>4</sup>Polytechnic Institute of Viseu, Viseu, 3504-510, Portugal

**Abstract:** Representing one of the most technological dependencies of contemporary societies, Critical Infrastructures (CIs) have to ensure the highest security levels to be able of fulfill their duty in any circumstances. This is the main goal of MICIE (Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures) FP7 ICT-SEC project: the design and implementation of a real-time CI risk level prediction and alerting system [1].

In order to reach this objective, one of the main key challenge to be addressed is the design and the implementation of a Secure Mediation Gateway (SMGW), namely a new innovative network element able to: (i) discover CI status information, (ii) overcome information heterogeneity and (iii) provide a secure communication of such information among peer CIs. All the information discovered and collected by the SMGW are then provided to a dedicated prediction tool which is in charge of calculating a risk prediction for the CIs.

This paper presents the functional architecture of the SMGW designed within the MICIE project, putting in evidence how it is possible to discover information and exchange critical information over a insecure network like Internet.

**Keywords:** Information discovery, Ontologies, Secure Communication, Critical Infrastructure

## 1. Introduction

MICIE FP7 ICT-SEC project (Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures)[1], aims to improve the critical infrastructure (CI) protection capability through the design and implementation of a MICIE alerting system that identifies, in real time, the level of possible threats induced on a given CI by undesired events happened in the reference CI and/or in other CIs which are interdependent with the reference CI. In fact, it is known that several interdependencies may occur among heterogeneous CIs, like electrical grid and telecommunication infrastructure or transport (railway) infrastructure.

MICIE alerting system will be able to provide, in real time, each CI operator with a CI risk level measuring the probability that, in the near future, he will no more be able to provide the CI services with the desired QoS in consequence of certain undesired events happened in the reference CI and/or in other interdependent CIs.

In order to make an accurate risk prediction, the alerting system needs information regarding the status of the CI object of the analysis, but also regarding all the interdependent CIs. Thus, a new system is needed able to: (i) discover all the distributed information that are relevant for the alerting system, (ii) overcome the heterogeneity of such information that are related to heterogeneous CIs (i.e. electrical infrastructure, telecommunication infrastructure, water distribution infrastructure, etc.), (iii) Exchange these information in a secure way over the Internet. To solve all these issues, a proper Secure Mediation Gateway (SMGW) is presented in this paper. The SMGW described in detail in the rest of the paper is able to discover distributed information by means of a dedicated information discovery framework; uses ontologies to create a common metadata for all the different CIs and provides the instruments for a secure communication over the Internet.

Other projects have already addressed this issues but with relevant differences.

One of them is IRRIS (Integrated Risk Reduction of Information-based Infrastructure Systems). According to [2], IRRIS main objective is the development of mechanisms that would permit raise the confiability, survivability and resilience of the information systems related to critical infrastructures.

IRRIS project has developed a set of applications named MIT (Middleware Improved Technology). Those applications make possible the communication between different CI's that use incompatible applications. MIT main objective is to permit a simple, fast and reliable information exchange between CI's, thus reducing response time to incidents that may occur in the CI's by maintaining network managers well informed about the CI state [2].

This system is working with data provided by a simulator (SimCIP) [2], while the SMGW object of this work able to work with raw data coming from CI real monitoring systems.

Another related project is CRUTIAL (CRITICAL UTILITY InfrastructurAL Resilience). In the CRUTIAL approach to security in CI's is given particular importance to CI's interdependency modeling to increase CI's resilience to faults and attacks [3].

But, at the best of author knowledge, CRUTIAL did not addressed the problem of exchanging information between remote CIs [3][4][5][6][7], so that most of the problems considered in this work are not taken into consideration in that project.

This paper is organized as follows. Section 2 presents the MICIE overall system architecture, while Section 3 describes in detail the SMGW architecture. Finally we draw the conclusions and indicate our perspectives for future work.

## **2. MICIE system architecture overview**

The identification and modeling of interdependencies can be very useful in order to limit the effects of a failure in a CI and even to prevent cascading effects. In particular, if a CI operator has the possibility to be informed of the status of their interdependent CIs, he can then make predictions on the status of delivered QoS level of its services and he can even undertake specific actions in order to prevent the failure of his CI when failures occurs in interdependent CIs.

To reach this goal, a communication system interconnecting different CIs is needed. Such interconnection system should allow the exchange of information between CIs.

The MICIE system, described in this paper, is the answer to the need of a proper communication framework between different CIs. Thanks to the MICIE framework,

different CIs can exchange proper information that is used by local prediction tools to calculate the risks for each CI, depending on the status of the CI and their interdependent CIs.

Figure 1 shows, at high level, the overall MICIE system architecture. In the picture it is possible to highlight the main entities of the MICIE system.

Each CI has its own monitoring system that collect, in real-time, information regarding the status of its components.

The SMGW provides a CI with a secure interface for exchanging important status information with other CIs on which it is interdependent. Namely, it focuses on

- Provision of a secure cross-CI communication infrastructure;
- Discovery of CIs critical events and propagation of relevant information to trusted interdependent CIs;
- Composition of CIs critical events and semantic inference;
- Extension of risk prediction from single CIs to multiple interdependent CI.

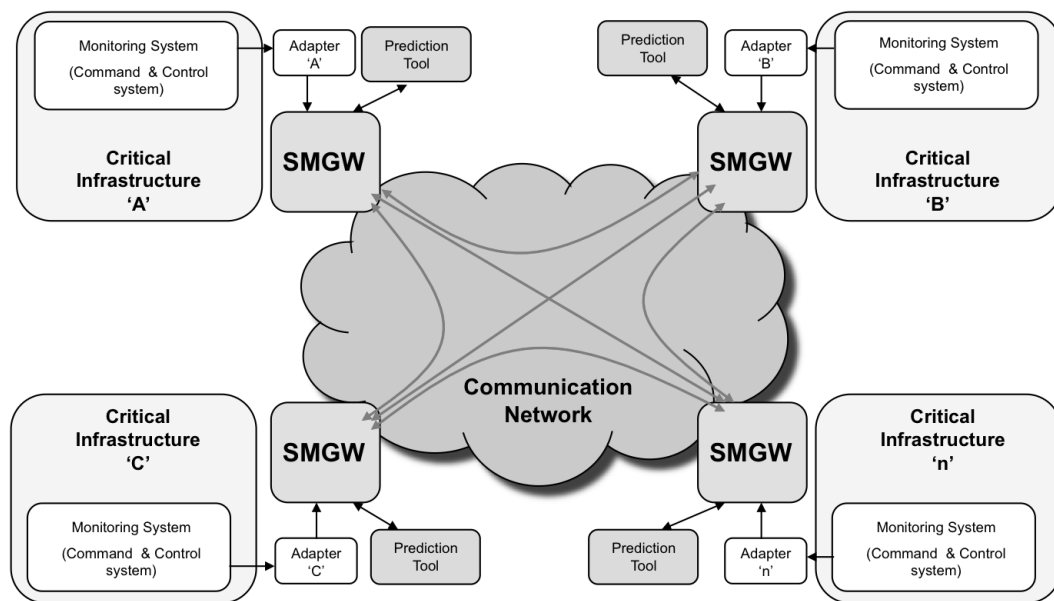


Figure 1: MICIE overall system architecture

SMGW is designed in order to be independent from the specific CI it belongs to. For this reason, a CI-specific adaptor is used to interconnect the SMGW to the CI. The role of the adaptor is to retrieve information from the CI specific monitoring system, to describe such information using a common data format and to provide these data to the SMGW. A specific adaptor has to be implemented for each CI in the system.

The Prediction Tool (PT) is the element of the system in charge of calculating a prediction of the risk for the CI and to provide that information to the CI operator in a display in the CI control room. To operate, the PT uses as input the models of the CIs system and the real-time information about the status of all the CIs included in the system and provided by the SMGW.

### 3. Secure Mediation Gateway architecture

Figure 2 depicts the SMGW architecture. The SMGW is a system implemented in each CI allowing reliable and secure communication and data exchange with other interdependent CIs. Each SMGW interacts with four main entities through the following interfaces:

- The local Critical infrastructure through the SMGW-Adaptor Standard i/f;
- The local Prediction Tool through the SMGW-PT i/f;
- Remote SMGWs of interdependent CIs through the SMGW-SMGW i/f;
- Personnel (PE) managing the SMGW through the SMGW control i/f.

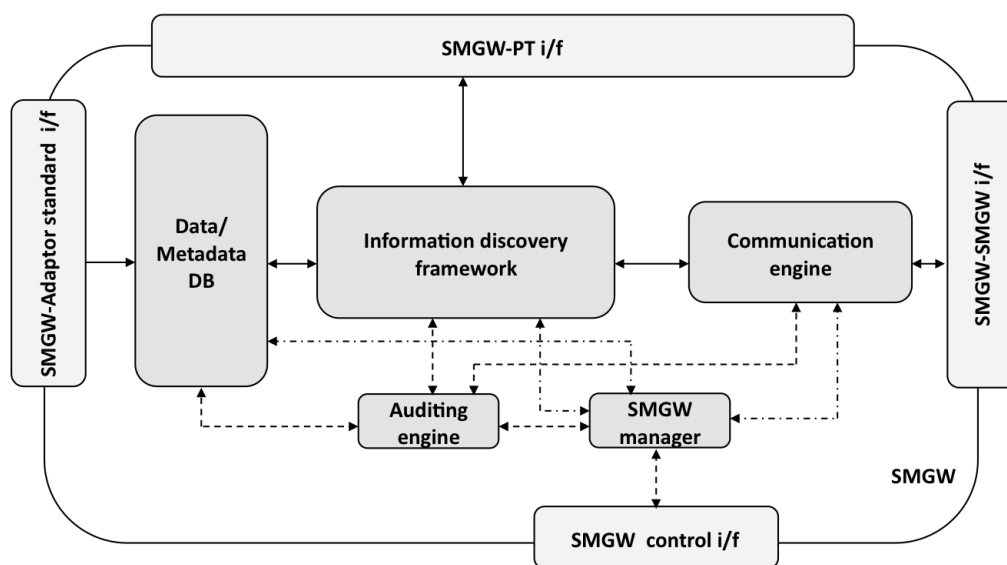


Figure 2: SMGW architecture

The internal architecture of the SMGW includes 5 entities implementing its main functionalities:

- Data/Metadata DB: this is an ontology-based DB used to conveniently store information about the local CI and remote interdependent CIs;
- Information Discovery framework: this is the agent able to detect critical events and important information to submit to the Prediction Tool for Risk assessment analysis;
- Communication engine: it implements secure communication support between CIs. It handles user and system authentication and encrypted data exchange with privacy and integrity protection. It implements firewalling;
- SMGW manager: manages the behaviour of all SMGW entities and detects malfunctioning performing SMGW monitoring through real-time and non-real-time log analysis. It also acts as intrusion prevention/detection engine by configuring firewalls in the communication engine;

- Auditing engine: it performs log management and realizes forensic analysis in order to verify correct and authorized access and use of the SMGW.

### 3.1 External Interfaces

The SMGW interacts with the exterior using 4 external interfaces:

**SMGW control interface** - It is used by a human operator to manage the SMGW, i.e. to check the status of devices, to configure policies and to retrieve management information from the SMGW.

**SMGW-Adaptor Standard interface** - It is used for the communication between the SMGW and the local CI. State information and characteristics of each CI are made available to the SMGW for sharing with authorized interdependent remote CIs in a standardized format. Vice versa data in standardized format are converted into local CI format when they have to be transferred from the SMGW to the local CI.

**SMGW-SMGW** - The communication engine is only responsible for providing a secure channel to other SMGWs over an untrusted network and the discovery engine is responsible for discovering and exchanging information. The main functionality of the interface between two SMGWs is therefore to provide a defined method that allows inbound and outbound connections.

To this scope an IP address and a port have to be defined to wait for incoming connections from the untrusted network and allow to establish connections to other SMGWs over the untrusted network. For instance, VPN provides a defined communication interface; the design of a communication interface between two SMGWs can therefore be neglected in the SMGW system design.

The definition of an interface as a translator between two entities that do not speak the same language can be neglected in this context as well, since all SMGWs are designed to use the same message format and therefore do not need an interface as a translator to understand each other.

**SMGW-PT** - It is used for communication between the SMGW and the local Prediction Tool subsystem. The PT uses this interface to indicate to the Information Discovery Framework (IDF) which information it needs for its operations and to provide to the SMGW the output of its predictions. The SMGW uses this interface to send information to the PT and to receive the output of PT predictions. The PT receives Metadata information from the SMGW. The PT provides correlated data which are stored in the SMGW and made available to authorized remote PTs.

### 3.2 Functional Entities

As stated, SMGW has 5 entities. In this section we present those functional entities:

**Auditing engine** - Auditing engine performs functionalities to support forensic analysis in case of SMGW failure or attack. Its operations are defined by a set of operational modes managed by the Security Management system. In order to provide forensic analysis support, the SMGW shall provide Live analysis support. In particular, SMGW shall

trace critical activities of each security software installed in the SMGW and trace critical activities of each custom service developed in the SMGW through log management procedures.

**SMGW manager** - SMGW Manager supports the use of policies implemented in form of a Policy Based Management Tool. This tool handles issues regarding the authorization, authentication and accounting. The SMGW manager controls both the interaction with peer SMGWs and all the internal operation of the SMGW, including also testing, alarming and the management of intrusion prevention and detection functions.

Defined policies will define all aspects of the relations between local SMGW and foreign SMGWs, including defining how each particular CI can connect and defining data access policies.

By example, the SMGW administrator can decide that we wants to exchange risk information with CI A, defining that he will only accept connections from this CI if the remote SMGW IP address is in one specific network. Also he can define that this remote SMGW must connect using a VPN connection and use a secure webserver for data transfer. Regarding data access, the policy GUI will permit to browse existent information and define everything that remote SMGW can view. He can also decide if remote SMGW can upload their status to our SMGW. All data access controls must be implemented with a high level of granularity but maintaining simplicity.

All the policies are represented in a formal way using a policy specification language and stored in a policy repository. SMGW manager will interact with other modules on the SMGW that will implement Policies acting as Policy Enforcement Points.

Ponder2 toolkit [8, 9] is used for the development of the SMGW manager where each SMGW entity is represented using Ponder2 concept of Managed Object. The complete set of SMGW entities will form a Ponder2 SMC (Self Managed Cell). Policies enforcement is based on Ponder2 Authorization Policies and Event Condition Action concepts.

**Data/Metadata DB** - It serves as an overall information database. It includes aggregated local information by the PT as well as raw information collected by the local adaptor. As for aggregated information from the PT it determines which kind of information can be made available for other peer prediction tools, on the basis of confidentiality as well as usability (information should allow peer prediction tool to work properly) requirements.

**Information Discovery framework** - It performs all the functionalities related to the discovery and composition of information required by the prediction tools.

The discovery process is a fundamental function provided by the SMGWs to the MICIE Prediction Tools. Thanks to the discovery process each SMGW is able to retrieve information on a specific request (on-demand mode) as well as intercept and notify spontaneously (trigger mode) some critical events which are of interest of the local Prediction Tool. The composition process acts with the discovery process to combine information from remote interdependent CIs and to enhance monitoring capabilities of the single Prediction Tool element in the local CI.

Namely in the on-demand mode, discovery is launched on request from an interdependent CI to collect information from a remote CI for local processing (on-demand

mode). Conversely, in the trigger mode the occurrence of an event and the modification of a status variables in a CI are propagated to interdependent CI through the cross-SMGW protected communication infrastructure spontaneously.

Through the composition process, local information available in a CI are combined with remote information provided by other interdependent CI in a single ontology. Semantic inference can be performed on the created ontology. Local ontologies in SMGWs, either following a composition process or directly available, are browsed through predefined navigation rules in order to discover new relationships among entities linked in the ontology. The Information Discovery framework could be implemented through the use of UPnP technology. Moreover security issues could be granted by the use of OpenVPN technology.

**Communication engine** - To allow secure communication between two SMGWs (i.e. a communication ensuring at least confidentiality, integrity and availability of data transmitted), a secure channel has to be established.. The best and cheapest way to provide a the confidentiality is to use a public communication network (untrusted network) and to encrypt all data exchanged, using a Secure VPN or a cryptographic protocol (HTTPS).

The availability of the communication is based on the availability of the communication channel (untrusted network) and on the availability of the SMGW communication device. The availability of a system can be threatened by different events, either by accidental or deliberate failure of equipment, either by denial-of-service attacks. For the communication channel, the availability is ensured by the network provider using a high availability solution as MPLS. For the SMGW devices, physical protection, redundancy and filtering or intrusion/detection systems must be implemented.

The communication engine has also to provide the integrity of the data exchanged. The loss of integrity can be accidental (e.g. a noisy communication channel) or deliberately an attacker. Methods to assure data integrity include, by example, message authentication (e.g. RSA protocol and digital signature).

The communication engine only provides a secure channel to exchange the messages. It might, however, be necessary to add certain security related data (e.g. timestamps, redundant information) to a message before transmission to provide application layer security features.

## 4. Conclusions

The present work describes the first research results of the FP7 ICT-SEC MICIE project. MICIE intends to develop a real-time risk level dissemination and alerting system. To achieve this objective, a system architecture has been presented. It is based on a distributed, reliable and secure communication network where the key enabling element is the Secure Mediation Gateway.

The SMGW allows heterogeneous CI to securely and timely communicate relevant data to predict in advance how local failures, threats, malfunction, adverse events can affect the operative level of interconnected CIs. The MICIE approach is disruptive and represents a sensible step beyond the state of the art. The use of a distributed architecture to setup a future-proof communication network, allows CI interoperability to achieve the common goal to predict and mitigate the widespread of local failures

in the whole system of interconnected CIs. The use of semantic technologies allows heterogeneous data to be exchanged among different CIs without ambiguities. The use of adaptors allows heterogeneous field data to be aggregated, filtered, semantically enriched and stored to be used by different CIs prediction tools. On the light of the above, the MICIE solution represents a milestone for the CIs interoperation and the project research team is willing to develop a proof of concept demonstrator to be tested on the field.

## 5. Acknowledgments

This work is partially financed by FP7 ICT-SEC MICIE project [1] grant agreement no. 225353, and by the Portuguese Foundation for Science and Technology (FCT - Fundação para a Ciência e Tecnologia) with the grant SFRH/BD/35772/2007. The authors want to thank all the involved partners for their valuable support to this work.

## References

- [1] Micie, “Micie - tool for systemic risk analysis and secure mediation of data ex-changed across linked ci information infrastructures,” *FP7-ICT-SEC-2007.1.7 – 225353 – Annex I – “Description of Work”*, 2008.
- [2] IRRIS, “Irriis project web site,” <http://www.irriis.org/>, 2008.
- [3] Crutial, “Crutial project web site,” <http://crutial.cesiricerca.it>, 2008.
- [4] P. Verissimo, N. Neves, M. Correia, Y. Deswarte, A. A. Kalam, A. Bondavalli, and A. Daidone, “The crutial architecture for critical information infrastructures,” *Architecting Dependable Systems V*, vol. Volume 5135/2008, 2008.
- [5] G. Dondossola, F. Garrone, J. Szanto, and F. Gennaro, “A laboratory testbed for the evaluation of cyber attacks to interacting ict infrastructures of power grid operators,” *SmartGrids for Distribution, 2008. IET-CIRED. CIRED Seminar*, pp. 1 – 4, May 2008.
- [6] P. Verissimo, N. F. Neves, and M. Correia, “The crutial reference critical information infrastructure architecture: a blueprint,” *International Journal of System of Systems Engineering*, Jan 2008.
- [7] A. Bessani, P. Sousa, M. Correia, and N. Neves, “Intrusion-tolerant protection for critical infrastructures,” *DI/FCUL TR*, Jan 2007.
- [8] K. Twidle, E. Lupu, N. Dulay, and M. Sloman, “Ponder2 - a policy environment for autonomous pervasive systems,” *Policies for Distributed Systems and Networks, 2008. POLICY 2008. IEEE Workshop on*, pp. 245 – 246, May 2008.
- [9] K. Twidle, N. Dulay, E. Lupu, and M. Sloman, “Ponder2: A policy system for autonomous pervasive environments,” *Autonomic and Autonomous Systems, 2009. ICAS '09. Fifth International Conference on*, pp. 330 – 335, Apr 2009.