Approach for Monitoring and Measurement of Interdependent Services in Critical Infrastructures

Anatolijs Zabasta, Nadezda Kunicina
Riga Technical University
Anatolijs.Zabasta@eudata.lv, Kunicina@latnet.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 that aims to monitor interdependent services based on generic risks and assurance levels using security properties: confidentiality, integrity and availability. Such approach helps to determine the quality of the provided service and allows each CI provider to react and adopt the best behavior corresponding to the security status and assurance level of its different services. A real life example is used to illustrate the computation of the measures and performance indices, and their application to the analysis of critical infrastructure interdependencies.

I. INTRODUCTION

The safety, security and reliability of critical infrastructures are strongly governed by mutual 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 interdependencies. These interdependencies are extremely difficult to understand, and become visible only when the critical infrastructures have been thoroughly studied and modeled [1].

In the literature several definitions of “dependency” and “interdependency” were presented; however one of the most widely accepted is:

Dependency is the capability of an infrastructure to influence the state of other infrastructures. Then infrastructure A depends on infrastructure B when the variation of at least one component of the infrastructure B has the capability to influence (e.g. modify) some states (e.g., behaviors, characteristics, properties, etc.) of the A infrastructure. It is, therefore, a unidirectional relationship.

On the other side the term interdependency represents a bidirectional relationship between two or more infrastructures where the state of each infrastructure is influenced or is correlated to the state of the other. In this paper we limit our attention only on the phenomena strictly related with service and functionality degradation.

In the following an abstract concept of inoperability will be used to define the interdependency indices. The inoperability of an element is the incapacity to perform its intended function. In the following we will indicate generically such metric with the letter $\mu$ and the corresponding level of inoperability with $x$. Specifically, $x_i = 0$ means that the element, with respect to the aspects crystallized by $\mu$ metric, is fully operative, while $x_i = 1$ means that it is completely unable to provide its function.

The definition of interdependency correlates the presence of a dependency among two infrastructures to the fact that a positive variation (an augment) of the inoperability in one infrastructure implies an augment of inoperability into the other [2]:

$$\frac{A \leftarrow B}{\mu^T_{A,i}, \mu^T_{B,j}} \rightarrow \Delta x_A(t) = \phi(t, x^0_A, x^0_B, \Delta x^0_B)$$ (1)

for $t \in [t_0, t_0+T]$, where $x^0_A$ represents the level of inoperability of the infrastructure $A$ measured using the metric $\mu^T_{A,i}$ before the injection of the inoperability; $x^0_B$ is the level of inoperability of the infrastructure measured using the metric $\mu^T_{B,j}$ before the injection of the inoperability. $\Delta x_A$ is the variation in the level of inoperability experienced by the infrastructure $A$ in the correspondence of an augment of the level of inoperability in infrastructure $B$ equal to $\Delta x_B^o$ (the apex “o” represent that this is the initial or injected degradation). Time $t_0$ represents the instant, in which the variation of inoperability is injected into infrastructure $B$ and $T$ is the time horizon assumed to evaluate the effects.

It is noticed that in the left side of expression (1) it is explicitly indicated the metrics $\mu^T_{A,i}, \mu^T_{B,j}$ used, respectively, to measure of the inoperability in infrastructure $A$ and $B$ and it is explicitly expressed the time horizon $T$ adopted for the calculation.

Starting from this definition, it is straightforward to assume the follow index for the dependency relationship: the dependency index is the ratio between the increments of inoperability in the depended infrastructure with respect to those of the source infrastructure. Then index (2) relates to the degree of dependency among two infrastructures to the effect induced on the level of inoperability:

$$\delta^T_{A,B} = \left( \int_{t_0}^{t_0+T} \Delta x_A(\tau)d\tau \right) \div \left( \int_{t_0}^{t_0+T} \Delta x_B(\tau)d\tau \right).$$ (2)

Specifically, the more the effect induced on the dependent infrastructure is larger than those observed in the source infrastructure, the more the first infrastructure depends on second one. Notice that from (2) it is evident that $\delta^T_{A,B}$ depends on a large set of parameters:

$$\delta^T_{A,B} = \delta^T_{A,B}(x^0_A, x^0_B, \Delta x^0_A, \Delta x^0_B, \eta_{A,i}, \eta_{B,j}, t_0, T).$$ (3)

51
In particular the dependency index depends on the specific metrics used to measure the inoperability level, on the time horizon considered and on the amplitude of the injected inoperability further to the “initial” inoperability conditions of the two infrastructures.

We can express previous definitions in terms of dependency of an infrastructure with respect to a component (and vice versa). Infrastructure $A$ depends on the component $q$ when an increment of the level of inoperability of such component $q$ induces an augment of the level of inoperability of infrastructure $A$:

$$\Delta x_A(t) = \phi(x_A^0, x_q^0, \Delta x_q^*) \text{ for } t \in [t_0, t_0+T]. \quad (4)$$

Here $q$ may belong to infrastructure $A$ or to another infrastructure $B$. In this second case, it could be of interest to globally characterize the degree of dependencies of the infrastructure $A$ with respect to all the $n$ components of the infrastructure $B$. This can be done with the following index:

$$\phi(x_A^0, x_q^0, \Delta x_q^*) = \frac{1}{n} \sum_{i=1}^{n} w_i \int_{t_0}^{T} \phi_A(t, x_A^0, x_q^0, \Delta x_q^*) dt$$

$$= \frac{1}{n} \sum_{i=1}^{n} w_i \int_{t_0}^{T} \Delta x_A(t, x_A^0, x_q^0) dt$$

with $w_i \in [0,1]$. \quad (5)

A different approach for CI interdependency is considered in the works [3], [4] where the direct metric, relative duration $R_{ij}$, which measures the cascading effect of an outage.

$$R_{ij} = \frac{T_j}{T_i}$$

is defined as the ratio of the duration $T_j$ of an outage in infrastructure $j$ due to an outage in infrastructure $i$ and the duration $T_i$ of the outage in infrastructure $i$. The computation of a shape metric involves measuring $R_{ij}$ and quantifying the impact on infrastructure $j$. $R_{ij}$ is a function $f(.)$ of the time $t$ and the set of sector-specific metrics $M_j$. This can be done with the following index:

$$R_{ij} = f(t, m^1_j, m^2_j, ..., m^p_j)$$

where $m^k_j \in M_j$. \quad (6)

According to work [4], if $R_{ij} < 1$, the infrastructure $j$ can react on its own to the outage (e.g., reconfigure its services). Otherwise, if $R_{ij} > 1$, the infrastructure $j$ is heavily dependent on the outage and it needs some time to restore its services after the outage ends.

An example of an aggregate measure of a shape metric is the total relative duration $R_j$ of an outage in infrastructure $j$ on a set of infrastructures $I$. Suppose that the power supply outage impacts the communication network and water supply system, and that the communication network outage impacts monitoring and control system of water supplier. The cascading effect begins when all the infrastructures are restored to their normal operating conditions. Then, the total relative duration of an outage in infrastructure $j$ is given by:

$$R_j = \max_{i \in I} (R_{ij}), \text{ where } R_{ij} \text{ is a function of sector specific performance indices of infrastructure } j.$$
designed to serve a very different purpose (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 in [7], [9] and [10].

The three modeling steps are detailed in the following sections:

- Service components assurance and risk assessment;
- Measurement aggregation;
- Services interdependencies linking

A. Service Components Assurance and Risk Assessment

This first step relies on a 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 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.

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 dependencies (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 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 in 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 [10], [11]. 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 (Wm). This weighting allows taking into account various measures differently 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):

$$AL_m = \left\{ \sum_{i=1}^{n} (AL_{\mu_i} \times W_{\mu_i}) \right\} / \left\{ \sum_{i=1}^{n} (W_{\mu_i}) \right\}.$$  (7)

where m is a metric, \(\mu\) is a measure, \(AL_{\mu_i}\) is the assurance level of the measure \(\mu_i\), \(n\) is the number of measures composing and \(W_{\mu_i}\) is the weight of the measure \(\mu_i\).

Risk level of the metric is determined in the similar way using the following formula:

$$RL_m = \left\{ \sum_{i=1}^{n} (RL_{\mu_i} \times W_{\mu_i}) \right\} / \left\{ \sum_{i=1}^{n} (W_{\mu_i}) \right\}.$$  (8)

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.

B. 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 states 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 (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:

$$\Delta = \left\{ (\mu - Ev) / Ev \times 100 \right\}.$$  (9)

where \(\mu\) is the measured value and Ev is the expected value.

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:

\[ RL(m_i) = (RL_{max} + 1) - \left( \sum_{i=1}^{n} \frac{NV(\mu_i) \cdot W_{mi}}{\sum_{i=1}^{n} W_{mi}} \right) \]

where \( m_i \) is a metric, \( RL_{max} \) is the maximum risk level, \( n \) is the number of measures for the metric, \( NV(\mu_i) \) is the normalized value of \( \mu_i \). Thus, the adopted aggregation method is a weighted mean using these weights. Criterion risk level will be computed using the following formula:

\[ RL(C) = \left[ \sum_{i=1}^{n} (RL(m_i) \cdot W_{mi}) / \left( \sum_{i=1}^{n} W_{mi} \right) \right] \]

where \( C \) is a criterion, \( m \) is a metric, \( RL(m_i) \) 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.

Similarly to criteria risk levels computation, criteria assurance level can be determined:

\[ AL(C) = \left[ \sum_{i=1}^{n} (AL(m_i) \cdot W_{mi}) / \left( \sum_{i=1}^{n} W_{mi} \right) \right] \]

where \( C \) is a criterion, \( m \) is a metric, \( AL(m_i) \) is the assurance 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.

### C. 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 couple 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 S4 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 S4 -> S1 with \( W_i \), S4 -> S2 with \( W_2 \) and S4 -> S3 with \( W_3 \). In case of interdependencies of several infrastructures and services this analysis will be considerably more complex.

### IV. TALSI CASE STUDY

#### A. Situation Description

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 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 aiming to validate 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 critical services and interdependencies shown in Fig. 1. In addition, Fig. 2 shows how each service is composed of components needed to provide the service. As shown in Figure 1, Talsi Water CI provides water supply, billing and customer care services. Water supply services utilize infrastructure components, for example, water 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.) [12]. Data transmission gateway infrastructure relies completely on GPRS service provider. Part of the infrastructure components is shared among services, for example, data bases and servers.

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).

For simplicity reasons it is assumed that Latvenergo infrastructure is presented by two electrical power substations, which divide observed territory in two parts (by dash lines) (see Fig. 3). At Fig. 3 circles denote water flow and pressure sensors, but triangles denote water pump stations of Talsi Water.

#### B. Interdependencies Between Services

At Fig. 1 one can see the internal service interdependencies of Talsi Water CI, as well as those between the Talsi Water CIs, Latvenergo and GSM Operator’s CIs. Customer service
and Billing depends on the data provided by Water supply service of Talsi Water. In its turn Water supply service depends on Data service and SMS service of GSM operator and also depends on Power supply service of Latvenergo.

Fig. 2. Talsi Water services decomposition.

C. Measurement Example

Measurement calculation example is made in accordance with methodology described in previous chapter. As an example Service assurance level and Risk level for Water supply service of Talsi Water are selected: \(AL_{WSS}\) and \(RL_{WSS}\).

As the first step of the methodology the base measures are produced for the Water supply service. For this purpose domain experts qualify each base measure in terms of weights used during aggregation. Examples of such weights and base measures are presented in Table II.

Fig. 3. Talsi Water infrastructures components: meters, sensors etc. [13]

<table>
<thead>
<tr>
<th>Water Supply Service Base Measures</th>
<th>Weight</th>
<th>Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>0.1</td>
<td>Water flow and pressure sensors</td>
</tr>
<tr>
<td>I</td>
<td>0.2</td>
<td>Data transmission gateways (GPRS)</td>
</tr>
<tr>
<td>A</td>
<td>0.2</td>
<td>Data bases, servers</td>
</tr>
</tbody>
</table>

The next step is to define a normalization scale for each base measure. It also can be done by domain experts and taking in account service level agreements used by the domain. Table III shows the various values for qualifying Data transmission (GPRS) measures and the corresponding normalized values using the normalization scale. To simplify the example such normalized values are used also for other measurers of the Water supply service.

The base measures (see Tab.4) are then joined into metrics; afterwards metrics concerning a same criterion are assembled in criterion to produce at most three indicators per service (C; I; A). Table IV also presents the aggregation results for the Water supply service.

<table>
<thead>
<tr>
<th>Water Supply Service Base Measures</th>
<th>Weight</th>
<th>Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>0.1</td>
<td>Water flow and pressure sensors</td>
</tr>
<tr>
<td>I</td>
<td>0.2</td>
<td>Data transmission gateways (GPRS)</td>
</tr>
<tr>
<td>A</td>
<td>0.2</td>
<td>Data bases, servers</td>
</tr>
<tr>
<td>C</td>
<td>0.1</td>
<td>Water pumps stations</td>
</tr>
<tr>
<td>I</td>
<td>0.3</td>
<td>Water flow and pressure sensors</td>
</tr>
<tr>
<td>A</td>
<td>0.5</td>
<td>Data transmission gateways (GPRS)</td>
</tr>
</tbody>
</table>

The calculations below are made for service availability (A) metric \(m_A\) of Water supply service. Let us consider that the base measure Water pumps stations, Data transmission gateways (GPRS) and Data bases, servers produce respectively the following normalized values 3, 3 and 5.

The corresponding metrics are computed for risk level according (8):

\[ RL_{m_A}(\text{Water pumps stations}) = ((5+1) - 3*0.5)/0.5\times 3 \]
\[ RL_{m_A}(\text{Data transmission gateways}) = ((5+1) - 3*0.5)/0.5\times 3 \]
\[ RL_{m_A}(\text{Data bases, servers}) = ((5+1) - 5*0.3)/0.3\times 1 \]

The corresponding metrics are computed for service assurance level according (7):

\[ AL_{m_A}(\text{Water pumps stations}) = 3*0.5/0.5\times 3 \]
\[ AL_{m_A}(\text{Data transmission gateways}) = 3*0.5/0.5\times 3 \]
\[ AL_{m_A}(\text{Data bases, servers}) = 5*0.3/0.3\times 5 \]

Taken in account the weights defined for criterion composition (see Tab.4), the risk level on availability for the Water supply service will be equal to:

\[ RL_{m_A} = ((3*0.5) + (3*0.5) + 1*0.3) / (0.5 + 0.5 + 0.3) = 2.53 \] with an assurance level AL3.

Accordingly the service assurance level on availability for the Water supply service will be equal to:

\[ AL_{m_A} = ((3*0.5) + (3*0.5) + 5*0.3) / (0.5 + 0.5 + 0.3) = 3.5 \] with an assurance level AL4. Furthermore other water supply service metrics could be calculated related to risk level and service assurance level: \(RL_{m_C}; RL_{m_I}; AL_{m_C}; AL_{m_I}\).
When Talsi Water services assurance and risks levels are calculated, it is possible to compute a risk and assurance level linked to its dependencies. Therefore using weightings defined for the dependency, the risk level producing by Latvenergo and GSM Operator will be integrated by the Talsi Water in the computation of its own risk level.

Interdependences between involved CI could be also evaluated by outage propagation metric $R_{ij}$. Let’s assume that one of electric power substation is failed, therefore GSM and water supplier infrastructure will be caused. Assuming that GSM base stations are able to operate a few hours due to batteries, therefore all three Talsi Water services will be degraded partly, but will be restored quickly after power supply restoration, because measurement data from sensors will be preserved by equipment using batteries; therefore $R_{ij} < 1$. In case of long power outage (one day and more) reserved batteries will not be able to ensure power supply, thus it will cause loss of the data necessary for water supply, billing and customer services. Much more time will be needed to restore services after the end of power supply outage, therefore $R_{ij} > 1$. So severity of power supply impact on dependant services of Talsi Water is strictly related to the time of power supply outages.

V. DISCUSSIONS AND FUTURE WORK

The three modeling steps were described in this work, which consist of service components assurance and risk assessment, measurement aggregation and services interdependencies linking. In this work we employed an idea 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 (confidence, 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 ubiquitious for heterogeneous CI.

The approach enabling critical information sharing among service providers allocated in neighborhood looks very 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.

An example, involving simulations of outage propagation scenarios, demonstrated the value of the approach and the metrics for analyzing critical infrastructure interdependencies. Two scenarios: “short time” and “longer time”, demonstrated the severity of dependency of Talsi Water services from the outage happened in energy provider (Latvenergo CI) and a telecommunication provider (GSM Operator CI).

Future work should focus on the enhancement of the approach in following areas:

- Enhancing universal approach to services decomposition and measures aggregation for heterogeneous CI,
- 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.

REFERENCES