

Critical Infrastructure Security Modelling and RESCI-MONITOR: A Risk Based Critical Infrastructure Model

Thomas SCHABERREITER¹, Jocelyn AUBERT¹, Djamel KHADRAOUI¹

¹*Centre de Recherche Public Henri Tudor, 29, avenue John F. Kennedy,
Luxembourg, L-1855, Luxembourg*

Tel: +352 425991-1, Fax: +352 42599-777,

Email: {firstname.lastname}@tudor.lu

Abstract: Critical infrastructure (CI) services are consumed by the society constantly and we expect them to be available 24 hours a day. A common definition is that CIs are so vital to our society that a disruption or destruction would have a severe impact on the social well-being and the economy on a national and an international level. CI sectors include, amongst others, the electricity, telecommunication, air traffic and transport sectors. CIs can be mutually dependent on each other and a failure in one infrastructure can cascade to another interdependent infrastructure to cause service disruptions. Methods to better assess and monitor CIs and their interdependencies in order to predict possible risks have to be developed. In this work we present a CI modelling approach called CI security modelling and RESCI-MONITOR, a tool that allows implementing a CI security model. The CI security model allows to monitor CI services and its associated dependencies in real-time by evaluating the current risk in CI services. The multi-agent based support tool RESCI-MONITOR is able to receive real-time measurements from the infrastructure, transform them into risk parameters and evaluate them in combination with the current risk in dependent infrastructure services.

Keywords: Critical infrastructures, risk, security modelling, multi-agent system.

1. Introduction

Critical infrastructures (CI) provide services that build the centre of our society and economy. For example, telecommunication infrastructures allow us to communicate with people and businesses at remote locations, transport and air traffic infrastructures allow us to travel to places far away for free-time or business activities. The electricity infrastructure enables a variety of services and applications that we take for granted. Furthermore, CIs depend on each other. A good example is the electricity infrastructure that is a requirement for all other CIs, since almost everything relies on a constant supply of energy nowadays. A failure in one CI can cascade to other CIs and cause service disruptions. To operate complex systems like CIs can be problematic and CI providers put substantial effort into keeping CIs running and reduce risks of any kind, for example the risk of failure, the risk of intrusion or the risk of incorrect operation.

In the context of risk in critical infrastructures, especially when taking the dependencies between infrastructures into account, some research questions can be raised. One question would be "How to address the complexity of CIs?". An approach that we evaluate is the partitioning of CIs into smaller, easier to comprehend entities. That leads to the next question "What is an adequate and useful way of partitioning CIs?". In general, a flexible way of representing portions of CIs following their real structure, portable to the various CI

sectors and their structural variety should be investigated. The approach that will be followed in this work is a service oriented approach which means that CIs are structured into services they provide to customers.

Another relevant question is "How to address the dependencies between CIs?". A CI provider might need the services of another CI provider to be able to operate. A way to notify dependent CIs or CI services of changes in the service level would be beneficial and allow CI providers to react adequately to risks in dependent services and prevent failures from cascading. That leads to the last two questions that will be covered in this work: "How can CIs be compared?" and "How can information be shared between CI providers in order to enhance security?". The main problem is that CIs are operated by different providers. Each provider has different infrastructure, operation strategies, business models, trade secrets, etc. Providers hesitate to share internal information that is often confidential and not intended to be shared with external parties. Furthermore, even if information is shared, the diversity of the infrastructures might make it difficult for an expert in one domain to interpret information received from a CI that is not related to his expertise. One approach to solve this problem can be abstraction. In this work we follow the approach of abstracting information gathered from CIs to risk related parameters which will be the same for all CI sectors. This enables us to compare different CIs and encourages information sharing since no internal, possibly confidential, information needs to be shared.

Related work focuses on different approaches to CI modelling (e.g. [1,2,3]) and risk in general (e.g. [4]) as well as risk assessment, estimation and calculation in CIs (e.g. [5,6,7]).

2. Objectives

The security modelling approach tries to address the challenge of on-line monitoring of the state of CI services and their interdependent services. Furthermore, another advantage of our approach is the reduction of the complexity of a service through abstraction to a common (risk related) set of parameters. This enables to compare CIs designed to serve a very different purpose (electricity, telecommunication, air traffic,...) and that are composed of very different infrastructure components. Usually information about the state of CIs is confidential and providers hesitate to share the information that would enhance security of their infrastructure or the quality of their services. Information sharing between CIs is seen as a key feature to enhance CI protection and we think that the abstraction to a small set of common parameters will encourage service providers to share them with interdependent providers.

3. Methodology

CI security modelling was presented in [8,9]. As illustrated in Figure 1, the aim of the approach is to transform real-world infrastructure information into common abstract risk related information (in our case confidentiality, integrity and availability- CIA), to use this information to monitor the state of the infrastructure and to share it with interdependent infrastructures in order to be able to evaluate the current infrastructure risk by taking into account the interdependencies.

Our methodology, as illustrated in Figure 2, is composed of three steps: an *off-line risk assessment*, a *measurement aggregation* and an *on-line monitoring* step.

The off-line risk assessment step deals with an analysis of the infrastructure. We see CIs as service providers which provide services to customers. Those customers can in turn be other dependent or interdependent CIs or CI services which need the service in order to provide their own service(s). In order to be able to observe the CI state, we need to identify observable entities in the infrastructure (base measurements). Each base measurement is associated to one or more CI service(s). Furthermore, to quantify the contribution of a base

measurement to the CIA of a service, a weight is associated to each base measurement. The same applies to each identified dependency. It is weighted to reflect how much a dependent service contributes to CIA of a service. In the model, each *service* can be composed of *sub-services* (0..n), *base measurements* (0..n) and *dependencies* (0..n).

Another concept of the CI security model is the concept of *assurance levels*. An assurance level reflects how much confidence one has in the correctness of a base measurement. They are formed by expert opinion and allow to assign a value between [1..5] to each base measurement, 1 meaning the lowest and 5 meaning the highest confidence in the accuracy of a base measurement.

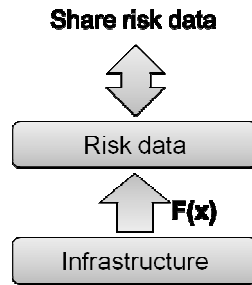


Figure 1: CI security modelling approach

In the measurement aggregation step, each identified base measurement is normalized to a five step scale to be able to compare base measurements. For discrete decimal values (e.g. current system load) this normalization is done by calculating the deviation from an expected value and categorizing this deviation into five classes. For Boolean data (e.g. switch is on/off) this normalization is easier, as it is either reached (5) or not reached (1). After the normalization, the base measurements assigned to each service are aggregated into risk data by calculating an averaged weighted sum of the normalized base measurements. This will produce three risk indicators (CIA) for each service, each representing a risk level between [1..5]. Sub-service risk levels are also taken into account in the service risk aggregation. Risk in this context can be seen as CI behaviour different from normal behaviour. This can be applied to virtually any situation where a CI service behaves different from normal operation. In our approach this can be expressed numerically in CIA indicators. The reduction to five levels of risk was chosen as a trade-off between granularity of risk representation and the interpretability of risk information by an operator in a stress situation.

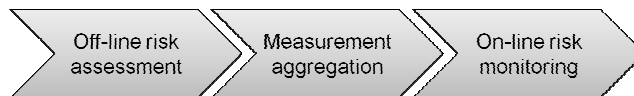


Figure 2: CI security modelling steps

Similar to the service risk level aggregation, assurance levels are aggregated to receive a service assurance level reflecting how much confidence one has in the correctness of the calculated service risk levels.

In the on-line risk monitoring step, each CI service receives risk indicators from interdependent CI services and can, after applying the associated interdependency weight for CIA, use this information to adjust the overall service risk in real-time.

4. Technology Description

RESCI-MONITOR, a tool that implements the CI security model, was presented in [10]. The overall architecture of RESCI-MONITOR can be seen in Figure 3.

The service agents (S_A) are used to represent CI services and aggregate risk levels. The probe agents (P_A) are used to collect and normalize base measurements from the infrastructure. The database management agent is used to receive updated risk information

from service agents and from the interconnection agent and store them in a database. The interconnection agent is used to establish a secure connection to other CIs via a web service and distribute updated risk information. The graphical user interface (GUI) is used to visualize CI service risk to an operator in real-time. Finally, the configuration engine is used to set up the structure of the tool via a predefined XML structure.

The multi-agent platform JADE is used to implement the tool on top of it because the concept of autonomous, intelligent and interacting agents perfectly supports the structure of the security model. Each CI can be represented by an instance of the JADE platform and each CI service can be represented by an agent.

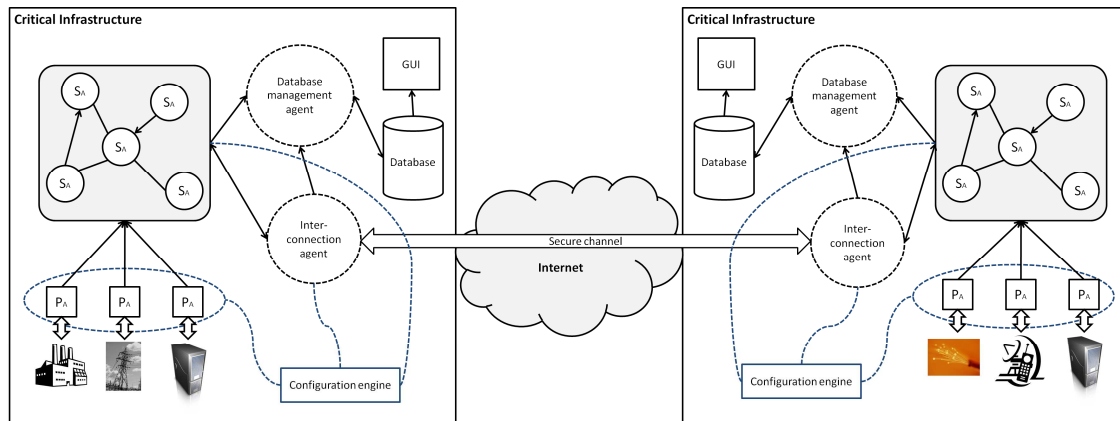


Figure 3: RESCI-MONITOR global architecture

4.1. Configuration engine

The off-line risk assessment step of the security model generates an XML structure used as configuration entity to RESCI-MONITOR. It contains information about identified services, dependencies and base measurements. Furthermore, the configuration contains connection information to interdependent CIs (or actually to their interconnection agents). This information is used to configure the interconnection agents and allows them to connect to an interdependent infrastructure if required.

The last class of information in the XML configuration is information about identified CI services. Each entry contains information about the associated base measurements (which is used to configure a service to register to the appropriate probe agents), the associated sub-services (which is used to configure a service to register for security states updates of those services) and it contains information about dependencies (which is used to configure a service to register to security states updates of internal or external dependent services).

4.2. Probe agents

Probe agents are actually organized in two parts: a generalized part that is used for base measurement normalization and a individual part that acts as an interface to the CI equipment that can provide base measurements. It has to be implemented separately for each type of CI equipment. The interface part is located at the CI equipment and communicates to the measurement agent via an IP interface. A base measurement is characterized by a unique name and the current base measurement value. A probe agent can register for a base measurement and the infrastructure interface will send updated values to all registered probe agents. In our test set-up, CIs are currently simulated via python scripts that generate random base measurement values and distribute them to registered probe agents.

The generalized part is responsible for measurement normalization. When an agent receives an updated value, it transforms this raw value into a normalized value in the [1..5] range that can be compared and processed. This transformation involves computing the deviation of the current value towards an expected value, and comparing this deviation with four threshold values previously defined. This last step enables producing discrete natural values between [1..5].

4.3. Service agents

The service agent is responsible for risk aggregation. It receives the information to aggregate from three different sources: normalized base measurements provided by probe agents [0..n], risk indicators provided by its sub-services [0..n], risk indicators provided dependent services [0..n]. The service risk is aggregated by calculating a weighted sum of all information sources. The expected service risk level is a natural value between [1..5]. If the aggregated risk level is different from the previous aggregated risk level, it is distributed either directly to dependent services (internal services) or via the interconnection agent (external services). Furthermore, the new risk level is stored in the database via the database management agent.

4.4. Database and database management agent

Each CI has his own database management agent and database to memorize the history of calculated and received risk level indicators. The database management agent is used as the only point of connection from to the relational database from within the multi-agent platform to operate CRUD (create, read, update and delete) operations on the data. This architecture was chosen to be able to host the database and database manager on a different, possibly more secure place since it is assumed that the database is a valuable point of attack. We utilize the fact that a distributed agent model permits to host the database management agent in a different location. The database management agent handles messages coming from the interconnection agent and the internal services and stores the information in the database. The GUI component of the tool has direct access to the information stored in the database to be able to display the calculated risk information in an external (outside the multi-agent platform) interface.

4.5. Interconnection agent

The interconnection agent is responsible for sending updated risk information of internal services to interdependent CIs and receiving updated risk values from interdependent CIs. Risk information received from interdependent CIs is distributed to subscribed internal services and additionally stored in the database via the database manager. Connection to interdependent CIs is achieved by maintaining a secure connection via a web service.

4.6. Graphical user interface

The graphical user interface presented in Figure 4 is designed to provide an easily understandable overview of the security status of a CI by displaying the real-time risk of each CI service. The major space on the left side of the interface (1) shows the risk of the service an operator is currently interested in. The displayed service risk includes the risk of all sub-services and dependencies of the service in question. The three lines in the risk diagram represent the evolution of the CIA service risk parameters over time in a scale [1..5]. On the right side of the service risk (2), a list of all sub-service risks is shown to allow a fast evaluation of causes in case the service risk increases. To support this, the sub-

service list is constantly rearranged to show the sub-services with the highest current risk on top. A click on one of the sub-services will cause the interface to display the risk centred around this sub-service and shows it in the area on the left side (1) as main service. Sub-service and dependency risk will be displayed according to the configuration of this service.

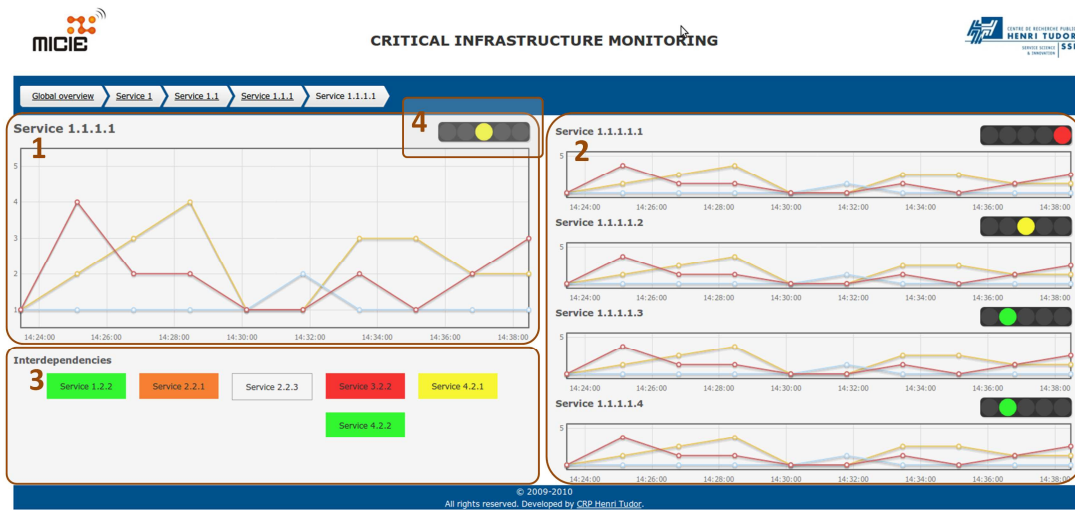


Figure 4: RESCI-MONITOR graphical user interface (GUI)

The traffic light inspired indicators (4) show the assurance level of the currently displayed risk and therefore the confidence we have in the correctness of this value.

Below the area of the main service, dependent service risks are displayed (3). The current risk of dependent services is indicated in different colouring, ranging from green (low risk) to red (high risk). The different visualization scheme (compared to the sub-service risk) was chosen since it is assumed that, if the service risk comes from another CI, no further investigation revealing the root cause of the failure can be done. Only the change in service risk is received from the interdependent CI, no details about the internal structure causing the failure are revealed.

5. Developments

A software tool was developed following the architecture described above. For the implementation a number of tools were used. Those tools include Eclipse 3.5.1 as development environment, the multi-agent platform JADE 4.0.1 and the JADE-S plug-in version 3.7. JavaScript InvoVis Toolkit 2.0.0 was used to generate dynamic graphs, the SQLite 3.0 library was utilized to provide a database management system using SQL. For the graphical user interface we used xHTML version 1.1 and PHP version 5.3 for database access. Apache HTTP server version 2.2.16 is used to enable remote access to the GUI. The tool was designed to be operating system independent.

6. Results

CI security modelling and RESCI-MONITOR have been validated using the reference scenario of the EU-FP7 project MICIE. This reference scenario is provided by an industrial partner and covers parts of an electricity infrastructure and a telecommunication infrastructure in the form of documents describing the high level structure of the infrastructures and more technical documents describing some of the infrastructure components. A focus of the reference scenario is in highlighting of the dependencies between the two providers which allows a useful utilization of the CI security model.

The provided reference scenario had some limitations when the CI security model was applied. Those limitations mainly concern the off-line risk assessment step of the security

model where the provided information was not detailed enough to conduct a meaningful risk assessment. Therefore, gaps in the scenario description were filled by publicly available information and assumptions. Information that has to be provided by domain experts, for example base measurement, sub-service and dependency weights, was estimated without consulting domain experts. However, it is assumed that the MICIE reference scenario and the provided information are sufficient for a proof-of-concept validation of the CI security model.

This reference scenario was implemented and simulated using RESCI-MONITOR. The MICIE reference scenario does not provide dynamic data of normal CI behaviour or incidents. The dynamic behaviour of the electricity and telecommunication infrastructure is emulated by changing the identified base measurements according to pre-defined scenarios. It has been shown that scenarios that produce a high risk in one service propagate the risk to higher level super-services and to dependent services and can be evaluated and monitored. However, the practical relevance of the risk monitoring using RESCI-MONITOR has not been evaluated yet. This could be done by showing the simulation to CI operators and evaluate the usefulness of the monitoring component with them.

7. Business Benefits

There are several benefits for businesses using CI security modelling to monitor the security state of their provided services. The abstraction of infrastructure to risk related parameters allows an operator to monitor services in a clearly represented manner. The reduction to five different risk magnitudes will support operators to maintain oversight of the current state of a CI service even in stress situations.

Including the risk of dependent services in the on-line monitoring of CI service risk will enhance the understanding of the general structure of the highly interdependent CI sector. Knowing the current risk present in a dependent CI service will allow operators to plan ahead in case of an incident in the dependent service and prevent disruptions or quality degradations in the service in question.

Information sharing is usually difficult for CI providers. CI information that could enhance security or quality of service in dependent CI services cannot be shared because it is confidential. The abstraction of possibly confidential data to risk related parameters will encourage to share this information and help to enhance the quality-of-service of CIs. This is seen as a major benefit for businesses.

Another benefit of the CI security model for businesses is the ability to compare different types of infrastructure using common risk related parameters. Especially the CI sector is characterized by a diversity of infrastructure designed to serve different purposes and provide services of different kind. Operators who depend on the services of other CIs and have information about the infrastructure can have difficulties to correctly interpret the provided information since they are not experts in the domain of the other CI. A common set of parameters makes it easier to interpret the information received from dependent CIs or CI services.

8. Conclusions

In this paper we presented CI security modelling, a risk based CI model enabling real-time monitoring of CI services. Furthermore, the design and implementation of RESCI-MONITOR, an agent-based support tool that implements the CI security model and enables simulation of CI security models was presented. The nature of the CI security model perfectly supports the use of a multi-agent system for implementation, the global architecture of the tool as well as the individual parts of the architecture were detailed.

Current and future work focuses on further enhancements of the security model. More specifically, it will be extended with a risk prediction component based on probabilistic networks that allows estimating the most probable future risk given a state change in the current risk of either the service or of an interdependent service. This approach will be integrated in the service agent component of the support tool to be able to predict, in real-time, the most probable evolution of a change in service risk.

The business based reference scenario provided by an industrial partner in the EU-FP7 project MICIE was evaluated using the CI security modelling approach and simulated using RESCI-MONITOR. This allowed a proof-of-concept validation of the security model as well as the RESCI-MONITOR tool in a close to reality set-up. Since the validation using the MICIE reference scenario had some limitations due to missing data, future work will focus on finding an industrial partner that can provide a more detailed reference scenario that will allow a more complete evaluation of the CI security modelling approach.

9. Acknowledgements

This work has been carried out in the framework of the MICIE project, partially funded by the EU with the contract FP7-ICT-225353/2008 and by the Luxembourgish Ministry of Culture, Higher Education and Research (MCESR). The authors thank all project partners for many interesting discussions which greatly helped to formulate the security modelling approach which lead to the implementation of the presented tool. One of the authors would like to thank the Luxembourgish National Research Fund (FNR) for funding his PhD research under AFR grant number PHD-09-103.

References

- [1] J. Sokolowski, C. Turnitsa, and S. Diallo, "A conceptual modeling method for critical infrastructure modeling," in Simulation Symposium, 2008. ANSS 2008. 41st Annual, April 2008, pp. 203–211.
- [2] S. Panzner, R. Setola, and G. Ulivi, "An approach to model complex interdependent infrastructures," in 16th IFAC World Congress, 2005, cISIA, Critical Infrastructures.
- [3] S. Rinaldi, "Modeling and simulating critical infrastructures and their interdependencies," in System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on, jan. 2004, p. 8.
- [4] E. Adar and A. Wuchner, "Risk management for critical infrastructure protection (CIP) challenges, best practices tools," in Critical Infrastructure Protection, First IEEE International Workshop on, 3-4 2005.
- [5] K. Haslum and A. Arnes, "Multisensor real-time risk assessment using continuous-time hidden markov models," in Computational Intelligence and Security, 2006 International Conference on, vol. 2, 3-6 2006, pp. 1536–1540.
- [6] D. Newman, B. Nkei, B. Carreras, I. Dobson, V. Lynch, and P. Gradney, "Risk assessment in complex interacting infrastructure systems," in System Sciences, 2005. HICSS '05. Proceedings of the 38th Annual Hawaii International Conference on, jan. 2005, pp. 63c–63c.
- [7] X. Tan, Y. Zhang, X. Cui, and H. Xi, "Using hidden markov models to evaluate the real-time risks of network," in Knowledge Acquisition and Modeling Workshop, 2008. KAM Workshop 2008. IEEE International Symposium on, 21-22 2008, pp. 490–493.
- [8] Aubert, J.; Schaberreiter, T.; Incoul, C.; Khadraoui, D.; Gateau, B.; , "Risk-Based Methodology for Real-Time Security Monitoring of Interdependent Services in Critical Infrastructures," Availability, Reliability, and Security, 2010. ARES '10 International Conference on , vol., no., pp.262-267, 15-18 Feb. 2010
- [9] J. Aubert, T. Schaberreiter, C. Incoul, and D. Khadraoui, "Real-time security monitoring of interdependent services in critical infrastructures. case study of a risk-based approach," in 21th European Safety and Reliability Conference (ESREL2010), September 2010.
- [10] T. Schaberreiter, C. Bonhomme, J. Aubert, C. Incoul, and D. Khadraoui, "Support tool development for real-time risk prediction in interdependent critical infrastructures," in Risk and Trust in Extended Enterprises (RTEE2010) Workshop. ISSRE Wksp 2010. IEEE International Symposium on Software Reliability Engineering, November 2010.