

Real-Time Security Monitoring of Interdependent Services in Critical Infrastructures.

Case study of a Risk-Based Approach.

Jocelyn Aubert, Thomas Schaberreiter, Christophe Incoul and Djamel Khadraoui

Public Research Centre Henri Tudor

Centre for IT Innovation (CITI)

29, avenue John F. Kennedy

L-1855 Luxembourg, Luxembourg

{firstname.lastname}@tudor.lu

Phone: +352 42 59 91 - 1

Fax: +352 42 59 91 - 777

In today's world, where most of the critical infrastructures (CIs) are based on distributed systems, security failures have become very common, even within large corporations. The critical infrastructures are tightly interconnected, mutually dependent, and are exposed everyday to new risks. These (inter)dependencies generate potential cascading effects that may spread a malfunction or an attack from one part of the system to another dependent infrastructure.

In this paper, we propose a risk-based methodology that aims to monitor interdependent services based on generic risks and assurance levels using the classical security properties: confidentiality, integrity and availability (C,I,A). This allows to determine the security state of a critical infrastructure service, taking its dependencies to other services into account. Furthermore, our approach allows to monitor the system state on-line during system operation. Monitoring of the security state of a service helps to determine the quality of the provided service (QoS) and allows each CI provider to react and adopt the best behaviour corresponding to the security status of its different services.

1 INTRODUCTION

A critical infrastructure (CI) is defined by the European Commission as "[...] those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States. Critical infrastructures extend across many sectors of the economy and key government services." (Brunner and Suter 2009).

The infrastructure of these systems is usually composed of systems that depend on each other. Rinaldi et al. (Rinaldi et al. 2001) define dependency as "a linkage or connection between two infrastructures, through which the state of one infrastructure influences or is correlated to the state of the other". An interdependency is given if two infrastructures mutually depend on each other. A malfunction or an attack

on one part of the system can lead to system failure or violation of information security in another part of the infrastructure or to an other dependent infrastructure. We assume that each critical infrastructure is composed of services that are provided to customers. Services may be self-contained or they depend on other services, which may be provided by the same or by another service provider.

Current risk analysis methods do not provide a way to share risk knowledge between providers forming a CI. Providers have expertise on risks on their own infrastructure, but not on related infrastructures of other providers. In most cases, this knowledge can not be shared for confidentiality reasons. Also, since different critical infrastructures are very different in nature, risk data gathered from an infrastructure can not easily be interpreted by non-domain experts.

In this paper we present an approach that allows monitoring of critical infrastructures by considering

the state of the service in question as well as the states of interdependent services. This can be achieved by abstracting data gathered from the infrastructure to a common set of parameters that can be shared with interdependent infrastructures.

Our methodology, as illustrated in Figure 1, is composed of three steps: an off-line risk assessment, the measurement aggregation and the on-line monitoring step. Each step will be explained in the following sections, although the focus of this work will be the measurement aggregation step.



Figure 1: Steps of the risk-based methodology

2 RELATED WORK

Critical infrastructure interdependencies are complex and not easy to understand. (Rinaldi et al. 2001) provide an excellent overview on the dimensions in which interdependencies can occur. In (Rinaldi and M. 2004) critical infrastructures and their interdependencies are analysed and different suitable modelling techniques are discussed.

The IRRIS project (IRRIIS 2009) aims to provide a collection of software components to facilitate communication between infrastructures and infrastructures providers in order to enhance security of large and complex CIs. An agent-based simulator has been developed to understand CIs and interdependencies.

The CRUTIAL project (CRUTIAL 2009) aims at modelling interdependent infrastructures attempting at casting them into new architectural patterns, resilient to both accidental failures and malicious attacks.

In the context of CRUTIAL, (Chiaradonna et al. 2007) aim at modelling electric power systems by separating the infrastructure and its control systems. (Laprie et al. 2007) are modelling the interdependencies between electricity and information infrastructures. From a high level representation of failures, the cascading, cascading/escalating and common-cause failures are addressed.

Conceptual modelling is used by (Sokolowski et al. 2008) to represent an abstract, simplified view of CIs. (Panzieri et al. 2005) utilize the complex adaptive systems (CAS) approach. The model is derived by modelling the mutually dependent sub-systems of the infrastructure. (Permann 2007) uses genetic algorithms to model and simulate critical infrastructures in the context of disaster protection and recovery. (Min et al. 2007) aim to model critical infrastructures and interdependencies based on system dynamics, functional modelling and non-linear optimization and take

physical as well as economic infrastructures into account. In (Svendsen and Wolthusen 2007) a graph based model to address critical infrastructures interdependencies is presented.

(Adar and Wuchner 2005) discuss challenges in critical infrastructure risk management and outlines methods as well as best practice guidelines to address risk management in critical infrastructures. In (Tan et al. 2008) real-time risk management is achieved in three phases: risk analysis, risk evaluation and risk prediction. The continuous time hidden Markov model is used for risk evaluation. In (Haslum and Arnes 2006) continuous-time hidden Markov models are used for real-time risk calculation and estimation.

3 SCOPE AND CONTRIBUTION

As mentioned in the introduction, the main focus lies on providing a strategy to monitor the quality of a provided service (QoS). One way to achieve this is to monitor the system state and detect changes in the system state caused by internal or external events (e.g. system failure or cyber attack). Due to the distributed nature of critical infrastructures, a service provider might also be interested in monitoring the system state of services needed to provide his service (dependencies or interdependencies).

Our approach tries to address the challenge of on-line monitoring of the state of critical infrastructure services and their interdependent services. To our knowledge, no approach was presented that does not only aim at monitoring the availability of a service, but also other important system parameters like confidentiality and integrity. Furthermore, an other 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 critical infrastructures designed to serve a very different purpose (energy, telecommunication, air traffic,...) and that are composed of very different infrastructure components. Usually information about the state of critical infrastructures 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 critical infrastructures is seen as a key feature to enhance critical infrastructure protection (ENISA 2009) and we think that the abstraction to a small set of common parameters will encourage service providers to share them with interdependent providers.

Unlike previous models discussed in the related work section, our methodology does not aim at enhancing critical infrastructure protection through modelling in order to better understand the nature of critical infrastructures and their interdependencies. Our focus lies on on-line monitoring to react and adopt the operation of services if a critical change in

the state of a service or of any of its interdependent services occurred.

4 METHODOLOGY

In this section the methodology is detailed. As illustrated in Figure 2, the aim of the approach is to transform real-world infrastructure information to abstract risk related information and to use this information to monitor the state of the infrastructure and to share it with interdependent infrastructures. The three modelling steps are detailed in the following sections.

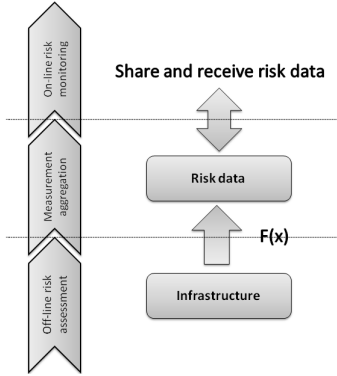


Figure 2: Outline of risk-based approach

4.1 Off-line risk assessment

This first step widely relies on a complete risk analysis of the concerned infrastructure to determine services that can be considered critical. During this first step, the following activities should be conducted: Critical services identification, Interdependencies identification, Base measures identification, Metrics composition and Interdependency weighting.

Critical services identification This first activity aims to identify services within the scope of the infrastructure that may be considered as critical. A critical service is a service for which failure to comply with confidentiality, integrity or availability would eventually undermine global functioning (e.g. QoS) of the infrastructure. Once the services are identified, all the assets contributing to the service’s goals should be identified. This identification consists of a detailed inventory of components used directly or indirectly by the service. Care has to be taken to achieve a detailed representation of critical services and components to reach a close representation of the current situation. In order to effectively perform this inventory, it is possible to rely on widely recognized risk analysis methods such as EBIOS, OCTAVE or CORAS.

Interdependencies identification Based on the list of identified critical services and components, this activity aims to identify all the relationships (dependencies or interdependencies) between services. The scope of this identification covers internal dependen-

cies (within the infrastructure) as well as external dependencies (between services of other infrastructures). Domain experts with advanced knowledge of the infrastructure can achieve this activity. In addition, external dependency identification may require to extract information documents like contracts (e.g. SLAs) or close collaboration with other infrastructures owners.

Base measures identification This activity aims to define relevant measures for each identified critical service extracted from the system components. Such base measures can be for example sensors outputs, intrusion detection systems outputs, etc. Measures, defined by domain experts, are categorized into two categories: boolean data (e.g. on/off, open/closed, etc.) and decimal discrete data (e.g. system load, etc.). As measures are generally realised by using software probes or a verification process, the quality of measurements can greatly influence the accuracy of the measure. This point is addressed by associating an assurance level with each measure; it enables to evaluate the confidence of measures. In order to define such a value, a specific taxonomy is defined (inspired by the Common Criteria scale (ISO 15408-1:2005 2005)) as presented in Table 1. This scale is composed of five assurance levels, not only to have an odd number of assurance levels, so that it is possible to have a medium assurance level (i.e. although only ordinal, the scale is required to have a conceptual middle), but also to avoid defining quite not reachable levels as the two last levels (EAL6 and EAL7) of the Common Criteria evaluation assurance scheme.

	Interpretation	Value
AL1	Rudimentary evidence for parts	1
AL2	Regular informal evidence for selected parts	2
AL3	Frequent informal evidence for selected parts	3
AL4	Continuous informal evidence for significant parts	4
AL5	Continuous semi-formal evidence for the entire system	5

Metrics composition In order to produce unified values for each service measure, measures associated to a same service are assembled in metric form. A metric is a modelling object defined as the process that allows producing a normalized risk level for a CI object, and is based on the measurement of various part/parameters of security functions. Such metrics can be assembled in criterion form, thus each service can be characterized by only three criteria:

- Confidentiality: absence of unauthorized disclosure of information concerning the data transmit-

ted by the critical service;

- Integrity: absence of improper system state alterations concerning the critical service;
- Availability: readiness for correct critical service.

Each measure will be used at least to produce one indicator. In this purpose composition weights in terms of CIA are associated to each measure (W_{μ_i}). This weighting allows to take into account various measures differently in terms of influence. These weights will be used not only during metric risks level determination but also during assurance level determination of the metric. Assurance level of the metric is determined using the following formula (the result is rounded to the nearest integer):

$$AL_m = \frac{\sum_{i=1}^n (AL_{\mu_i} * W_{\mu_i})}{\sum_{i=1}^n (W_{\mu_i})}$$

where m is a metric,

μ is a measure,

AL_{μ_i} is the assurance level of the measure μ_i ,

n is the number of measures composing and

W_{μ_i} is the weight of the measure μ_i .

The definition of weights composing metrics rely for the time being on an experts' assessment. Their quality heavily relies on the competence and motivation of the experts involved and is therefore exposed to subjectivity. In order to limit the subjectivity of the weighting process suitable methods have to be evaluated. One approach we currently consider and that involves less human estimations is based on failure pattern recognition (c.f. Section 6 - Discussion). Similarly, metrics composing a same criterion are weighted (W_{m_i}) in order to reflect the relative importance of each metric.

Interdependency weighting Based on interdependencies identification, domain experts describe each dependency in terms of confidentiality, integrity and availability by assigning respective weights. These weights should represent the local impacts of service degradation on related services.

Thus, if we consider a service (S) requiring electrical power and that it is provided in equal parts by two complementary services ($Se1$ and $Se2$), an easy way is to assign the same dependency weight value to each dependency ($S - Se1$ and $S - Se2$). In most cases this analysis will be considerably more complex.

4.2 Measurement aggregation

Using the model defined during the off-line risk assessment step, this step aims to perform periodic measurement on critical services, in order to estimate the overall risk levels for the three security criteria.

Normalization The normalization process transforms heterogeneous data into normalized data that can be compared and processed. This process uses a five states scale as presented in Table 2. Such a scale is determined for each measure. The determination requires a thorough knowledge of the considered service area (i.e. "below which value is the service considered to be in a critical situation?", "what are the expected variations from the service measurements?", etc.) and therefore is realized by an expert or a group of experts.

Decimal discrete data is normalized as follows: a reference value (expected value, Ev) is defined for each measure. This value is used to compute the measure deviation towards the expected value, expressed as a percentage, using the following formula:

$$\Delta = \left| \frac{\mu - Ev}{Ev} * 100 \right|$$

where μ is the measured value and

Ev is the expected value.

In parallel, four threshold values (T_1, T_2, T_3, T_4) are defined in order to classify values into the following classes: *not reached* (1), *weak* (2), *acceptable* (3), *correct* (4) and *reached* (5). For this purpose, five real intervals of values (supremum included, infimum excluded) are composed using the four threshold values to qualify the evaluated measure. These intervals are described in Table 2.

Table 2: Measures normalisation scale.

Value	Level	Interval
1	Not reached	$[T_4; \infty[$
2	Weak	$[T_3; T_4[$
3	Acceptable	$[T_2; T_3[$
4	Correct	$[T_1; T_2[$
5	Reached	$[0; T_1[$

In case of boolean data, normalization is more trivial, as a data is either *not reached* (1) or *reached* (5).

Metrics risk level aggregation This normalization enables the definition of measures formulated in a common scale. As defined during the off-line risk assessment, normalized measures will be composed into metrics by aggregation. The retained aggregation formula is straightforward and based on weighted-sum and average and enables to obtain a global reasonable estimate of the metric risk level. Indeed, weighted-sum and average, in contrast to other functions such as min or max, helps to express a central tendency of a data set. The expected value is an integer between the smallest (1) and the highest (5) risk level as defined in Table 3. The following formula is used to determine a single risk level value for a metric, which will be rounded to the nearest integer value:

$$RL(m_x) = (RL_M + 1) - \left(\frac{\sum_{i=1}^n (NV(\mu_i) * W_{\mu_i})}{\sum_{i=1}^n (W_{\mu_i})} \right)$$

where m_x is a metric,

RL_M is the maximum risk level,

n is the number of measures for the metric,

$NV(x)$ is the normalized value of x ,

μ is a measure and

W_{μ_i} is the weight of the measure μ_i .

In order to express the risk level, the scale presented in Table 3 has been defined:

Table 3: Risk levels scale

Risk level	Interpretation	Value
RL1	Small	1
RL2	Medium	2
RL3	Strong	3
RL4	Very strong	4
RL5	Unacceptable	5

Aggregation After having determined the risk level of each metric, the various metrics can be aggregated into criterion. Metrics composing a criterion have a specific weight (W_{m_i}) given by domain experts, that specified the importance of each metric in the criterion building. Thus, the adopted aggregation method is a weighted mean using these weights. Criterion risk level will be computed using the following formula:

$$RL(C) = \frac{\sum_{i=1}^n (RL(m_i) * W_{m_i})}{\sum_{i=1}^n (W_{m_i})}$$

where C is a criterion,

m is a metric,

$RL(m_i)$ is the risk level for the metric m_i ,

W_{m_i} is the weight of the metric m_i and

n is the number of metrics for the criterion.

Similarly to criteria risk levels computation, criteria assurance level can be determined, using the following formula:

$$AL(C) = \frac{\sum_{i=1}^n (AL_{m_i} * W_{m_i})}{\sum_{i=1}^n (W_{m_i})}$$

where C is a criterion,

m is a metric,

AL_{m_i} is the assurance level for the metric m_i ,

W_{m_i} is the weight of the metric m_i and

n is the number of metrics for the criterion.

In order to obtain an integer value, this two previous computation results are rounded to the nearest integer value.

4.3 On-line risk monitoring

Using the weighted interdependency functional model, each CI service will send normalized criteria risk levels coupled with respective computed assurance levels. A service that receives a couple of criteria risk and assurance levels can use them to compute a risk linked to its dependencies. We assume that a service $S1_B$ receives from the service $S2_A$ the following information:

Table 4: Data received by $S1_B$ from $S2_A$

Data received	
Confidentiality	$\langle RL_C(S2_A), AL_C(S2_A) \rangle$
Integrity	$\langle RL_I(S2_A), AL_I(S2_A) \rangle$
Availability	$\langle RL_A(S2_A), AL_A(S2_A) \rangle$

Using weightings defined for the dependency, $S1_B$ is able to define dependency risks levels, which will be used to complete it's own risk levels computation.

Table 5: Consolidated data from $S1_B$ point of view

	Weight	Risk level	Dependency risk level
C	W_C	$RL_C(S2_A)$	$RL_C(S2_A) * W_C$
I	W_I	$RL_I(S2_A)$	$RL_I(S2_A) * W_I$
A	W_A	$RL_A(S2_A)$	$RL_A(S2_A) * W_C$

The global risk level for the service will be updated using the computed dependency risk level; the corresponding assurance level will be represented as an additional information to the computed risk level, for example by using a specific colour scheme to visualise risk (e.g. dark red for high risk with high confidence and light red for high risk with low confidence).

In order to obtain a global view on risks regarding a service, an aggregation of the criteria risk level is possible, using weighted mean. Identically, the whole CI is able to determine a risk level for all its services by using the aggregation process.

5 CASE STUDY

In order to show the feasibility of the methodology it is applied to a reference scenario in this section. The reference scenario is composed of a high level representation of a telecommunication provider (Telco CI) which presents interdependencies with an energy provider (Energy CI). This scenario should not be seen as a realistic representation of real-world infrastructure, but rather as an example to validate the risk-based methodology. A more complex and realistic representation is not possible due to the space constraints.

The off-line risk analysis of the Telco CI has identified the critical services and interdependencies shown in Figure 3. In addition, Figure 4 shows that each service is composed of components needed to provide the service.

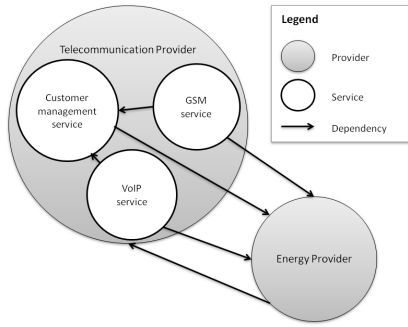


Figure 3: Interdependencies between services and providers

5.1 Telecommunication provider

As shown in Figure 4, the Telco CI provides a VoIP (voice over IP) service, a GSM (global system for mobile communications) service and a customer management service. The customer management system is used to provide information about the customers to the VoIP service and the GSM service (e.g. data authentication). It is assumed that the VoIP service and the GSM service would not be able to provide the service without the data provided by the customer management service. Similar to the Telco provider, a risk analysis would have identified critical services in the Energy provider (e.g. power generation, power distribution...). For simplicity reasons, we did not detail the Energy provider and provide only the model of the Telco provider.

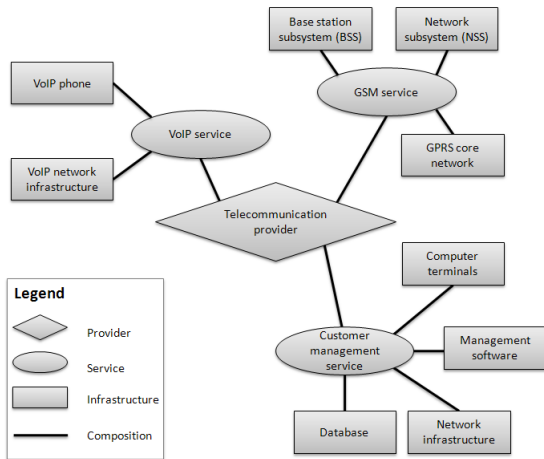


Figure 4: Simplified structure of the telecommunication provider

5.2 Interdependencies

Figure 3 presents the internal service interdependencies of the Telco CI, as well as those between the Telco and Energy CIs. The VoIP and the GSM services depend on the customer management service. Furthermore all Telco CI services depend on the energy delivered by Energy CI. It exists also an inter-

dependency between the Energy CI and the services of the Telco CI. The Energy CI's owner will need to receive the local status of the Telco CI in order to incorporate this dependency in the computation of the status.

5.3 Base measures

The first step of the methodology (off-line risk assessment) applied to the aforementioned infrastructure could produce for the GSM service the base measures detailed in Table 6.

Base measure	Weights $\langle C, I, A \rangle$	AL
Network coverage (BSS)	$\langle 0.0, 0.2, 0.5 \rangle$	AL3
Component failure (BSS)	$\langle 0.0, 0.6, 0.0 \rangle$	AL4
HLR integrity (NSS)	$\langle 0.0, 0.6, 0.0 \rangle$	AL4
HLR confidentiality (NSS)	$\langle 0.4, 0.0, 0.0 \rangle$	AL4
Bandwidth (GPRS)	$\langle 0.0, 0.1, 0.6 \rangle$	AL3

For each base measure, its normalization scale is defined. The following example illustrates the normalization process considering the base measure Network coverage (BSS). We consider that the “normal” level is full coverage (100%), in parallel we define the following threshold values: $T_1 = 1\%$, $T_2 = 3\%$, $T_3 = 6\%$ and $T_4 = 10\%$. This means that a measure will be considered as “normal” if its deviation from the reference value (Ev) does not exceed 1%. Table 7 shows the various values for qualifying BSS network coverage measures, while Table 8 shows the corresponding normalized values using the normalization scale above.

Table 7: BSS network coverage normalization scale.

Value	Level	Interval
1	Not reached	$[10\%; \infty[$
2	Weak	$[6\%; 10\%[$
3	Acceptable	$[3\%; 6\%[$
4	Correct	$[1\%; 3\%[$
5	Reached	$[0\%; 1\%[$

In parallel, domain experts qualify each base measure in terms of weights used during aggregation and an assurance level used to introduce a notion of confidence in the measurement. Examples of such weights and assurance levels are presented in Table 6. These base measures are then joined into metrics; afterwards metrics concerning a same criterion are assembled in criterion to produce at most three indicators per service (CIA). Table 9 presents the aggregation results for the GSM service.

Table 8: BSS network coverage normalized values.

Measure	Δ	Normalized value
0%	100%	1
40%	60%	1
80%	20%	1
90%	10%	2
93%	7%	3
96%	4%	4
100%	0%	5

Table 9: GSM service aggregation results

	Metric	Weight	Measure
C	$m_C(NSS)$	0.8	HLR confidentiality
I	$m_I(BSS)$	0.2	Network coverage
			Component failure
	$m_I(NSS)$	0.5	HLR integrity
	$m_I(GPRS)$	0.5	Bandwidth
A	$m_A(BSS)$	0.7	Network coverage
	$m_A(GPRS)$	0.4	Bandwidth

The aggregation mechanism can be illustrated with the following example; let's consider that the base measure *Network coverage* and *Bandwidth* produce respectively the following normalized values 2 and 3. The corresponding metrics are computed $m_A(BSS)$ will be equal to 4 ($6 - ((2 * 0.5) / 0.5)$) and $m_A(GPRS)$ will be equal to 3 ($6 - ((3 * 0.6) / 0.6)$). Given the weights defined for criterion composition, the risk level on availability for the GSM service will be equal to 3 ($((4 * 0.7) + (3 * 0.4)) / (0.7 + 0.4)$) with an assurance of AL3.

Once this framework is defined, the Telco CI's owner is able to periodically compute risk levels associated to all its services. These risk levels will be provided to dependent CIs. In order to illustrate the methodology, the following scenario is applied to the Telco CI: as the Energy CI is a customer of the Telco CI, a malicious user who compromised data in the customer management service can possibly compromise the confidentiality and the integrity of the Energy Telco. Such an attack on the CMS will be reflected by a high risk level in terms of confidentiality and integrity for the CMS. This high risk level will be integrated by the Energy CI in the computation of its own risk level. Thus the Energy CI's owner is able to make the right decisions necessary to address this growing risk.

6 DISCUSSION

One question that could be asked is why we choose to focus only on three parameters to capture the state of infrastructure services. The idea is to abstract services to a small set of common parameters that a variety of services will have in common and the security parameters of a system seem to be a well suited. These three parameters are widely used for evaluation of systems

security, as for example (ISO/IEC 27001:2005 2005) considers the use of C,I,A for establishing an Information Security Management System sufficient as they perfectly reflect the overall state of security. Still, the question remains if C,I,A will be sufficient to adequately capture the state of an infrastructure or a service, but we reckon that the current development of a support tool and discussions with domain experts will help us to answer this question. If necessary, the model is easily extensible to include other parameters.

Another question that might be asked is if service providers will be willing to share risk data with other interdependent providers in order to allow monitoring of the services. So far, our methodology only enables risk data sharing between direct neighbours (only a direct dependency will share risk data). The only information that has to be shared is information about the offered service (e.g. my infrastructure provides energy) and the related C,I,A parameters. No confidential information about the infrastructure itself and no direct information about the state of interdependent services has to be shared. We think this is a major advantage of our approach, but we do not imagine that service providers will be willing to share this information without supporting measures like contracts, SLAs or policies. Furthermore, it is not clear yet if the approach of enabling only direct neighbours to share information will be sufficient in a large scale scenario where cascading failures and indirect interdependencies are an issue.

On the algorithmic side of our approach one might ask if the weighted sum is a suitable approach to transform real world measurements into abstract risk related parameters. We think it is a simple, straightforward implementation that unfortunately highly depends on the quality of the measurements and the quality of the weights (expert knowledge). A well performed off-line risk assessment will provide highly accurate risk data, but a poorly performed risk assessment won't. As an advantage, a change in the state of the infrastructure will be immediately reflected in the risk parameters. To have a qualitative assessment of the performance of our approach we plan to implement another method based on intelligent algorithms to be able to compare and analyse two different approaches.

7 SUMMARY AND FUTURE WORK

In this paper a methodology to enable on-line monitoring of critical infrastructures is presented. The approach is based on reducing the complexity of an infrastructure by abstracting it to a set of risk related parameters. The advantage of this methodology compared to existing approaches is that it allows to compare the state of different critical infrastructures, since the actual complexity and diversity of the infrastruc-

tures is hidden behind a common set of abstract parameters. Furthermore, risk information sharing between interdependent critical infrastructures is facilitated since only a few abstract parameters capturing the security state of an infrastructure have to be exchanged. Compared to other critical infrastructure modelling approaches, our approach does not only capture the availability of an infrastructure, but also other risk related information.

Current and future work will focus on the enhancement of the approach. Deeper work will also be conducted to enhance weights definition on the functional model, for example to transform static into dynamic weights to make the model more independent from expert knowledge. After an initial definition of the base measures and interdependency weights for C,I,A in the off-line risk assessment step, this weights can be adapted during the on-line monitoring phase after receiving feedback from the model.

8 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 approach described here.

REFERENCES

Adar, E. and A. Wuchner (2005). Risk management for critical infrastructure protection (cip) challenges, best practices & tools. In *IWCIP '05: Proceedings of the First IEEE International Workshop on Critical Infrastructure Protection*, Washington, DC, USA, pp. 90–100. IEEE Computer Society.

Brunner, E. M. and M. Suter (2009, September). *International CIIP Handbook 2008/2009*, Volume 4. Center for Security Studies, ETH Zurich.

Chiaradonna, S., P. Lollini, and F. Di Giandomenico (2007, June). On a modeling framework for the analysis of interdependencies in electric power systems. In *Dependable Systems and Networks, 2007. DSN '07. 37th Annual IEEE/IFIP International Conference on*, pp. 185–195.

CRUTIAL (2009). Critical utility infrastructural resilience. <http://crutial.cesiricerca.it>.

ENISA (2009). Good practice guide network security information exchanges. Technical report, ENISA - European Network and Information Security Agency.

Haslum, K. and A. Arnes (2006, Nov.). Multisensor real-time risk assessment using continuous-time hidden markov models. In *Computational Intelligence and Security, 2006 International Conference*

on, Volume 2, pp. 1536–1540.

IRRIIS (2009). Integrated risk reduction of information-based infrastructure systems. <http://www.irriis.org/>.

ISO 15408-1:2005 (2005). *Part 1: Introduction and general model – Information technology – Security techniques – Evaluation criteria for IT security*. ISO, Geneva, Switzerland.

ISO/IEC 27001:2005 (2005). *Information technology – Security techniques – Information security management systems – Requirements*. ISO, Geneva, Switzerland.

Laprie, J., K. Kanoun, and M. Kaaniche (2007). Modelling interdependencies between the electricity and information infrastructures. *Lecture Notes in Computer Science 4680*, 54–67.

Min, H., W. Beyeler, T. Brown, Y. Son, and A. Jones (2007). Toward modeling and simulation of critical national infrastructure interdependencies. *IIE Transactions 39(1)*, 57–71.

Panzieri, S., R. Setola, and G. Ulivi (2005). An approach to model complex interdependent infrastructures. In *Proceedings of the 16th IFAC World Congress*. IEEE Computer Society.

Permann, M. (2007, May). Toward developing genetic algorithms to aid in critical infrastructure modeling. In *Technologies for Homeland Security, 2007 IEEE Conference on*, pp. 192–197.

Rinaldi, S. and S. M. (2004). Modeling and simulating critical infrastructures and their interdependencies. In *HICSS '04: Proceedings of the Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS'04) - Track 2*, Washington, DC, USA, pp. 20054.1. IEEE Computer Society.

Rinaldi, S., J. Peerenboom, and T. Kelly (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine 21*, 11–25.

Sokolowski, J., C. Turnitsa, and S. Diallo (2008). A conceptual modeling method for critical infrastructure modeling. Volume 0, Los Alamitos, CA, USA, pp. 203–211. IEEE Computer Society.

Svendsen, N. and S. Wolthusen (2007). Graph Models of Critical Infrastructure Interdependencies. *4543*, 208–211.

Tan, X., Y. Zhang, X. Cui, and H. Xi (2008, Dec.). 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*, pp. 490–493.