

Risk-Based Methodology for Real-Time Security Monitoring of Interdependent Services in Critical Infrastructures

Jocelyn Aubert, Thomas Schaberreiter, Christophe Incoul, Djamel Khadraoui, Benjamin Gâteau
Public Research Centre Henri Tudor
Centre for IT Innovation (CITI)
29, avenue John F. Kennedy, L-1855 Luxembourg, Luxembourg
{firstname.lastname}@tudor.lu

Abstract—In today’s world, where most of the critical infrastructures (CI) 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. This allows each CI owner to monitor, react and adopt the best behaviour corresponding to the security status of its different services.

Keywords—Critical Infrastructure; CI Interdependency; Security; Monitoring; Risk Management

I. INTRODUCTION

A critical infrastructure (CI) is defined by the European Commission as “those assets or parts thereof which are essential for the maintenance of critical societal functions, including the supply chain, health, safety, security, economic or social well-being of people. Such systems can be found, for example, in sectors like Energy, Nuclear Industry, Information, Communication Technologies” [1].

The infrastructure of these systems is usually composed of systems that depend on each other. Rinaldi and al. [2] 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”. A malfunction or an attack on one part of the system can lead to failure or violation of information security in another part of the infrastructure or to an other dependent infrastructure.

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 cannot be shared between providers for confidentiality reasons. The idea of the approach presented in this paper is to allow a close to reality representation of the security properties of interdependent systems. Using security properties to abstract the physical

implementation will allow to address a wider range of systems since the security objectives are the same for all systems. The security properties of an interdependent system are defined by the attributes Confidentiality, Integrity and Availability (CIA). One of the main advantages of this approach is that the exchange of data between the CIs is limited to the status of the security properties related to shared services. Confidential information about the CI (infrastructure, tools, equipment) are not exchanged. Our methodology, as illustrated in Figure 1, is composed of three steps: the security model step, the measurement and aggregation step and the monitoring step. Each one is detailed in the following sections.



Figure 1. Steps of the risk-based methodology

The paper is organized as follows. In section II, a summary of related work concerning different modelling approaches is briefly detailed. In section III, the security model is explained in detail. Finally, section IV draws the conclusions and gives an outlook on future works.

II. RELATED WORK

Critical infrastructures interdependencies are complex and not easy to understand. [2] provides an excellent overview on the dimensions in which interdependencies can occur. In [3] critical infrastructures and their interdependencies are analysed and different suitable modelling techniques are discussed.

The IRRIS project [4] 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. A agent-based simulator has been developed to understand CIs and interdependencies.

The CRUTIAL project [5] 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, [6] aims at modelling electric power systems by separating the infrastructure and its control systems. [7] is 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 in [8] to represent an abstract, simplified view of CIs. [9] utilizes the complex adaptive systems (CAS) approach. The model is derived by modelling the mutually dependent sub-systems of the infrastructure. [10] uses genetic algorithms to model and simulate critical infrastructures in the context of disaster protection and recovery. [11] aims to model critical infrastructures and interdependencies based on system dynamics, functional modelling and non-linear optimization and takes physical as well as economic infrastructures into account. In [12], [13] a graph based model to address critical infrastructures interdependencies is presented.

[14] discusses challenges in critical infrastructure risk management and outlines methods as well as best practice guidelines to address risk management in critical infrastructures. In [15] 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 [16] continuous-time hidden Markov models are used for real-time risk calculation and estimation.

The current work on critical infrastructure modelling concentrates on determining system failures in order to deal with the consequences of failure. We think that our security related model presents a more complete view on critical infrastructures where system failure is only one aspect of the model, the Availability. Furthermore, current modelling approaches aim at providing a close to reality representation of critical infrastructures. This has some drawbacks, especially when information sharing between independent critical infrastructure providers is an issue. We think that the abstraction to security related properties provides an advantage in this area since no information related to the actual infrastructures is shared in our model, but only abstracted security related values.

III. METHODOLOGY

The three steps of the methodology illustrated in Figure 1 are presented in the following sections.

A. Step 1: Security model

Our approach, illustrated in Figure 2 aims to define a generic level of risks and assurance of the different critical services that will be exchanged among interdependent CIs. The sources of information are:

- Functional model, that will define and balance in terms of importance the relations between each critical service.
- The result of risk analysis made on each CI. Such an analysis aims to identify the main critical services of each infrastructure to be monitored.

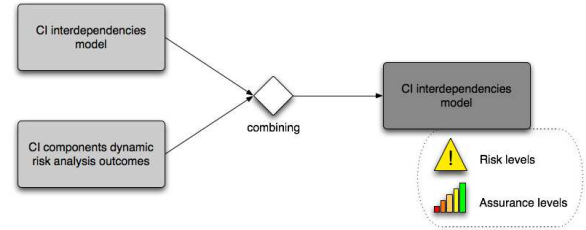


Figure 2. Security modelling approach

The reasoning based on the security model is only possible if all the CIs share a common representation of assurance and risk levels. For this, we defined a generic scale for the assurance level (i.e.: based on the ISO/IEC 15408 levels [17]) and a generic risk level scale.

We describe a metric as 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 parts/parameters of security functions. As shown in Figure 3, a metric is linked to one and only one CI service while one CI service can be linked to several metrics. Depending on the measurements being performed, metrics can be classified into categories.

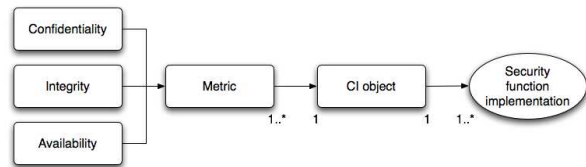


Figure 3. Metric decomposition

Considering the security measures performed on each critical service, we propose to classify metrics based on CIA indicators. Within the security model, these components have the following definition:

- Confidentiality: absence of unauthorized disclosure of information concerning the data transmitted by the critical service;
- Integrity: absence of improper system state alterations concerning the critical service;
- Availability: readiness for correct critical service.

These three indicators will characterize each critical service. The information transmitted from each critical service

to the other CI will be composed of the computation of the level of assurance of each indicator and the corresponding risk level calculated. The approach is explained in the following sections.

1) *Interdependencies mapping*: A mapping between the functional model and risk information will drive the security modelling. The functional model, illustrated in Figure 4 introduces dependencies between services of each CI.

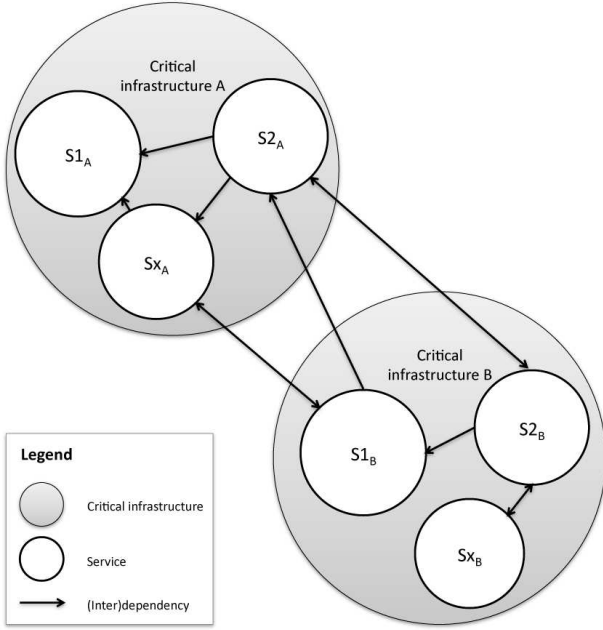


Figure 4. Interdependency functional model

This first model is extended with the introduction of dependencies weights attached on CIA properties. These weights are estimated by experts using a risk management approach. As defined in [18], a risk management process includes a step during which the assets are identified and studied. This step enables to study and quantify dependencies on the services. Thus, if we consider a service (S) requiring electrical power and that it is provided by two complementary services ($Se1$ and $Se2$), then an easy way is to assign a dependency weight value of 0.5 to each dependency ($S-Se1$ and $S-Se2$).

Interdependency links are divided into dependency links, in order to determine the dependency degree via appropriate weight between the producer (*target*) and the beneficiary (*source*). The extended model is presented in Figure 5.

In order to ensure Confidentiality on sensitive data, CIs do not share models. Only direct dependent CIs share a common model; each CI uses its own view to specify its own weights on inner and external dependencies.

2) *Measurement elaboration*: Once the weighted model is defined, the measures for each service are fixed. These

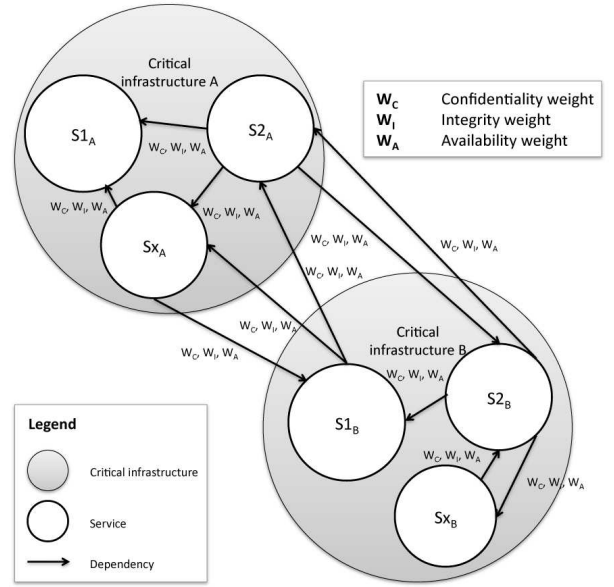


Figure 5. Weighted interdependency functional model

measures, called base measures, are categorized into two categories:

- Boolean data (e.g. on/off, open/closed, ...)
- Decimal discrete data (e.g. functioning percentage, ...)

B. Step 2: Measurement and aggregation

1) *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 I. Such scale is determined for each service. The determination requires a thorough knowledge of the considered service area (i.e. “below which value does the service can be considered as in critical situation?”, “what are the expected variations of the service value?”, etc.) and therefore is realized by an expert or a group of experts.

Decimal discrete data are normalized as follows. A reference value (expected value) 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:

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

where: μ : the measured value,
 Ev : the expected value.

In parallel, a tolerance threshold value for the deviation (T) is fixed. It enables to classify values into these various 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 computed

to position the distance to the tolerance threshold of the evaluated measure. These intervals are described in Table I. In case of boolean data, normalization is more trivial, as a data is either *not reached* (1) or *reached* (5).

Table I
MEASURES NORMALISATION SCALE

Level number	Description	Value included in
1	Not reached	$[4T; \infty[$
2	Weak	$[3T; 4T[$
3	Acceptable	$[2T; 3T[$
4	Correct	$[T; 2T[$
5	Reached	$[0; T[$

Figure 6 illustrates the normalization scale definition.

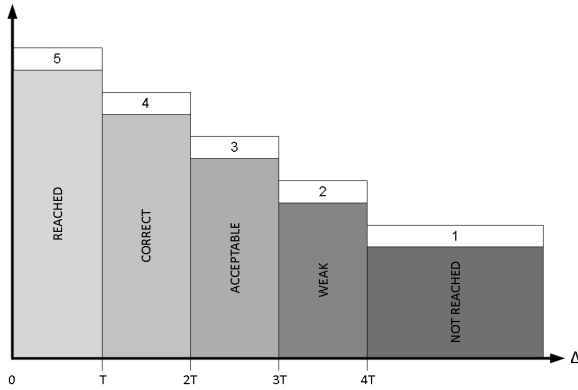


Figure 6. Normalisation scale definition

The following example illustrates the normalization process. Let's define a measure concerning the output voltage level of an electrical transformer. We consider that the "normal" level is about 230V and the tolerance threshold is set to 3%. This means that a measure is considered as "normal" if its deviation from the reference value does not exceed 3%. Table II shows the various values for qualifying output voltage level measures.

Table II
ELECTRICAL TRANSFORMER OUTPUT VOLTAGE LEVEL
NORMALIZATION SCALE

Levels	Values	Intervals
Not reached	1	$[12\%; \infty[$
Weak	2	$[9\%; 12\%[$
Acceptable	3	$[6\%; 9\%[$
Correct	4	$[3\%; 6\%[$
Reached	5	$[0\%; 3\%[$

Table III shows the corresponding normalized values of various measures using the normalization scale above.

2) *Metrics risk levels aggregation*: This normalization enables the definition of measures formulated in a common

Table III
ELECTRICAL TRANSFORMER OUTPUT VOLTAGE LEVEL NORMALIZED
VALUES

Measures	Δ	Normalized value
0V	100%	1
200V	13.04%	1
205V	10.87%	2
210V	8.70%	3
220V	4.35%	4
228V	0.87%	5
230V	0.00%	5
250V	8.70%	3
300V	30.43%	1
600V	160.87%	1

scale. The retained aggregation formula is straightforward and based on weighted-sum and average that 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 IV. The following formula is used to determine a single risk level value for a metric, which will be rounded to the nearest integer value:

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

where: m_x : a metric,

RL_M : the maximum risk level,

n : the number of measures for the metric,

$NV(x)$: the normalized value of x and

μ : a measure result.

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

Table IV
RISK LEVELS SCALE

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

3) *Assurance levels*: The assurance levels, that allow evaluating the confidence of measures, are associated to each metric. In order to define such a value, a specific taxonomy is defined (inspired by the Common Criteria scale [17]) as presented in Table V. 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.

Table V
ASSURANCE LEVELS SCALE

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

An expert or a team of experts is able to determine for each metric an assurance level, by evaluating some properties of the probe that produces the metric. A proposed set of evaluated criteria can be for example: scope, depth, rigour, reliability, timeliness, frequency, stability. Each criteria is individually evaluated, using a proper scale, in order to determine a level. This level will contribute to the global assurance level determination. Such a definition aims to produce reproducible assurance levels (i.e. that can be reproduced or replicated by someone else).

4) *Aggregation*: After having determined the risk level of each metric, the various metrics composing C, I and A can be aggregated into criterion. Metrics composing a criterion have a specific weight (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 this 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 : a criterion,

m : a metric,

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

n : the number of metrics for the criterion and

W_{m_i} : the weight of the metric m_i .

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 : a criterion,

m : a metric,

$AL(m_i)$: the assurance level for the metric m_i ,

n : the number of metrics for the criterion and

W_{m_i} : the weight of the metric m_i .

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

5) *Risk levels consolidation*: Using the framework described above, each CI will be able to determine its normalized criteria risk levels for its services, i.e. the level of risk for each criterion normalized by the determined assurance level. Thus, this risk level includes confidence. Table VI proposes a possible matrix for determining a normalized risk level given risk and assurance levels.

Table VI
NORMALIZED RISK LEVELS MATRIX

		Assurance level				
		AL1	AL2	AL3	AL4	AL5
Risk level	RL1	2	2	1	1	1
	RL2	3	3	2	2	1
	RL3	4	4	3	3	2
	RL4	5	4	4	3	3
	RL5	5	5	5	4	4

The table above enables to consolidate a risk level value, considering an assurance level value. Thus, a risk level of 3 ($RL3$) obtained thanks to metrics with assurance level of 2 ($AL2$) is extended to 4 ($RL4$). Indeed, the fact that the metrics are associated to the low assurance level (*Regular informal evidence for selected parts*) allows for lower confidence in the returned results. By contrast, a risk level of 3 ($RL3$) obtained thanks to metrics with assurance level of 5 ($AL5$) is reduced to 2 ($RL2$). Indeed, the high assurance level (*Continuous semi-formal evidence for the entire system*) brings more confidence in the measurements.

C. Step 3: Monitoring

Using the weighted interdependency functional model, each CI will send normalized criteria risk levels to each service that depends on its services. A service that receives normalized criteria risk levels can compute a risk linked to its dependencies, by using defined weights for each criterion on the dependency. If we consider the example introduced in Figure 5, we assume that the service $S1_B$ receives from the service $S2_A$ the following information:

Table VII
DATA RECEIVED BY $S1_B$ FROM $S2_A$

	Normalized risk level
Confidentiality	$C(S2_A)$
Integrity	$I(S2_A)$
Availability	$A(S2_A)$

Using weightings defined on dependency, $S1_B$ is able to define dependency risks levels, which will be used to complete its own risk levels computation.

The global risk level for the service will be updated using the computed dependency risk level. In order to obtain a global view on risks regarding the 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 aggregation process.

Table VIII
CONSOLIDATED DATA FROM $S1_B$

	Weight on dependency $S1_B - S2_A$	$S2_A$ normalized risk level	Dependency $S1_B - S2_A$ risk level
Confidentiality	W_C	$C(S2_A)$	$\frac{C(S2_A) *}{W_C}$
Integrity	W_I	$I(S2_A)$	$\frac{I(S2_A) *}{W_I}$
Availability	W_A	$A(S2_A)$	$\frac{A(S2_A) *}{W_A}$

IV. CONCLUSION AND FUTURE WORK

This paper introduced a security methodology to represent the security properties in the context of interdependent systems using a generic level of risks and assurance of CI services related to other CIs. This approach hides the complexity of CI and needs only to be interfaced via some attributes while keeping the accuracy of the model close to real world implementation.

Current and future work will focus on the enhancement of the approach. The first step is to finalize the support tool development ; this tool will enable to evaluate the methodology in real conditions of CIs. Deeper work will also be conducted to enhance weights definition on the functional model, a track can be to transform static weights into dynamic ones, to gain flexibility according to the current situation.

V. 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

- [1] "Directive of the council on the identification and designation of european critical infrastructure and the assessment of the need to improve their protection," 2006, com(2006)787.
- [2] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems Magazine*, vol. 21, pp. 11–25, 2001.
- [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, pp. 8 pp.–.
- [4] "Integrated risk reduction of information-based infrastructure systems (irriis) project," online, August 2009, <http://www.irriis.org/>.

- [5] "Critical utility infrastructural resilience (crutial) project," online, August 2009, <http://crutial.cesiricerca.it>.
- [6] S. Chiaradonna, P. Lollini, and F. Di Giandomenico, "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*, June 2007, pp. 185–195.
- [7] J. Laprie, K. Kanoun, and M. Kaaniche, "Modelling interdependencies between the electricity and information infrastructures," *Lecture Notes in Computer Science*, vol. 4680, p. 54, 2007.
- [8] J. Sokolowski, C. D. Turnitsa, and S. Y. Diallo, "A conceptual modeling method for critical infrastructure modeling," in *Annual Simulation Symposium*. IEEE Computer Society, 2008, pp. 203–211.
- [9] S. Panzneri, R. Setola, and G. Ulivi, "An approach to model complex interdependent infrastructures," in *Proceedings of the 16th IFAC World Congress*. IEEE Computer Society, 2005.
- [10] M. Permann, "Toward developing genetic algorithms to aid in critical infrastructure modeling," in *Technologies for Homeland Security, 2007 IEEE Conference on*, May 2007, pp. 192–197.
- [11] H. Min, W. Beyeler, T. Brown, Y. Son, and A. Jones, "Toward modeling and simulation of critical national infrastructure interdependencies," *IIE Transactions*, vol. 39, no. 1, pp. 57–71, 2007.
- [12] N. Svendsen and S. Wolthusen, "Graph Models of Critical Infrastructure Interdependencies," *Lecture Notes in Computer Science*, vol. 4543, p. 208, 2007.
- [13] N. K. Svendsen and S. D. Wolthusen, "Multigraph dependency models for heterogeneous infrastructures," in *Critical Infrastructure Protection, 2007*, pp. 337–350.
- [14] 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*, Nov. 2005, pp. 8 pp.–.
- [15] 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*, Dec. 2008, pp. 490–493.
- [16] 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, Nov. 2006, pp. 1536–1540.
- [17] ISO 15408-1:2005, *Part 1: Introduction and general model – Information technology – Security techniques – Evaluation criteria for IT security*. ISO, Geneva, Switzerland, 2005.
- [18] ISO 31000:2009, *Risk management – Principles and guidelines*. ISO, Geneva, Switzerland, 2009.