Theoretical and Applied Informatics
Vol. 28 (2016), no. 1&2, pp. 13–36
DOI: 10.20904/281-2013

Critical infrastructures risk management: Case study*

Andrzej Białas†

Institute of Innovative Technologies EMAG
ul. Leopolda 31, Katowice, Poland

Abstract The paper concerns a risk assessment and management methodology in critical infrastructures. The aim of the paper is to present researches on risk management within the experimentation tool based on the OSCAD software. The researches are focused on interdependent infrastructures where the specific phenomena, like escalating and cascading effects, may occur. The objective of the researches is to acquire knowledge about risk issues within interdependent infrastructures, to assess the usefulness of the OSCAD-based risk manager in this application domain, and to identify directions for further R&D works. The paper contains a short introduction to risk management in critical infrastructures, presents the state of the art, and the context, plan and scenarios of the performed validation experiments. Next, step by step, the validation is performed. It encompasses two collaborating infrastructures (railway, energy). It is shown how a hazardous event impacts the given infrastructure (primary and secondary effects) and the neighbouring infrastructure. In the conclusions the experiments are summarized, the OSCAD software assessed and directions of the future works identified.

Keywords critical infrastructure; risk assessment; risk management; interdependencies; tools for risk management

Received 18 JAN 2016 **Revised** 23 MAY 2016 **Accepted** 24 NOV 2016

1 Introduction

The paper presents a case study related to risk management in critical infrastructures. The risk management encompasses a continuous management process related to risk. These are the main objectives of this process:

- to identify the source of risk, analyse the cause and nature of risk, and assess potential hazards and their consequences; hazards may impact the system and its assets or processes (activities); this is called risk assessment and can be asset- or process-oriented,

*The paper is an expanded and updated version of the paper *Research on critical infrastructures risk management* [1], presented at the 10th International Conference *Internet in the information Society 2015*.

†E-mail: andrzej.bialas@ibemag.pl

- to identify and introduce risk control measures (countermeasures) to eliminate or reduce potential harms to people, environment, or other assets.

Risk management is broadly applied in many domains of application [2], however risk management in critical infrastructures is a more complex issue and still remains a challenge.

Critical infrastructures (CIs) consist of large scale infrastructures which, when degraded, disrupted or destroyed, are likely to have a serious impact on health, safety, security or well-being of the society or effective functioning of governments and/or economies.

CI is a very complex socio-technical system, sometimes called a system of systems. The system of systems (SoS) is composed of multiple, heterogeneous, distributed, occasionally independently operating systems which are embedded in networks at multiple levels and evolve over time [3].

Typically, such infrastructures are energy, oil, gas, finance, transport, telecommunications and health sectors.

In order to function properly, CIs need many different assets (technological, IT hardware, software, environmental, personal, organizational) and complex processes interrelated with other processes across different economy sectors.

Assets and processes of critical infrastructures may be breached by different kinds of threats and hazards, such as: natural disasters and catastrophes, technical disasters and failures, espionage, international crime, physical and cyber terrorism.

CIs are extremely important for today's societies and ensure proper relationships between the citizens and governments. The well developed countries, including the EU countries, are more focused on the protection of their critical infrastructures than the others. The European Council (EC) Directive [4] specifies the CIP-related needs on the EU and member-state levels. The EC Directive provides a definition of ECI (European critical infrastructure) and its basic taxonomy. ECI means 'critical infrastructure located in member states the disruption or destruction of which would have a significant impact on at least two member states'. ECIs are identified in particular countries with the use of sectoral criteria and cross-cutting criteria. The criteria include casualties, economic and public issues. The ECI taxonomy will be presented in Sec. 3.2.

The European Programme for Critical Infrastructure Protection (EPCIP) is aimed at European and national infrastructures. EPCIP was elaborated in 2006. Its revised and more practical implementation is included in the EC document [5].

The paper presents the continuation of the researches described in the author's earlier publications. The paper [6] identifies the basic requirements for the risk management software. The implementation of these requirements is discussed in the publication [7]. This implementation is based on the ready-made OSCAD platform [8]. This software was originally developed to support business continuity management according to ISO 22301 and information security management according to ISO/IEC 27001. It is designed to identify different disturbances of business processes and/or breaches of information assets in different companies and organizations. OSCAD has three main functionalities: to perform risk management (preparedness), to manage incidents (reaction, recovery), and to ensure a continual improvement of the security-related management processes.

Thanks to its openness and flexibility, the OSCAD software can be easily adapted to protect assets or processes in different application domains, e.g.: flood protection [9], railway safety management systems [10] and coal mining [11]. The question is whether it can be applied to a new domain of application, i.e. critical infrastructure risk management.

The OSCAD risk management functionality is the subject of the case study presented here. The aim of the study is to assess the OSCAD usability with respect to the critical infrastructure domain of application. Two groups of requirements are taken into account:

- general requirements for the critical infrastructure risk manager specified in [6],
- specific requirements implied by the European CIRAS[1] project [12].

The activities presented here can be considered as the preliminary researches of the CIRAS project. CIRAS, related to 'The Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme (CIPS)', was launched by the international consortium, including the author's organization:

- ATOS Spain SA (ATOS),
- Centre for European Security Strategies from Germany (CESS),
- Institute of Innovative Technologies EMAG from Poland (EMAG).

The CIRAS methodology is based on the FP7 ValueSec approach [13]. According to this approach, the decision maker should select a countermeasure that:

- properly reduces the risk volume to ensure security on an accepted level and to bring benefits for CI stakeholders,
- is cost-effective during implementation and operation,
- is free of social, psychological, political, legal, ethical, economical, technical, environmental, and other limitations; these intangible factors in the CIRAS project are called 'qualitative criteria'.

The novelty of the CI risk management method presented in the paper is to analyze direct primary impacts caused by a hazardous event in the given CI, as well as the event secondary impacts in the same CI (internal escalation) and in other co-operating CIs (external escalation). This method was embedded into the CI resilience analysis process (Sec. 2.2) and implemented by the author on the OSCAD platform.

The objective of the paper is to perform the validation experiment of this method on the near real data related to the given set of CIs. The experiment embraces:

- planning the validation scenario, which should be relatively simple, but presenting all features of the method,
- identifying the input data, e.g.: assets, processes, threats, vulnerabilities, etc. and implementing them in the software,

[1]This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the European Commission cannot be held responsible for any use which may be made of the information contained therein (Grant Agreement clause).

- defining the risk measures for risk analyses focused on both consequences and causes, and configuring the software tool,
- performing the validation based on the planned scenario and with the use of the OSCAD tool,
- summarizing researches with respect to the acquired risk-related knowledge, usefulness for the OSCAD adaptation to the CIRAS project needs.

As a result of researches, OSCAD-CIRAS, a CI-dedicated risk manager was developed. The results of the author's researches are used as the project input to indicate directions for more comprehensive researches according to the CIRAS project schedule.

The paper includes: a short review of the critical infrastructure specific issues and the state of the art related to risk management in CIs (Sec. 2), preparations to the validation (Sec. 3), the validation process (Sec. 4), and conclusions.

2 Critical infrastructure security and safety—specific issues

Critical infrastructures are very complex socio-technical systems. It is a difficult task to protect them due to their complexity, heterogeneity, distributed nature and existing interdependencies. Apart from interdependencies, the resilience issue and its relationship with risk management are specific for the critical infrastructures.

2.1 Interdependencies and phenomena related to them

Interdependencies are different mutual dependencies between co-operating infrastructures. Generally, dependency defines a unidirectional relationship between infrastructures, while interdependency defines a bidirectional relationship. Researches [14, 15] distinguish four types of interdependencies: physical, cyber, geographical, and logical ones.

Certain specific effects implied by interdependencies are observed in critical infrastructures:

- a cascading effect [2] should be understood as a sequence of component failures when the first failure shifts its load to one or more nearby components; these components fail and, in turn, shift their loads to other components, and so on,
- an escalating failure is when a disruption in one infrastructure causes an independent disruption in another infrastructure [14],
- common cause failures; they are failures implied by a single shared cause and may occur almost simultaneously.

Dire effects of hazardous events propagate across the collaborating infrastructures because of the existing interdependencies. Frequently, such effects escalate outside the area where they occur and aggravate the consequences of a given event. Due to this situation the second failure is more severe and it takes longer to restore it.

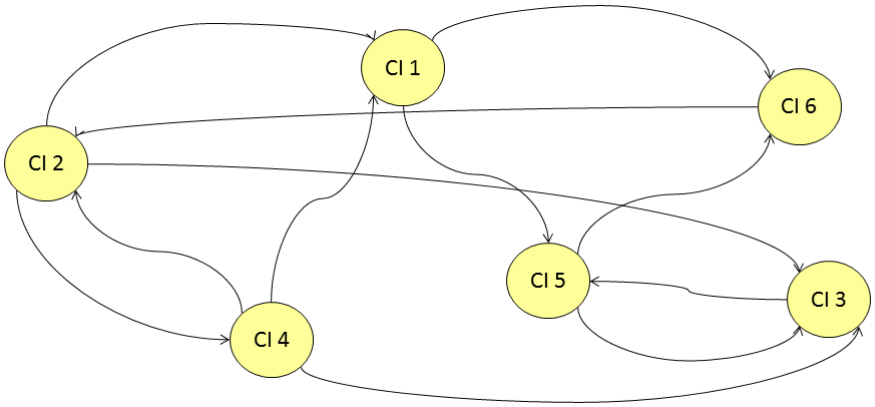

Figure 1 Example of a dependency.

Interdependencies and dependencies are expressed by matrices of relationships or by graphs [16].

Fig. (1) shows a sample dependency diagram. Dependent infrastructures are pointed by arrows, e.g. CI5 depends on CI3 and CI1, CI2 depends on CI4 and CI6. Generally, the dependent CI needs products or services from others to operate.

Dependency diagrams are products provided by the resilience analysis.

2.2 Critical infrastructure resilience analysis and risk management

The resilience of a critical infrastructure concerns its ability to mitigate the magnitude or duration of hazardous events, in other words, it concerns the ability to anticipate, to absorb, to react, to adapt to a critical situation, or to recover after the disruptive event. Resilient CIs are resistant to external and internal disturbances and are able to work on an acceptable efficiency level even when these disturbances occur.

The relations between the resilience analysis and risk assessment are understood according to the work [16]: 'The concept of resilience can be seen as a superset in which typical risk assessment is a complementary part'. The CI resilience analysis process includes the following main activities [16]:

1. Structural analysis of the CI—most critical elements, most vulnerable points, dependencies and interdependencies are identified; here dependency diagrams/matrices are elaborated, playing the roles of the CIs static models,

2. Dynamic analysis to identify the most dangerous risk scenarios—generally, the subject of the analysis or simulation based on the CI static model are: propagation of dire effects of CIs phenomena across interdependent CIs, identification of the threats impact, analyses of common failures, system response to a failure or an incident, recovery process, etc.; as a result the set of risk scenarios is identified,

3. Prioritization of risk scenarios—potentially most dangerous scenarios are delivered to the risk management process for a detailed analysis.

2.3 Risk management specific issue and state of the art

Risk management is the essential part of the resilience process. Special programmes and methodologies which are developed for CI protection are focused on the preparedness and response to incidents. In order to ensure preparedness and incident response ability, it is necessary to identify the risk source, character and level, as well as to implement and monitor the right countermeasures with respect to their effectiveness. Effective CIs protection is based on risk management.

The risk management methodologies and tools are a subject of current R&D on the national and international levels, including the EU level. An exhaustive review of laws, standards, frameworks, methods and tools was conducted in the course of the CIRAS project [17]. This review refers to the following knowledge sources in the field:

- the report [18] of the Institute for the Protection and Security of the Citizen, one of the EC Joint Research Centres (JRC); the report assesses and summarizes 21 existing risk management methodologies/tools on the EU and global level; it identifies their gaps and prepares the ground for R&D in this field,
- the book [15]; Appendix C compares the features of about 22 commonly used risk analysis methods,
- the EURACOM report [19] features a desktop study of 11 risk assessment methodologies related to the energy sector,
- the ISO 31010 standard [20] describes about 30 risk assessment methods for different applications,
- the ENISA website [21] provides an inventory of risk management/assessment methods, mostly ICT-focused.

To secure a better direction of the CIRAS toolset development, it is necessary to carry out certain researches of the existing tools, including the OSCAD tool.

The review based on the elaborated project criteria for methods reflected the following characteristics: capability, maturity, adaptability, availability (i.e. copyrights, high license fees), application of qualitative criteria (intangible factors), recognition in the CI application domain, CIs effects inclusion (i.e. interdependencies, cascading/escalation effects). The following preselected methods were assessed:

- Bayesian networks [2, 20],
- BIA (Business impact analysis) [20, 22],
- Consequences-probability matrix [2, 20],
- Bow-tie analysis [2, 20],
- CBA (Cost/benefit analysis) [13, 20],
- ETA (Event tree analysis) [2, 20, 23],

- FMEA/FMECA (Failure mode effect analysis/Failure mode, effects, and criticality analysis) [2, 20, 24],
- FTA (Fault tree analysis) [2, 20, 25],
- HAZOP (Hazard and operability) study [2, 20],
- LOPA (Layers of protection analysis) [2, 20],
- MCDA (Multi-criteria decision analysis) [20, 26],
- PHA (Preliminary hazard analysis) [2, 20],
- RVA (Risk and vulnerability analysis) [15, 18],
- SWIFT (Structured 'What if' technique) [2, 20].

Similar criteria were elaborated for tools. In this case the following were considered: tool functionality, maturity, flexibility, availability (source code, high license fees), application of qualitative criteria (intangible factors), recognition in the CI application domain, and CIs effects inclusion. A huge number of preselected software tools were reviewed against the above criteria. There are many different risk assessment tools which can be considered to apply in the project domain, e.g.:

- Free web-based fault tree analysis software (FTA) [27],
- Expert choice (MCDA/Saaty method) [28],
- Open FTA (FTA) [29],
- GeNIe 2.0 (Bayesian networks) [30],
- CAFTA—Computer aided fault tree analysis system (FTA, ETA) [31],
- BowTieXP (BowTie analysis method) [32],
- RAM commander (FMEA/FMECA, FTA, ETA) [33],
- HAZOP manager version 7.0 (HAZOP, PHA, Hazard identification, FMEA/FMECA) [34],
- InfraRisk (PHA, Bow tie model with FTA/ETA, DECRIS project tool) [35],
- PHAWorks (PHA, HAZOP, SWIFT, FMEA) [36],
- Reliability workbench (FMEA/FMECA, FTA, ETA, Markov analysis) [37],
- THESIS BowTie (Bow-tie analysis, LOPA) [38],
- Xfmea—Synthesis platform (FMEA/FMECA) [39],
- OSCAD (Consequences-probability matrix, BIA) [8].

During the review the general requirements for CI risk manager identified in [6] were taken into account, i.e. the ability of the method/tool:

- to consider interdependencies and phenomena related to them,
- to analyze consequences and causes of a given hazardous event (the bow-tie risk management concept [2]),
- to express the most important data included in the risk register; please note that the risk register is a managed inventory of hazardous events,
- to define risk measures parameters (e.g.: likelihood, probability, frequency, consequences, their categories, scales of measures) in a flexible way.

Apart from the general requirements, the CIRAS project requirements [12] were considered, i.e. the possibility:

- to assess the risk value before and after the countermeasure implementation—to identify the risk reduction implied by the given countermeasure,
- to use in the risk management process parameters dealing with the cost, benefit, and intangible restrictions [9],
- to consider single countermeasures as well as packages of countermeasures,
- to consider several alternative packages of countermeasures, to select the right one for the final implementation,
- to consider cross-sectoral risk management.

The review shows that many risk assessment methods and tools can be applied in the critical infrastructure domain. They were developed for different organizations with a view to solve their technical or organizational risk-related problems within the limited environments. Initially they were not dedicated to critical infrastructures, however, later, many of them were adapted to CI needs.

The reviewed methods [17] do not explicitly distinguish CI internal and external causes of hazardous events. What is more, they do not distinguish CI internal non-escalating consequences, consequences generating hazards/threats in the same infrastructure, and consequences generating external hazards/threats for other collaborating infrastructures either. There is no method which would consider the cost, benefit, and intangible restrictions with respect to the CIs.

The paper [7] describes how the general purpose risk manager implemented in the OSCAD software could be adapted to the CIs application. This paper also presents the validation plan of the OSCAD-CIRAS tool, based on the defined scenario which is focused on the railway transport CI interacting with the electricity CI. OSCAD-CIRAS is able to distinguish internal and external causes of hazardous events as well as internal and external consequences implied by these events.

Due to the CIs complexity, interdependencies, specific effects, different abstract levels applied to manage CIs (national, sectoral, operational) and other factors, the risk management in critical infrastructures still remains a challenge.

3 Preparing the OSCAD-CIRAS validation process

The subject of the validation is the OSCAD-CIRAS experimentation tool presented in the publication [7]. The aim of the validation is to get knowledge about risk issues through performing a representative use case in critical infrastructures and to assess whether the validated tool can be useful for the CIRAS project.

3.1 Critical infrastructure risk management requirements and their implementation in the OSCAD software

The paper [7] presents the OSCAD software adapted for risk management experimentations in critical infrastructures (OSCAD-CIRAS) and basic scenarios of these experiments with respect to such CIs phenomena as escalations and cascading effects implied by the CIs interdependencies. The process of meeting the requirements can be summarized as follows:

Bow-tie as the conceptual model of the risk manager OSCAD-CIRAS has a functionality to analyze the multidimensional consequences of hazardous events:

- Asset Oriented Business Impact Analyzer (ABIA),
- Process Oriented Business Impact Analyzer (PBIA),

as well as functionalities to analyze the causes of hazardous events:

- Asset Oriented Risk Analyzer (AORA),
- Process Oriented Risk Analyzer (PORA).

Each pair: AORA-ABIA and PORA-PBIA can be understood as the bow-tie model implementation.

Implementation of the risk register and risk-related data The risk register contains information about assets (and/or processes) impacted during a hazardous event, consequences, event frequency, threats, vulnerabilities, and assessed multidirectional impacts. They are predefined and placed in OSCAD-CIRAS system dictionaries, used by the asset and process inventories and by the four above mentioned risk assessment tools.

Risk measures and the assessment process The BIA risk measures expressing multidimensional impacts of the hazardous event encompass loss subcategories belonging to three main impacts categories:

- CI internal degradation/damages (CID),
- generated internal hazards, called here internal escalation effects (IE),
- generated external hazards, called here external escalation effects (EE).

Please note that the BIA-type method introduced in the paper takes into account hazards generated in the same CI (IE) and hazards generated in the neighbouring CIs (EE) as the distinguished impacts categories.

Distinguishing these three main categories allows to consider different CI specific phenomena in risk management. The numbers of loss subcategories and loss levels in loss matrix are configurable.

RA uses event likelihood categories and consequences categories (the latter derived from BIA results). All of them are user-defined.

The assessment process starts from the scenario of the highest criticality obtained from the resilience analysis. First, BIA (a consequences analysis) is performed, and its results encompass CID, IE and EE impacts.

Next, RA (a causes analysis) is performed to identify threat/vulnerability pairs leading to the hazardous event. The likelihood related to these pairs is assessed. OSCAD requires the event consequences input as well. The consequences are derived from the BIA results.

Detecting the external effect (EE) implies an additional BIA-RA pair of analyses performed in the impacted dependent CI.

Detecting the internal effect (IE) launches a BIA-RA pair for the breached security barrier belonging to the same CI. This secondary effect may cause new secondary internal damages (CID), an external impact (an additional EE-related risk scenario) as well as a new IE-related risk scenario. These analyses focus on internal propagations and are repeated until no additional internal secondary effects occur. Then, the next risk scenario is taken into account and analyzed in the same way. The whole process stops when all scenarios obtained from the resilience process are analyzed.

Interdependencies and critical infrastructure specific phenomena Before risk management starts, the dependencies should be known. They are identified during the resilience analysis and obtained in the form of a dependency diagram. All possible CI phenomena (Subsection 2.1) can be detected for the set of collaborating infrastructures.

3.2 Validation context

The European Council (EC) Directive [4] specifies two groups of European Critical Infrastructures (ECIs):

- energy, encompassing the following ECIs: Electricity (Ele), Oil (Oil), Gas (Gas),
- transport, embracing other ECIs: Road Transport (RoT), Rail Transport (RaT), Air Transport (AiT), Inland Waterways Transport (IWT), and Ocean and Short-Sea Shipping and Ports (Sea).

Please note the ECI mnemonics in parentheses, introduced in this paper and used as labels in OSCAD-CIRAS.

Other categories of CIs (i.e. non-ECI), e.g. electronic communication, banking and finance, health, social and social security services, are not considered here.

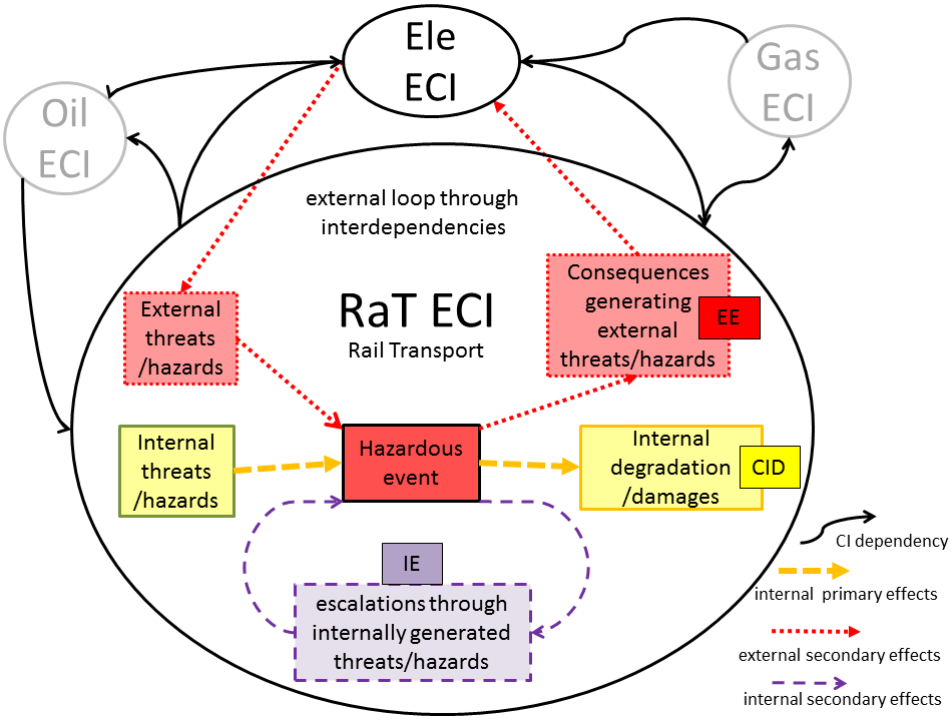

Figure 2 Validation context.

3.3 OSCAD-CIRAS as the validation subject

Fig. (2) shows the Rail Transport (RaT), Electricity (Ele), Oil (Oil) and Gas (Gas) critical infrastructures and dependencies between them (a dependency diagram).

The validation process will be focused on railway transport (RaT) collaborating with Electricity (Ele). Fig. (2) shows direct CI damages as well as the propagation path for external and internal effects caused by the hazardous event.

The validation considers:

- threats/hazards issued inside RaT or passed from the external Ele ECI,
- internal consequences of a hazardous event occurring in RaT,
- internally generated escalation caused by a hazardous event,
- impact on the external Ele ECI by generating threats for Ele ECI or increasing vulnerabilities within this infrastructure.

The OSCAD-CIRAS tool is discussed more thoroughly in the publication [7], therefore only basic information will be presented in the paper.

The adaptation of the open OSCAD software platform to the CI applications embraces the identification of the CI domain data, elaboration of system dictionaries on this basis and configuration of the system as a whole.

The main (primary) assets of the given CI are the subject of AORA, therefore they are protected. An asset name is preceded by a CI mnemonic, e.g.: RaT:Node, Ele:Power plant. The associations of auxiliary (secondary) assets are grouped around the given primary asset. The secondary assets are not the subject of the AORA analysis. For this reason, a special category of secondary assets A=C (Countermeasures considered as assets) is distinguished to enable risk analysis. These assets represent security-related objects which can be a subject of an attack, e.g. security zone, perimeter. An asset of this category (A=C) can be added to a given asset group. This approach allows to consider additional effects of security breaches, i.e. secondary effects with respect to the hazardous event. This mechanism allows to analyze the propagation of internal secondary effects (IE).

The risk register is defined in OSCAD as a set of risk scenarios which are identified as threats worked out during AORA or PORA. They are compatible with the incident inventory. Assuming that the threat agent is identified as the hazard trigger, OSCAD allows common representation of threats and hazards.

OSCAD has predefined and flat lists of threats which are the basis to organize vulnerabilities and countermeasures placed in dictionaries in a hierarchical structure. On the upper hierarchy level threats can be ordered by critical infrastructures, and for each infrastructure the following taxonomy is used for threats: Behavioural/Social, Natural/Force majeure, Organizational, and Technological. A given threat (T) has its relevant vulnerabilities (V) associated, while for the given pair threat-vulnerability, the recommended countermeasures (C) can be proposed.

The ABIA/PBIA analyses have certain measures defined of multidimensional consequences of the hazardous events. Three groups of consequences are distinguished. The basic group concerns the CI degradation (CID). The remaining two groups of consequences are introduced especially to propagate the escalation/cascading effects:

- IE (Internal escalation effects) express new internally generated threats or new or increased vulnerabilities which influence the considered CI and are caused by the hazardous event,
- EE (External escalation effects) express generated threats which impact the external CIs or new or increased vulnerabilities in the external CIs and are caused by the hazardous event.

The loss subcategories of these three main categories are defined in the business loss dictionary (Fig. (3)).

Each category is assessed in the range from level 1 to level 5. The number of subcategories and levels is configurable. In the example presented in the paper the Worst Case Model (WCM) is used to calculate the BIA result, as it is very simple. The BIA result is the maximum value of the CID, IE and EE impacts, it means that the BIA result is in the range 1 to 5. OSCAD-CIRAS allows to apply the product or total calculation models as well—not discussed here.

The RA analyses need to define the 'Event likelihood' and 'Event consequences' measures which are used to calculate the risk with the use of a simple formula

$$\text{Risk} = \text{Event likelihood} \times \text{Event consequences}.$$

The RA 'Event likelihood' measures with their interpretations are based on measures proposed in [2, 6]:

Business loss matrix

Business loss category	Level1	Level2	Level3	Level4	Level5
CID: Economic losses dimension (Mio Euro)	< 0.1	[0.1-1)	[1, 100)	[10-100)	⩾ 100
CID: Environmental impact dimension	No impacts or not significant impacts (surrounding area, recovery < 1 year)	Minor impacts (limited area, recovery time < 5 years)	Major damages (considerable area, e.g. plant area, recovery time 5-10 years)	Severe damages (broad area, e.g. region, recovery time 10-20 years)	Very large area impacted, e.g. country, recovery time >20 years)
CID: Live and injury dimension	< 4 injured /seriously ill	4–30 injured /seriously ill	1–2 fatalities, 31–100 injured /seriously ill	3–20 fatalities, 101–600 injured /seriously ill	> 20 fatalities, > 600 injured /seriously ill
CID: Social impact dimension	None or not significant	Minor social dissatisfaction	Moderate dissatisfaction, possible episodic demon-strations	Serious dissatisfaction, possible demonstrations , strikes, riots	Migration from the affected area or country
EE: Generation of threats/hazards to the external...	Neglibible. No threats/hazards generated	Minor damage. 1-2 threats/hazards influence a single external CI	Major damage. 3-5 threats/hazards influence a single external CI	Severe loss. 6-10 threats/hazards influence 1 or 2 external CIs	Catastrophic. More than 10 threats/hazards influence more than 2 external CIs
EE: Increasing vulnerabilities to threats/hazards i...	Negligible No influence on the external CIs vulnerabilities	Minor damage Incr eased 1-2 vulnerabilities of a single external CI	Increased 3-5 vulnerabilities of a single external CI	Increased 6-10 vulnerabilities of 1 or 2 external CIs	More than 10 increased vulnerabilities of 2 or more external CIs
IE: Increasing vulnerabilities to internal threats/h...	Negligible No influence on the internal CI vulnerabilities	Minor damage Incr eased 1-2 vulnerabilities of the considered CI	Increased 3-5 vulnerabilities of the considered CI	Increased 6-10 vulnerabilities of the considered CI	More than 10 increased vulnerabilities of the considered CI
IE: Internal threats/hazards generation	Negligible No threats/hazards issued	Minor damage 1-2 threats/hazards of the 1st generation issued for the	Major damage 3-5 threats/hazards of the 1st generation issued for the	Severe loss 6-10 threats/hazards of the 1st generation issued for the	Catastrophic More than 10 threats/hazards of the 1st generation issued for the considered CI OR more than 5 threats/hazards of the 2nd generation issued for the considered CI OR the 3rd or next threats/hazards

Figure 3 Event impacts measures with CID, IE and EE categories (in rows) and impact levels (columns)—the OSCAD-CIRAS business loss matrix. Source: OSCAD-CIRAS risk manager during validation.

- 1 (Improbable), extremely rare event (from 0 to 10^{-5} per year),
- 2 (Remote), very rare event that will not necessarily be experienced in a similar plant (from 10^{-5} to 10^{-3} per year),
- 3 (Possible), rare event, but will be possibly experienced by personnel (from 10^{-3} to 10^{-1} per year),
- 4 (Occasional), event that may happen now and then and will normally be experienced by personnel (from 0.1 to 1 per year),
- 5 (Fairly normal), event that is expected to occur frequently (from 1 to 10 per year).

The RA 'Event consequences' measures are derived from the loss matrix categories:

- 1 (Negligible damage), when BIA impact equals 1,
- 2 (Minor damage), when BIA impact equals 2,
- 3 (Major damage), when BIA impact equals 3,
- 4 (Severe loss), when BIA impact equals 4,
- 5 (Catastrophic), when BIA impact equals 5.

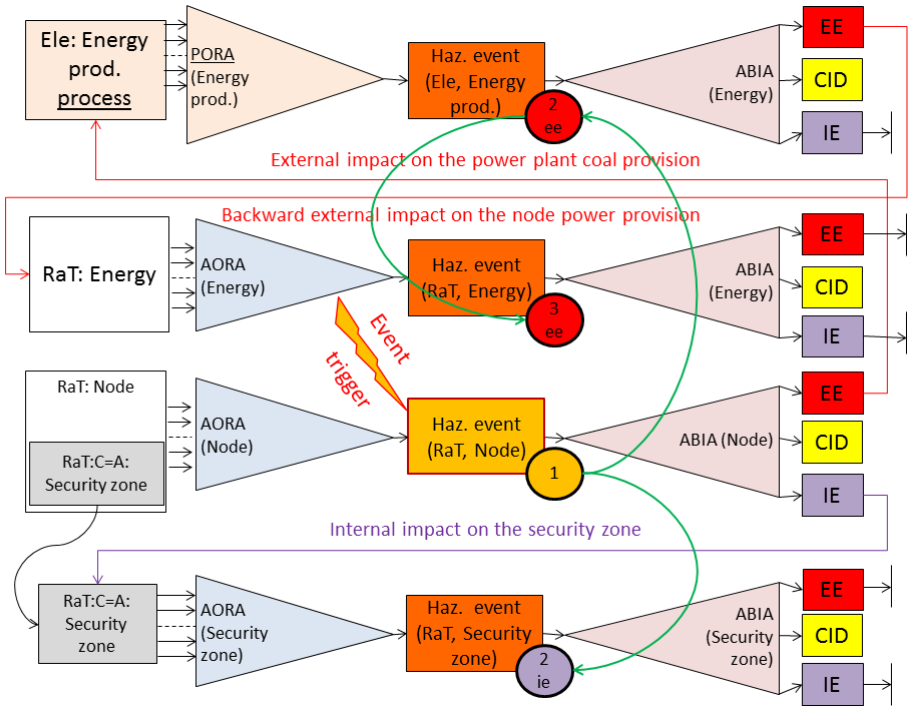

Figure 4 Validation scenario.

3.4 Validation plan and scenarios

Fig. (4) presents an example of a risk assessment scenario for the validation process. The scenario embraces four pairs of analyses (RA-BIA). Each pair can be considered a single bow-tie model related to a certain hazardous event [2, 6]. However, in OSCAD-CIRAS the analysis starts from BIA, followed by RA, because the consequences of both analyses were harmonized. Please note that this order following the OSCAD-CIRAS validation process is used in Sec. 4.

The scenarios are driven by risk situations which occur within two interdependent RaT and Ele infrastructures. Please note that the consequences of hazardous events in a given CI can impact the same CI again and/or can impact the neighbouring CIs. This way a complex sequence of impacts can occur. For this reason, it is recommended to order these impacts and the needed analyses. On this basis the management rules of the analyses should be elaborated to run them pseudo-concurrently. This issue needs further researches. For simpler applications, the analyses can be done manually, depending on the identified kinds of consequences.

Please note the numbers in circles which order the sequence of analyses pairs in Fig. (4). For example, '2ie' means iteration 2 caused by internal effects (ie). The following general scheme of numeration is assumed: iteration number with a postfix representing the kind of impact.

For the validation purpose a sequence of scenarios and related analyses is elaborated:

Initiation, a basic scenario obtained from the resilience analysis In RaT:Node an event occurs which causes a hazardous event, e.g. intentional derailment impacting the node area.

1st iteration '1 ABIA(RaT:Node)' identifies the multidimensional consequences of the hazardous event:

- the internal degradation (mostly financial consequences) caused by the intentional derailment (CID),
- breaches of the security zone which is a secondary asset of RaT:Node (IE),
- impacts of the external infrastructure Ele (EE) occurring because the coal transport for the power plant is stopped for a long time.

'1 AORA(RaT:Node)' identifies the risk related to this hazardous event based on Eq. (3.3).

2nd iteration Due to the internal escalation effects (IE), an extra pair of analyses of the security zone is needed:

- '2ie ABIA(RaT:Node->Security zone)',
- '2ie AORA(RaT:Node->Security zone)'.

The related ABIA identifies CI secondary damages caused by unauthorized access which occurred after the security zone breach. No further IE or EE impacts are revealed. RA calculates the risk of unauthorized access facilitated by the zone breach.

Due to the external escalation effects (EE), an extra analysis of the energy production/delivery process in the Ele ECI is required.

- '2ee ABIA(Ele:Energy)' identifies the CI degradation caused by an externally generated threat and backward external impacts to the RaT infrastructure (energy provision for the RaT:Energy), while it does not identify any internal escalation effects (IE),
- '2ee PORA(Ele:Energy production)' assesses the risk related to the energy production process in the power plant, i.e. assesses how a coal delivery disturbance impacts the energy production process (in this case the process-oriented analysis is applied).

3rd iteration Due to the external threat generated by Ele ECI for RaT:Energy, an additional pair of analyses is performed:

- '3ee ABIA(RaT:Energy)',
- '3ee AORA(RaT:Energy)'.

The CI internal degradation is assessed and no internal/external propagations are detected. In the 3rd iteration both RaT and Ele infrastructures achieve a stable state – no further analyses are needed.

Particular analyses will be performed during the validation process.

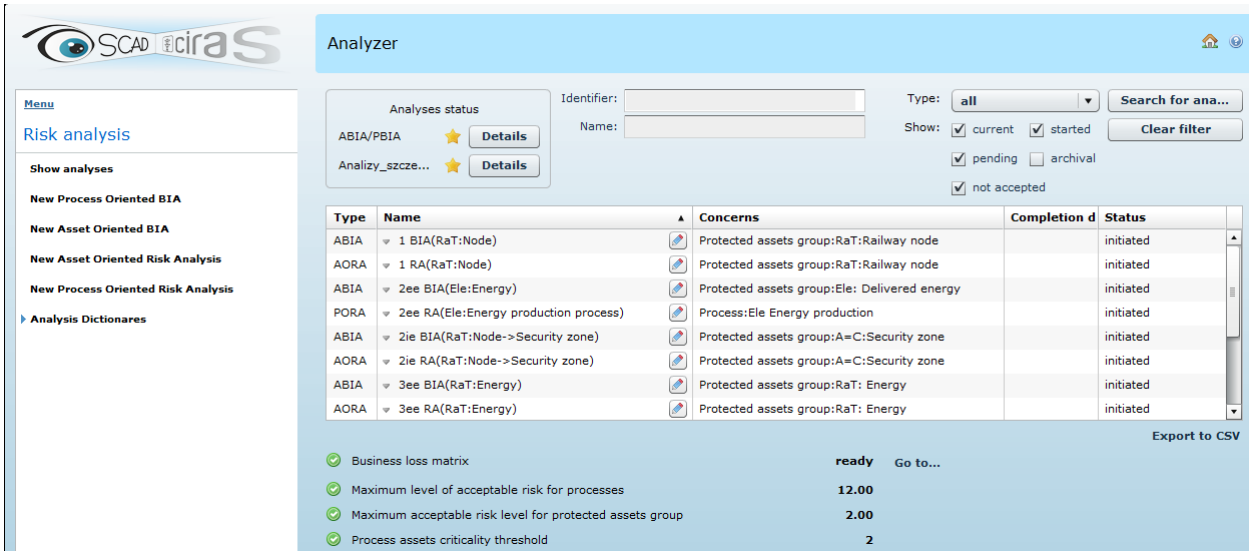

Figure 5 OSCAD-CIRAS tool presenting analyses encompassed by the validation process Source: OSCAD-CIRAS risk manager during validation.

4 The OSCAD-CIRAS validation process

Fig. (5) shows all analyses in the OSCAD-CIRAS tool, mentioned in the validation scenario.

The left side features the tool menu/submenu depending on the operation context, e.g. risk analyses. The right part shows all performed analyses, their status, and risk acceptance parameters (not discussed here). It is an entry point to view/modify details of each analysis. Please note the names of analyses compliant with the validation scenario, and in the next column ('Concerns')—the related assets or processes.

Initiation (a basic scenario obtained from the resilience analysis) According to the validation scenario (Fig. (4)) an event is triggered in the railway node. It is classified as intentional derailment.

1st iteration This hazardous event is the subject of the "1 ABIA(RaT:Node)" consequences analysis. Fig. (6) shows the assessed CI degradation (CID) caused by the impacted node—impacts assessed in five time horizons.

Similar analyses (but without time horizons) are performed with respect to:

- the internal escalation effects attribute (IE), a breach of the security zone is identified, implying '2ie ABIA(RaT:Node->Security zone)' shown in Fig. (8) and '2ie AORA(RaT:Node->Security zone)' in Fig. (9); will be analyzed in the 2nd iteration,
- the external escalation effects attribute (EE) – disturbance of the fuel (coal) delivery for the power plant is detected, causing '2ee ABIA(Ele:Energy)' shown in Fig. (10) and '2ee PORA(Ele:Energy production)' in Fig. (11); will be analyzed in the 2nd iteration.

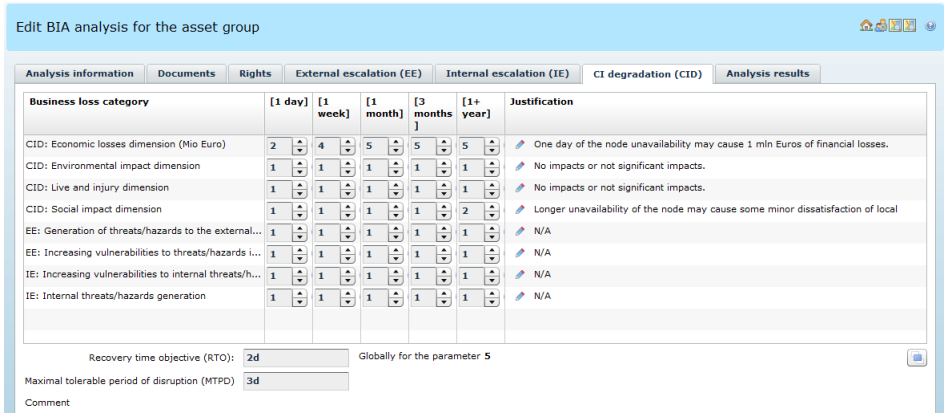

Figure 6 ABIA analysis for the railway node Source: OSCAD-CIRAS risk manager during validation.

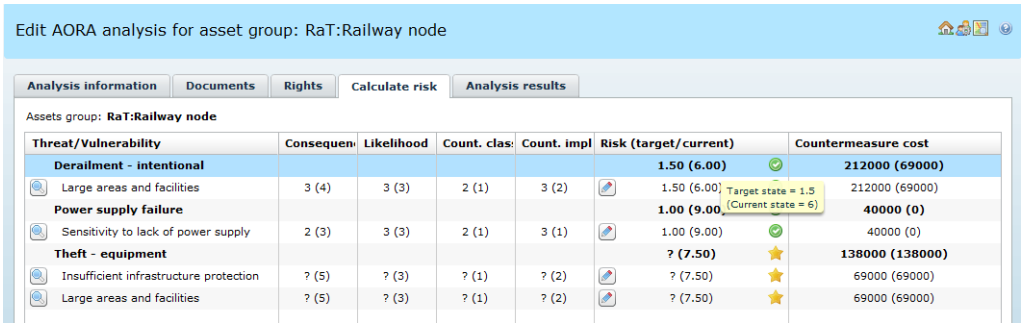

Figure 7 Asset-oriented risk analysis for the railway node (a cause analysis). Source: OSCAD-CIRAS risk manager during validation.

After identifying the consequences, the causes are analysed. The basic hazardous event now is the subject of the '1 AORA(RaT:Node)' analysis, shown in Fig. (7). The vulnerability related to this threat deals with difficulties to monitor large areas of the railway node. Inherent risk was 6.0, but after applying certain countermeasures (an example of countermeasures selection during risk management is shown in [7]) the risk value was decreased to 1.5 (max. value is 25.0). Please note that the countermeasures cost rises from 69.000 PLN to 212.000 PLN. This hazardous event concerns the 'RaT:Railway node' asset. Together with this event, two others can be analyzed (power supply failure, equipment theft) related to the same asset (RaT:Railway node).

In this point of the validation scenario the first (basic) iteration is finalized (a pair BIA-RA).

Please note that both internal and external impacts are detected. These imply the second iteration of the risk analyses encompassing both the internal and external impacts.

2nd iteration In this case both internal and external propagations should be considered. Let us start from the internal ones.

During the 1st iteration an internal threat against the security zone is identified within the

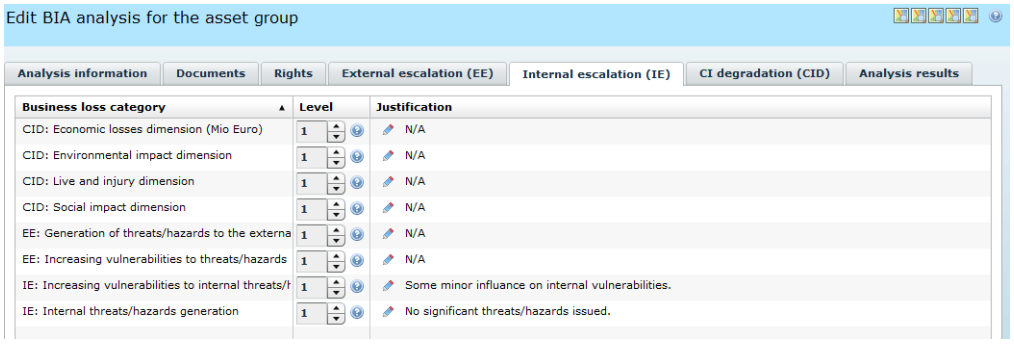

Figure 8 ABIA analysis for the security zone of the railway node (IE aspects) Source: OSCAD-CIRAS risk manager during validation.

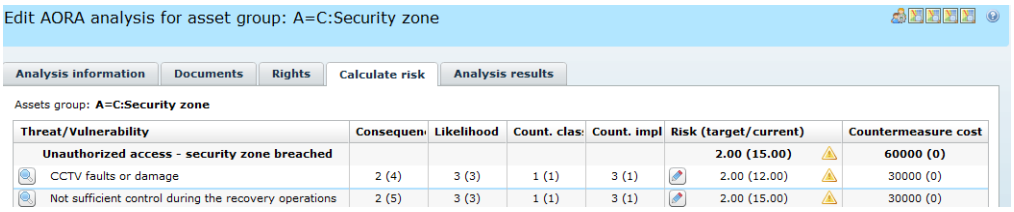

Figure 9 AORA analysis for the security zone of the railway node Source: OSCAD-CIRAS risk manager during validation.

railway node. Please note that the security zone has twofold meaning (marked as: 'C=A', a special asset category [7]). Firstly, the zone is an asset, as a part of the node facilities. Secondly it is also a countermeasure. It protects some objects in its interior which can be damaged due to the zone breach. These damages are CI internal, secondary effects. These effects can be assessed with the use of the pair of analyses:

- '2ie ABIA(RaT:Node->Security zone)'; consequences analysis (Fig. (8)),
- '2ie AORA(RaT:Node->Security zone)'; causes analysis (Fig. (9)),

Fig. (8) exemplifies ABIA for the security zone with respect to further internal escalations—none of them serious. No external escalations are detected either (not shown). This stable situation makes further analyses unnecessary.

The internal escalation constitutes certain internal loops within the considered CI. The internal secondary effects (effects caused by primary effects) follow this path until no further impacts are identified—the CI damages stabilize.

Fig. (9) shows AORA with respect to the secondary asset 'A=C:Security zone', being a part of the previously analyzed primary asset 'RaT:Node'. Please note that for the threat 'Unauthorized access—security zone breached' two vulnerabilities are considered.

In the 2nd iteration the external escalations should be analyzed, because they were detected in the 1st iteration. This way the influence of RaT CI on Ele CI is considered.

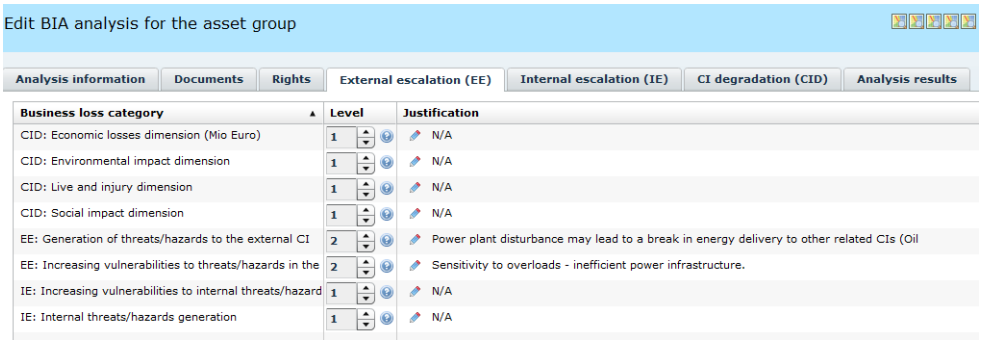

Figure 10 ABIA for the energy asset provided by the power plant – consequences analysis Source: OSCAD-CIRAS risk manager during validation.

The disturbances of the energy production process may negatively influence the basic asset—the energy delivered to customers, including railways. The CID degradation was assessed rather low (not shown), and no further internal consequences are generated (simplification).

Only the Ele external escalation may occur (Fig. (10)), i.e. disturbance of the energy delivery. It is assumed that this problem may touch the energy provision for the railway CI (see further Fig. (12) and 13), including the considered railway node. It implies the third iteration, causing the pair of analyses: '3ee ABIA(RaT:Energy)' and '3ee AORA(RaT:Energy)'. The causes of the energy production disturbance are analyzed with the use of PORA (Fig. (11)).

The PORA analysis considers the energy production process. The fuel (coal) delivery disturbances (threat), with the coincidence of insufficient fuel in stock (vulnerability), may break the energy production process efficiency or even the continuity of the process.

3rd iteration Stoppages in energy delivery by the external provider (a threat), coupled with the sensitivity to overloads (a vulnerability), may disturb the work of electrical equipment placed in the railway node.

Loss of the power supply quality (breaks, low quality) impacts the considered node, but this impact is rather limited (CID) because there are redundant power lines for the node. Moreover no serious IE/EE effects are escalated. Fig. (12) shows the external effects assessment.

AORA (Fig. (13)) is focused on the causes of the energy disturbance in the node.

The risk value for the pair:

- the threat 'Break in energy supply',
- the vulnerability 'Sensitivity to overloads',

was sufficiently mitigated from 6.0 to 0.67 by electrical infrastructure investments in the past. As a result of these investments, the railway node is supplied by three independent energy sources.

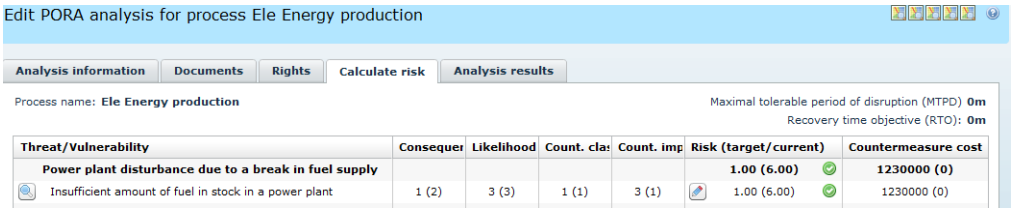

Figure 11 PORA for the energy production process – causes analysis Source: OSCAD-CIRAS risk manager during validation.

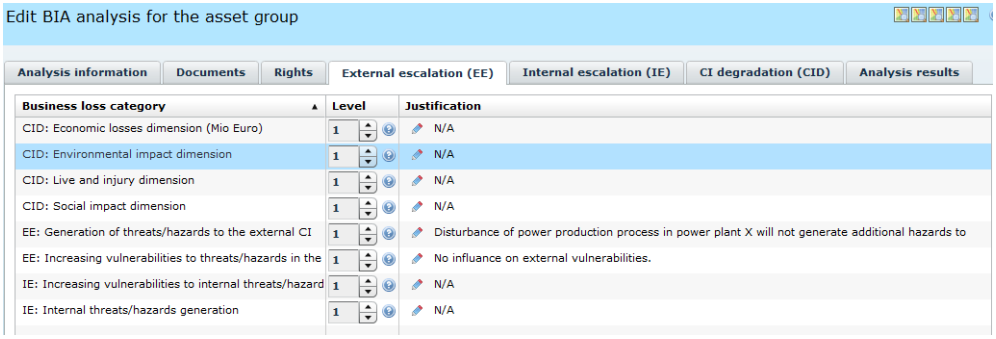

Figure 12 Consequences analysis for the node power provided by the Ele infrastructure Source: OSCAD-CIRAS risk manager during validation.

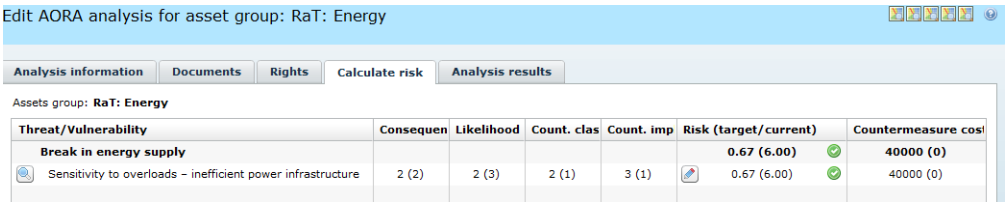

Figure 13 Causes analysis for the node power provided by the Ele infrastructure Source: OSCAD-CIRAS risk manager during validation.

5 Conclusions

The author presents the validation of the experimental tool used for risk management in critical infrastructures. The validation is based on the planned scenario encompassing two critical infrastructures: railway transport and electricity provision.

The internal escalation effects (through a CI internal path) and the external escalations effects (through a path crossing one or more CIs) are demonstrated. These are the key features of the method presented and validated in this paper. Please note that the scenario depends on the risk encountered during the analysis. It means that other risk situation may drive quite a different scenario in the same set of infrastructures. For this reason, the scenario can be called a risk driven scenario.

The validation according to the planned scenario was performed successfully, but some issues require comments.

While implementing the novel risk management method OSCAD-CIRAS should be supported by an external graph (a dependency diagram) which guides the risk assessment process. Consequences of hazardous events may propagate only along dependency paths, for this reason dependencies should be known a priori.

The indirect bow-tie model implementation in OSCAD-CIRAS is quite useful. To improve the model management, a certain management mechanism is needed to control the sequences of analyses.

The novelty of the method presented in the paper is the introduction of three CI attributes:

- CID, i.e. CI degradation, expressing different impacts to assets, as in traditional risk assessment,
- IE, i.e. internal escalation effects, expressing the security problems issued by the CI to itself,
- EE, i.e. external escalation effects, allowing to express impact of hazardous events on dependent critical infrastructures.

According to these attributes, three kinds of consequence analyses are performed. Moreover, the CID-type consequences can be assessed in several time horizons, as in the business continuity domain. This is also a novel element in the risk management in CIs.

Please note that the escalation path is broken when no other IE/EE impacts are produced. In such a situation no further iterations are issued.

The internal/external escalations concern mostly the threats generation (demonstrated). Moreover, it is possible to express the consequences as the increasing internal/external vulnerabilities (not demonstrated). Please note that the flooding of a certain area, causing different damages, such as fire and landslides, can weaken the protection system. To consider such vulnerabilities, the threats associated with them should be identified (if exist), and for each threat-vulnerability pair the risk should be assessed.

It is possible to analyze multilayer protection systems related to assets/processes. However, as many iterations are needed, this may be cumbersome.

The AORA and PORA analyses consider cost parameters of countermeasures. In the CIRAS project this functionality will be extended and supplemented by benefits and intangible parameters. During the risk management process several security alternatives (each composed from

different kinds of countermeasures) can be considered in OSCAD [7] to select the most advantageous one for implementation.

The implemented causes-focused risk analyses (AORA/PORA) and consequences-focused analyses (ABIA/PBIA) are rather simple. In certain applications (multi-layer protection) they may not be sufficient. In this case the fault tree analysis [27] approach for causes and the event tree analysis [23] for consequences may be a helpful alternative in certain circumstances. All these conclusions can be considered during the CIRAS toolset development.

The performed researches allow to acquire knowledge about risk issues within interdependent infrastructures needed for the European CIRAS project. The usefulness of the OSCAD-based risk manager in this application domain was assessed and directions for further R&D works were identified. The research results were used in the CIRAS project. The project is at its final stage now. All pillars: the OSCAD-based risk manager (RRA), the cost-benefits component (CBA) and the qualitative criteria component (QCA) were integrated and validated in two project use cases with the stakeholders' participation (big energy provider, large metro transport operator). The results were presented soon during the international final conference of the project.

References

[1] A. Białas. Research on critical infrastructures risk management. In *Internet in the information Society 2015 – 10th International Conference Proceedings*, pages 93–108. Scientific Publishing University of Dąbrowa Górnicza, 2015.

[2] M. Rausand. *Risk assessment: theory, methods, and applications*. J. Wiley & Sons, 2011.

[3] I. Eusgeld, C. Nan, and S. Dietz. "System-of-systems" approach for interdependent critical infrastructures. *Reliability Engineering & System Safety*, 96(6):679–686, 2011. DOI: 10.1016/j.ress.2010.12.010.

[4] EU Commission. COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. *Official Journal of the European Union*, 2008.

[5] EU Commission. Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure. *SWD (2013) 318*, 2013.

[6] A. Białas. Critical infrastructures risk manager – the basic requirements elaboration. In W. Zamojski, J. Mazurkiewicz, J. Sugier, T. Walkowiak, and J. Kacprzyk, editors, *Theory and Engineering of Complex Systems and Dependability: Proceedings of the Tenth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX, June 29 – July 3 2015, Brunów, Poland*, pages 11–24. Springer International Publishing, 2015. DOI: 10.1007/978-3-319-19216-1_2.

[7] A. Białas. Experimentation tool for critical infrastructures risk management. In *Proceedings of the 2015 Federated Conference on Computer Science and Information Systems*. Polish Information Processing Society PTI, 2015. DOI: 10.15439/2015f77.

[8] OSCAD project website. http://www.oscad.eu. Accessed: 22.05.2016.

[9] A. Białas. Risk assessment aspects in mastering the value function of security measures. In *New Results in Dependability and Computer Systems*, pages 25–39. Springer International Publishing, 2013. DOI: 10.1007/978-3-319-00945-2_3.

[10] A. Białas. Computer support for the railway safety management system – first validation results. In W. Zamojski, J. Mazurkiewicz, J. Sugier, T. Walkowiak, and J. Kacprzyk, editors, *Proceedings of the Ninth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX. June 30 – July 4, 2014, Brunów, Poland*, pages 81–91. Springer International Publishing, 2014. DOI: 10.1007/978-3-319-07013-1_8.

[11] A Białas. Business continuity management, information security and assets management in mining. *Mechanizacja i Automatyzacja Górnictwa*, 8:125–138, 2013.

[12] CIRAS project website. http://www.cirasproject.eu. Accessed: 22.05.2016.

[13] ValueSec FP7 project website. http://www.valuesec.eu. Accessed: 22.05.2016.

[14] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems*, 21(6):11–25, 2001. DOI: 10.1109/37.969131.

[15] P. Hokstad, I. B. Utne, and J. Vatn. *Risk and Interdependencies in Critical Infrastructures.* Springer London, 2012. DOI: 10.1007/978-1-4471-4661-2.

[16] G. Giannopoulos and R. Filippini. *Risk assessment and resilience for critical infrastructures: Workshop proceedings 25-26 April 2012 Ranco, Italy.* Publications Office, 2012. DOI: 10.2788/35914.

[17] J. Bagiński, A. Białas, D. Rogowski, and et al. *D1.1—State of the Art of Methods and Tools.* CIRAS Deliverable. Responsible: Institute of Innovative Technologies EMAG, Dissem. level: RE/CO, 2015. Available for: beneficiaries, stakeholders, Europ. Commission.

[18] G. Giannopoulos, R. Filippini, and M. Schimmer. *Risk assessment methodologies for critical infrastructure protection.* Publications Office, Luxembourg, 2012. DOI: 10.2788/22260.

[19] Deliverable D2.1. Common areas of Risk Assessment Methodologies, 2007.

[20] IEC 31010:2009. Risk Management — Risk Assessment Techniques, IEC/ISO.

[21] ENISA. http://www.rm-inv.enisa.europa.eu/methods. Accessed: 22.05.2016.

[22] I. Charters. *A practical approach to business impact analysis: understanding the organization through business continuity management.* BSI British Standards, 2011. DOI: 10.3403/9780580731013.

[23] Analysis techniques for dependability. event tree analysis (ETA). IEC 62502:2010.

[24] Procedures for performing a Failure Mode, Effects and Criticality Analysis. *Department of Defence of the USA*, 1980.

[25] IEC IEC. Fault Tree Analysis (FTA). IEC 61025:2007, 2006.

[26] J.S. Dodgson, M. Spackman, A. Pearman, and L.D. Phillips. Multi-criteria analysis: a manual. 2009.

[27] Free Web-based FTA project website. http://www.fault-tree-analysis-software.com. Accessed: 07.05.2016.

[28] Expert Choice project website. http://www.expertchoice.com. Accessed: 13.05.2016.

[29] Open FTA project website. http://www.openfta.com. Accessed: 13.05.2016.

[30] GeNIe project website. http://www.dslpitt.org/genie. Accessed: 05.05.2016.

[31] CAFTA project website. http://www.epri.com. Accessed: 21.05.2016.

[32] BowTieXP project website. http://www.cgerisk.com/software. Accessed: 20.05.2016.

[33] Ram Commander project website. http://www.aldservice.com/en/fmea/fmea-and-fmeca.html. Accessed: 17.05.2016.

[34] HAZOP Manager project website. http://www.lihoutech.com. Accessed: 18.05.2016.

[35] InfraRisk project website. http://www.infrarisk.com. Accessed: 09.05.2016.

[36] PHAWorks project website. http://www.primatech.com/software/phaworks. Accessed: 19.05.2016.

[37] Reliability Workbench project website. http://www.isograph.com/software/reliability-workbench. Accessed: 20.05.2016.

[38] THESIS project website BowTie. http://www.absconsulting.com/thesis. Accessed: 12.05.2016.

[39] Xfmea project website. http://www.xfmea.reliasoft.com. Accessed: 22.05.2016.