APPLICATION OF UML FOR RISK BASED INTERDEPENDENCIES MODELLING IN CRITICAL INFRASTRUCTURES

Anatolijs Zabasta [(a)], Oksana Nikiforova [(b)], Nadezhda Kunicina [(c)]

[(a)] M.oec.ing., Riga Technical University
[(b)] Dr.sc.ing., Riga Technical University
[(c)] Dr.sc.ing., Riga Technical University

[(a)] Anatolijs.zabasta@rtu.lv, [(b)]Oksana.nikiforova@rtu.lvl, [(c)] Nadezda.kunicina@rtu.lv

ABSTRACT
This paper presents a systematic approach for computing metrics and performance indices of interdependent critical infrastructures based on their information content, expert views and risk analysis capabilities. The paper also proposes a risk-based methodology based on generic risks and assurance levels using security properties: availability, confidentiality and integrity. Unified Modelling Language (UML) is proposed in order to define a model for research of critical infrastructures interdependences.

Keywords: Critical infrastructures, modelling, Unified Modelling Language.

1. INTRODUCTION

The safety, security and reliability of critical infrastructures are strongly governed by interaction phenomena. Direct dependency mechanisms are relatively easy to identify, model and analyze in very small portions of critical infrastructures. However, in the case of multiple, large-scale critical infrastructures, direct dependencies between elements form loops and give rise to mutual dependencies, i.e., interdependencies (Setolaa, Porcellinise, and Sforna 2009).

Most researchers represent a generic view at critical infrastructure (hereafter abbreviation CI will be used) and its services interdependencies, which supports overall concept, but not rather practical for real world. Therefore an approach that aware heterogeneous nature of CI interrelating at observed territory (for example city, region) is needed.

Let us assume that each critical infrastructure is composed of services that are provided to customers. Services may be self-contained or may 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 CI. Usually providers have expertise on risks on their own infrastructure, but not on related infrastructures of other providers. Also, since different critical infrastructures are very divergent in nature, risk data gathered from particular infrastructure cannot be easily interpreted by non-domain experts.

In this work is presented an approach that allows monitoring critical infrastructures by considering the state of the services as well as the states of interdependent services. This can be achieved by abstracting data gathered from the CI to a common set of parameters that can be shared with interdependent infrastructures.

We also propose an application of the Unified Modelling Language (UML) in order to define a model for research of CI dependences. The approach taken in applying of the UML has been towards establishing a fair basis for multi-agent modelling and simulation of critical infrastructures. However simulation of critical infrastructures is not a task of this work.

The approach described in this work could help service providers allocated in neighbourhood to make more qualified decisions and to plan risk mitigation actions. Furthermore the ontology proposed in this work can be readily adapted to other cases, taking into account the specifics of each city.

The paper is structured as follows. Authors summarize the related work in the area of CI analysis and describe the difference of their own ideas from the results presented in previous researches. The essence of the approach offered in the paper is expressed in Section 3, which details main steps proposed by authors for monitoring of the state of CI and their interdependent services. An example of dependence of water supply and telecommunication services from the outages happened in power grid is described in Section 4. The main contribution of the research, general results and possible directions for future work are discussed in the conclusion of the paper.

2. RELATED WORKS

Casalichio and Galli (2008) presents a taxonomy that classifies interdependency metrics on the basis of their information content, decision support and risk analysis capabilities, and computational costs. A risk-based methodology that aims to monitor interdependent services based on generic risks and assurance levels

which allows determining the security state of a critical infrastructure service is described in Aubert, Schaberreiter, Incoul and Khadraoui (2010) work.

A MICIE project among other objectives had a task to develop methodologies, algorithms and tools to perform quantitative evaluations of risks and threats deriving from interdependencies existing among CIs (Project MICIE 2010). In Rinaldi (2005) work critical infrastructures and their interdependencies are analyzed and different suitable modelling techniques are discussed. Dependencies can be either to one of the other services identified during the decomposition or to a service provided by another CI (Schaberreiter at al. 2010).

CI security modelling approach was presented in (Aubert at al. 2010; Aubert, Schaberreiter, Incoul, and Khadraoui 2010). The aim of the approach is to transform real-world infrastructure information into common abstract risk related information.

A risk-based methodology that aims to monitor interdependent services based on generic risks and assurance levels using security properties: confidentiality, integrity and availability were demonstrated in Zabasta and Kunicina (2012) work.

Bagheri and Ghorban (2006) proposed an extension to the Unified Modelling Language (UML) in order to define a model for research of CI dependences and a fair basis for multi-agent modelling and simulation of critical infrastructures. UML multi-agent model that captures the static structure and dynamic behaviour of a water distribution networks was presented by Lin, Sedigh, and Miller (2010).

3. METHODOLOGY

The goal of the presented approach is to address the challenge of monitoring of the state of critical infrastructures and their interdependent services. Our hypothesis is, that it is possible to reduce the complexity of a service through abstraction to a common (risk related) set of parameters. This enables to compare critical infrastructures designed to serve very different purposes (energy, telecommunication, water supply, transport and etc.) and composed of very different infrastructure components. It enables also to monitor important system parameters like availability, confidentiality and integrity. The abstraction to a small set of common parameters will encourage service providers to share them with interdependent providers.

The authors used considerably adjusted methodology described by (Aubert, Schaberreiter, Incoul and Khadraoui 2010; Schaberreiter at al. 2010; Zabasta, Kunicina 2012).

The four modelling steps are detailed as follows (see Fig. 1):

- Service components assurance and risk assessment;
- Measurement aggregation;
- Services interdependencies linking
- CI interdependencies modelling using UML

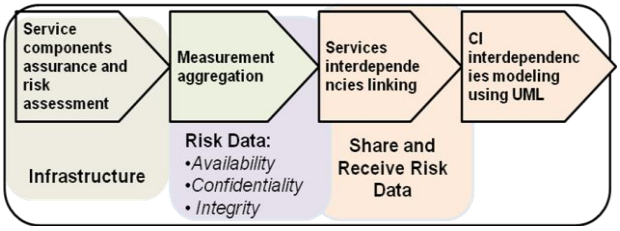

Figure 1: Four Modelling Steps of CI Interdependences

3.1. Service Components Assurance and Risk Assessment

The first step of the offered methodology relies on a risk analysis of the concerned infrastructure to determine services that can be considered as 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 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.

For interdependencies identification the list of identified critical services and components is utilized. This activity aims to identify all the relationships (dependencies or interdependencies) between services. The scope of this identification covers internal dependencies (within the infrastructure) as well as external dependencies (between services of other infrastructures). Domain experts with advanced knowledge of the infrastructure can implement this activity. In addition, external dependency identification may require extracting information documents like contracts or close collaboration with other infrastructures owners.

Base measures identification 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. Taking into account heterogeneous nature of infrastructure components an assurance level is associated with each measure. In order to define a particular level, a specific scale is applied: ISO 15408-1:2009 (2009), ISO/IEC 27001:2005 (2005). This scale is composed of five assurance levels excluding quite not reachable levels as the two last levels (EAL6 and EAL7).

Metrics composition: In order to produce unified values for each service measure, measures associated to a same service are assembled in metric form. 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 transmitted 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 confidentiality, integrity and availability (C, I, A) are associated to each measure (W_{μ_i}). This weighting allows taking into account various measures diversity in terms of influence. These weights will be used during metric risks level and 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):

$$AL_m = [\sum_{i=1}^{n}(AL_{\mu_i} * W_{\mu_i})]/[\sum_{i=1}^{n}(W_{\mu_i})], \quad (1)$$

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 $W_{\mu i}$ is the weight of the measure μ_i.

Interdependency weighting is based on interdependencies identification, thus 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.

3.2. Measurement Aggregation

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 using a five levels scale. The determination requires a thorough knowledge of the considered service area and therefore is realized by an expert or a group of experts. Decimal discrete data is normalized as follows: a reference value is defined for each measure. This value is used to compute the measure deviation towards the expected value, expressed as a percentage. In parallel, threshold values are defined in order to classify values into the following classes: not reached: 1, weak: 2, acceptable: 3, correct: 4 and reached: 5.

Metrics risk level aggregation: At the next step normalized measures will be composed into metrics by aggregation. The aggregation formula is based on weighted-sum and enables to obtain a reasonable estimate of the metric risk level. The expected value is an integer between the smallest "1" and the highest "5" risk level as defined above. The following formula is used to determine a single risk level value for a metric, which will be rounded to the nearest integer value:

$$RL(m_x) = (RL_M + 1) - [\sum_{i=1}^{n}(NV(\mu_i) * W_{\mu_i})]/[\sum_{i=1}^{n}(W_{\mu_i})], \quad (2)$$

where m_x is a metric, RL_M is the maximum risk level, n is the number of measures for the metric, $NV(\mu)$ is the normalized value of μ, μ is a measure and $W_{\mu i}$ is the weight of the measure μ_i.

Criterion aggregation: After having determined the risk level of each metric, the various metrics can be aggregated into criterion. Metrics composing into criterion have a specific weight (W_{mi}) 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:

$$RL(C) = [\sum_{i=1}^{n}(RL(m_i) * W_{m_i})]/[\sum_{i=1}^{n}(W_{m_i})], \quad (3)$$

where C is a criterion, m is a metric, $RL(_{mi})$ is the risk level for the metric m_i, W_{mi} 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.

3.3. Services Interdependencies Linking

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 pair of criteria risk and assurance levels can use them to compute a risk linked to its dependencies. For example we can consider critical infrastructure with services S1, S2 and S3, which require a service S_P from electrical power supplier. Since services of involved CI have been described and evaluated in the same measure system, the dependency weight values should be assigned to each dependency $S_P \rightarrow$S1with W_1, $S_P \rightarrow$ S2 with W_2 and $S_P \rightarrow$S3with W_3. In case of interdependencies of several infrastructures and services this analysis will be considerably more complex.

3.4. Interdependencies modelling using UML

The increasing role of modelling in software system development promotes a methodology, mostly represented by OMG's (Object management Group) solution for system abstraction, modelling, development, and reuse—Model Driven Architecture (MDA) (OMG Model Driven Architecture 2012). The key component of system modelling, which underlies the principles of MDA—Unified Modelling Language (UML)—is a widely accepted standard for modelling and designing different types of systems and is used to define several kinds of diagrams, their elements and notation (OMG Unified Modelling Language 2012).

The MDA models can be formally expressed by any sort of modelling language; however UML has been the dominant choice. The main goal of MDA is to

provide the ability of automated transformations from platform independent models into platform-specific source code. Thus the models in MDA can have two different forms. The first form of models is the models that are independent of the operating platform. These types of models are called Platform Independent Models (PIM).

PIMs are abstract models that do not directly map to a specific environment. In order to perform the PIMs, Platform Specific Models (PSM) should be created. For instance the model of CI interdependencies expressed in UML and created during the study (described in Section IV of the paper) using StarUML tool (StarUML 2012) is platform independent and can be classified as a PIM. However to be able to create a real simulation, an agent based tool should be selected to apply it for model simulation. The PIM then should be transformed to a PSM to make it executable. Thereby the idea of problem domain abstraction from programming details and set of models proposed by MDA is borrowed for the analysis and implementation of risk level assessment for critical infrastructure.

4. WATER SERVICE PROVIDER CASE STUDY

In order to show the feasibility of the methodology a reference scenario is applied in this section, the UML use case diagram is created and the appropriate object interaction expressed in terms of the UML sequence diagram is summarized in the UML class diagram.

4.1. Situation Description

The reference scenario is composed of a high level representation of water utility (Talsi Water), which presents interdependencies with energy provider (Latvenergo CI) and a telecommunication provider (GSM Operator CI). This scenario is demonstrated as an example for validating the risk based methodology. A more complex and realistic representation is not possible due to the lack of the data and this work space constraint.

The risk analysis of Talsi Water CI has identified the internal service interdependencies of Water CI, as well as interdependencies between the Talsi Water CIs, Latvenergo and GSM Operator's CIs (see Fig. 2). Furthermore Fig. 3 shows how each service is composed of components needed to provide the service.

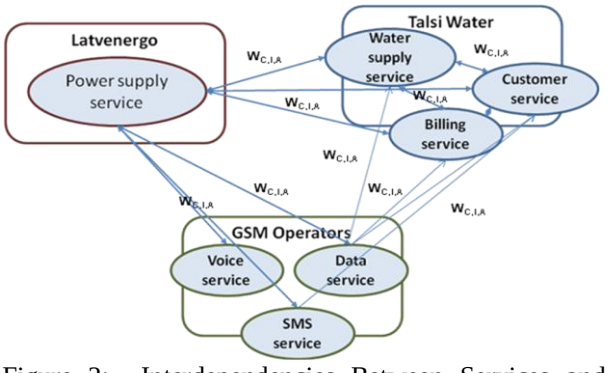

Figure 2: Interdependencies Between Services and Services Providers

As it is shown in Fig. 2, Talsi Water CI provides water supply, billing and customer care services. Water supply services utilize infrastructure components, for example, water supply service is based on water pumps, SCADA for water supply management, water meters and sensors – transmitters, data transmission gateways and data centre equipment (servers, data bases etc.) (Zabasta, Kunicina, Chaiko, and Ribickis, 2011). Data transmission gateway infrastructure relies completely on GPRS service provider. The part of the infrastructure components is shared among services, for example, data bases and servers.

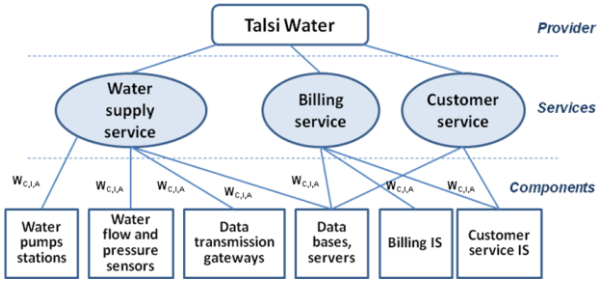

Figure 3: Talsi Water Services Decomposition

To simplify the example, it is assumed that the main infrastructure or GSM operator at reviewed territory consists of the base stations, which enable data traffic and SMS services for water supplier. It is assumed that the data transmission (GPRS) service and the GSM service would not be able to provide the service without power supply services (base station batteries enable back up for a few hours).

4.2. Interdependencies modelling with UML

In order to create the UML model of interdependent CI we apply StarUML, an open source UML tool, licensed under General Public License (GPL).

Use cases. As an example of the UML use case diagram, showed in Fig.4, let us consider the risk level assessment of integrated water supply service, which is influenced by data service of a telecommunication operator and power supply service of Latvenergo.

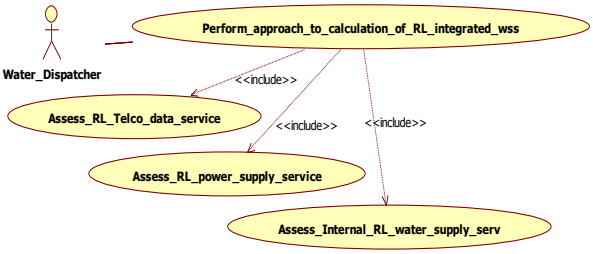

Figure 4: Use Case Diagrams for The Risk Level Assessment

We use the actor symbol to represent the agent that activates the use case, which in our example is a water supply dispatcher, who wants to know the integrated risk level of water supply service.

The relation between the use case "*Perform approach_ to_ calculation_of_RL_integrated_wss*" and other use cases are represented by the relationship's stereotype «include» graphically depicted with a dashed arrowed line beginning at base use case and ending with an arrows pointing to the include use case.

Sequence diagrams. The detailed description of the interdependencies modelled through the use case diagrams is provided by one of the sequence diagrams in Fig. 5, which refines integrated risk level of water supply service. We have decided to use the sequence diagram because it focuses on the participants (agents, infrastructures and services) and links (interactions and interdependencies). Moreover the sequence diagram allows providing a clear description of the object interaction, message ordering, and the synchronous and asynchronous messages.

Furthermore the sequence diagrams describe in the similar way participants, interaction and interdependences in other use cases, but due to the lack of space we do not describe them in this work.

Class diagrams. Fig. 6 shows thirteen classes, where five of them represent water supply service with its services components, five classes represent power supply, one class data transmission services but one class starts and controls services risk level assessment process. The parameters of attributes and operations in each class have been omitted in the interest of figure clarity. One particular class, namely "Metrics", have been created in order to describe parameters of classes' attributes and classes' operations. The class has attributes "value", "weight" and "reference level" that are referred to the service parameters (availability, confidentiality and integrity). Creation of particular class makes sense since unified normalized parameters are applied to divergent CIs.

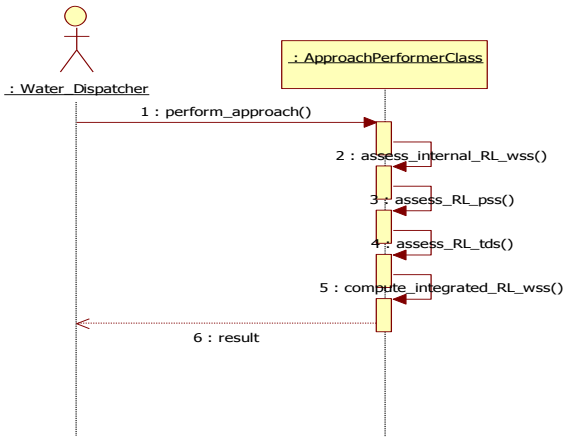

Figure 5: Calculating of Integrated Risk Level of Water Supply Service.

The ontology proposed in Fig. 6 was created in order to study CI interdependencies of the particular city, but can be readily adapted to other cases, taking into account the specifics of each city.

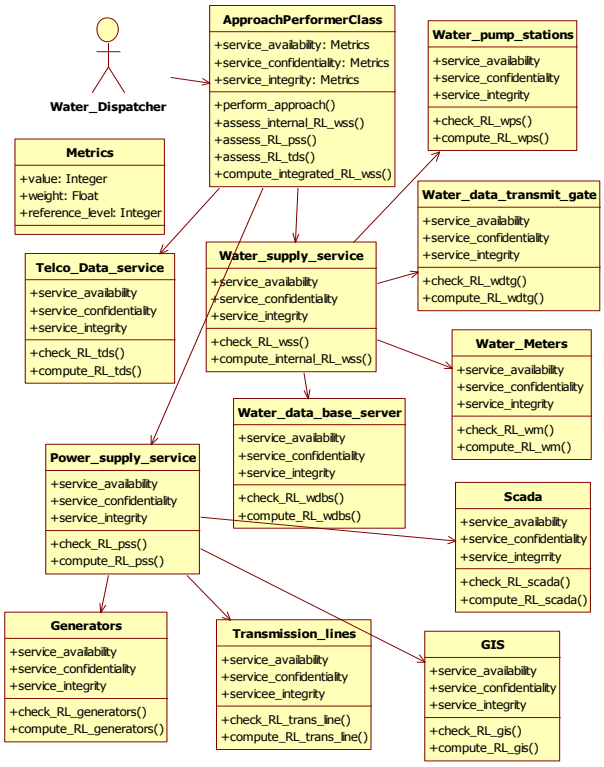

Figure 6: Interdependencies Class Diagram.

5. DISCUSSIONS AND FUTURE WORK

The four modelling steps are described in this work, they are service components assurance and risk assessment, measurement aggregation, services interdependencies linking and CI interdependencies modelling using UML. In this work we proved the hypothesis to abstract and to decompose services to a small set of common parameters; therefore three parameters were chosen to evaluate the state of services of different CI (confidentiality, integrity and availability), which are widely used for evaluation of systems security. The main advantage is that the model is easily extensible for including additional parameters and is ubiquitous for heterogeneous CI.

Another benefit of the CI security model for businesses is the ability to compare different types of infrastructure using common risk related parameters. A common set of parameters makes it easier to interpret the information received from dependent CIs or CI services.

The approach enabling critical information sharing among service providers allocated in neighbourhood looks quite attractive, because it helps to CI owners to make more qualified decisions and to plan risk mitigation actions. Moreover, the question is how to encourage service providers to elaborate, refine and issue critical information to other CI owner.

In this paper authors use the modelling notation offered by UML and the idea of information abstraction in models, defined at different levels of abstraction proposed by the MDA approach. We recognize that the used notational conventions bring about a better

understanding and a clearer picture of the CI internal arrangement and external interdependencies.

An example of dependences of water supply and telecommunication services from the outages happened in power greed is described aiming to study CI interdependencies of the particular city; furthermore the ontology proposed in this work can be readily adapted to other cases, taking into account the specifics of each city.

One of the approach limitations is necessity to involve experts for weights definition; therefore future work should focus on enhancing weights definition on the functional model, transformation static into dynamic weights making the model less dependent from expert knowledge; looking for the methods for on-line monitoring of CI and mutual alerting of the critical levels of interdependent services. Future work also should focus on enhancing universal approach to services decomposition and measures aggregation for heterogeneous CI.

Another limitation is that simulation of critical infrastructures is not a task of this work; therefore to form a complete modelling and simulation cycle, we plan to transform PIM, developed in the research, into platform specific model. The intended PSM will be based on an agent based architecture because we need to get input from distributed systems such power supply systems, telecommunication networks and water distribution networks.

REFERENCES

Aubert, J., Schaberreiter, T., Incoul C. and Khadraoui D., 2010. Real-Time Security Monitoring of Interdependent Services in Critical Infrastructures, *Proceedings of ESREL 2010*, pp.1-8, Rhodes, Greece, September 5-9. 5

Aubert, J.; Schaberreiter, T.; Incoul, C.; Khadraoui, D.; Gateau, B., 2010. Risk-Based Methodology for Real-Time Security Monitoring of Interdependent Services in Critical Infrastructures, ARES '10 International Conference on Availability, Reliability and Security, pp. 262-267, Feb. 15 – 18, 2010, Krakow, Poland. 8

Bagheri E., Ghorbani A., Towards an MDA-Oriented UML Profile for Critical Infrastructure Modelling, *Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services, PST 2006*, pp.1-1212, Oct.30 – Nov. 1, Ontario, Canada. 11

Casalicchio, M. and Galli, E., 2008. Metrics for Quantifying Interdependencies, *Proceedings of Second IFIP WG 11.10 International Conference on Critical Infrastructure Protection*, pp. 1-8, George Mason University, Arlington, VA, USA, March 2008. 2

ISO 15408-1:2009, 2009. Part 1: Introduction and general model, Information technology Security techniques, Evaluation criteria for IT security, pp.1-72, ISO, Geneva, Switzerland. 13

ISO/IEC 27001:2005, 2005. Information technology, Security techniques, Information security management systems – Requirements, pp.1-188, ISO, Geneva, Switzerland 14

Lin J., Sedigh S., and Miller A., 2010. Modelling Cyber-Physical Systems with Semantic Agents, *34th Annual IEEE Computer Software and Applications Conference Workshops (COMPSACW 2010)*, pp.13-18, July 19- 23, Seoul, Korea. 12

OMG Model Driven Architecture, [Online]. Available from: http://www.omg.org/mda [Accessed: March 21, 2012] 15

OMG Unified Modelling Language, [Online]. Available from: http://www.uml.org [Accessed: March. 21 2012]. 16

Refined interdependency metrics and indexes for risk prediction formulation, 2010. Project D3.1.2. *Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures* (MICIE), FP7, STREP, 22/06/2010, pp.1-186. 3

Rinaldi, S.M., 2005. Modelling and simulating critical infrastructures and their interdependencies. *Proceedings of the Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS'04) - Track 2*, pp.1-8, Washington, 4.1. IEEE Computer Society. 6

Setolaa, R., De Porcellinise, S., Sforna M., 2009. Critical infrastructure dependency assessment using the input– output inoperability model, *International Journal of Critical Infrastructure Protection*, 2, pp. 170 – 178. 1

Schaberreiter T., Bonhomme C., Aubert J., Incoul C. and Khadraoui D., 2010. Support tool development for real-time risk prediction in interdependent critical infrastructures service, International *Workshop on Risk and Trust in Extended Enterprises (RTEE'2010*), pp. 1- 8, San Jose, California – USA, November 1-4, 2010. 7

StarUML - The Open Source UML/MDA Platform, [Online]. Available from: http://staruml.sourceforge.net/en/download.php [Accessed: March 21, 2012] 17

Zabasta A., Kunicina N., Chaiko Y., and Ribickis L., 2011, Automatic Meters Reading for Water Distribution Network in Talsi City, *in proceeding of EUROCON 2011*, 27-29 April 2011, pp. 1-6, Lisbon, Portugal. 20

Zabasta A., Kunicina N., 2012. Approach for Monitoring and Measurement of Interdependent Services in Critical Infrastructures, *Proceeding of the 11th International Symposium, Faculty of Power Engendering, Tallinn University of Technology*, pp.51-56, Pärnu, Estonia. 10