sustainability

Article

Risk Management in Critical Infrastructure—Foundation for Its Sustainable Work

Andrzej Bialas

Institute of Innovative Technologies EMAG, 40-189 Katowice, Leopolda 31, Poland; andrzej.bialas@ibemag.pl; Tel.: +48-32-200-77-00; Fax: +48-32-200-77-01

Academic Editors: Adam Jabłoński, Giuseppe Ioppolo and Marc A. Rosen
Received: 24 October 2015; Accepted: 26 February 2016; Published: 4 March 2016

Abstract: The paper concerns research related to the European project CIRAS and presents a validation experiment with the use of a risk management tool adapted for critical infrastructures. The project context and state of the art are discussed. The adaptation of the risk management tool is performed according to previously elaborated requirements which consider interdependencies, cause-consequences analysis, risk measures and risk register implementation. A novel structured risk management method was proposed how to deal with internal and external impacts of a hazardous event which occurred in the given CI. The method is embedded into the critical infrastructure resilience process. These requirements can be implemented on the ready-to-use software platform for further experiments. The experimentation results are used as the input for CIRAS. The discussed tool can be applied as the risk reduction component in the CIRAS Tool, and the validation process presented here is the basis to elaborate two project use cases.

Keywords: critical infrastructure; risk management; bow-tie concept; software tool; interdependencies

1. Introduction

The paper concerns the risk management issue in critical infrastructures. Today's societies are based on products and services provided by large-scale technical infrastructures of such sectors as energy, oil, gas, finances, transport, telecommunications, health, *etc.* These infrastructures, when disrupted or destroyed, have a serious impact on health, safety, security or well-being of the society or effective functioning of governments and/or economies, therefore they are called critical infrastructures (CIs). Smooth functioning of the CIs builds right relationships between the citizens and governments. Modern societies are very sensitive to any disturbances in critical infrastructures. The CI disturbances or damages hamper the economic growth, social prosperity and sustainable development of our civilization. For this reason, it is very important to mitigate any negative impact on critical infrastructures. Risk management, which plays the key role in the CI protection, still remains a challenge due to many unresolved problems. This was the author's motivation to undertake research in this field.

CI is identified as a very complex socio-technical system, sometimes called a system of systems. The system of systems (SoS) consists of multiple, heterogeneous, distributed, occasionally independently operating systems embedded in networks at multiple levels, which evolve over time [1]. To function properly, CIs include many diversified components (technological, IT hardware, software, environmental, personal, organizational) and complex processes interrelated with other processes across different economy sectors.

In such environments different kinds of threats and hazards may occur, such as: natural disasters and catastrophes, technical disasters and failures, espionage, international crime, physical and cyber terrorism. To avoid disturbances in CIs and to minimize possible consequences of threats, critical infrastructure protection (CIP) programmes are implemented, which specify a consistent set of diversified security measures applied for the given CI: technical, organizational and procedural. The measures should properly affect the identified risk. The measures selection is based on risk management principles.

1.1. Resilience and Risk Management in Critical Infrastructures

Risk management is a continuous process including the identification, analysis, and assessment of potential hazards in a system or hazards related to a certain activity. Based on the recognized risk picture, the risk control measures are proposed to eliminate or reduce potential harms to people, environment, or other assets. The risk management process encompasses risk monitoring and communication. ISO 31000 [2] is the basic risk management standard. Examples of the most recognized risk management methods and techniques are included in IEC 31010 [3].

The risk management issue in critical infrastructures has a specific character because CIs are very complex, diversified and there are mutual interrelations between different infrastructures. Because of relationships between infrastructures, the state of each infrastructure influences or is correlated to the state of the other. They are called interdependencies [4–7] and can be divided to four categories: physical, cyber, geographical and logical interdependency. The effects of an incident may propagate across CIs with dire consequences. The paper takes into account interdependencies, however the complex interdependencies issues are not the basic topic of the paper.

Well-secured CIs can resist external and internal disturbances and are able to work on an acceptable efficiency level even when these disturbances occur. To improve the CI resilience is the main objective of CI stakeholders. The CIs resilience is an effective, sustainable use of critical infrastructures by stakeholders to perform tasks for the economy, government and citizens. "The concept of resilience can be seen as a superset in which typical risk assessment is a complementary part" [6]. The following activities leading to the CI resilience are proposed in this publication:

- preparing the CI specification based on the structural analysis—the most critical elements, the most vulnerable points, dependencies and interdependencies are identified; please note: dependency defines a unidirectional relationship between infrastructures, while interdependency defines a bidirectional relationship;
- running the dynamic analysis to identify the most dangerous risk scenarios—generally the subject of analysis or simulation are: propagation of dire effects of CIs phenomena, identification of the threats impact, analyses of common failures, system response to a failure or an incident, recovery process, *etc.*
- the most dangerous risk scenarios, prioritized, are taken into account later during the risk management process.

1.2. Research Related to the CIRAS Project

The critical infrastructure protection is recognized in European Union (EU) as one of the key issues. The CIP related needs on the EU and member-state levels are expressed in the European Council (EC) Directive [8]. It specifies rules of the CI identification based on the casualties, economics and public criteria, as well as the risk analysis issues and management programmes. In 2006 the European Programme for Critical Infrastructure Protection (EPCIP) was issued. A revised version is included in the EC document [9].

The CIP programmes encompass diversified (physical, technical, organizational) countermeasures, applied on the basis of risk. The risk management issue in CIs is extremely important and has not been fully solved so far. There are several dozen EU or worldwide CIP R&D projects, either already completed or currently running (Framework Programmes—FP6 and FP7, Horizon 2020, The Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme—CIPS). Most of them deal with risk management methodologies and their supporting tools. The CIRAS (Critical Infrastructure Risk Assessment Support) project [10] is one of them.

The paper concerns a preliminary research of the CIRAS project. CIRAS was launched by the international consortium comprising:

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

The CIRAS objective is to develop a methodology and tool to support decision makers in the security measures selection for critical infrastructures. The CIRAS approach to security management in critical infrastructure protection takes into account typical CI phenomena like interdependencies, cascading and escalation of incident impacts.

The novelty of the CIRAS approach lies in a holistic assessment of all aspects of CIs security measures, including the expected risk reduction and its cost, financial benefits, as well as many vague socio-political factors to be considered in the security planning process. To select the right security measure (countermeasure) according to the CIRAS methodology, 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 vague factors in the project are called "qualitative criteria".

To support the decision making process, these issues are solved by three separate pillars, implemented as the key software components of the CIRAS Tool:

- a Risk Reduction Assessment (RRA) component,
- a Cost-Benefit Assessment (CBA) component,
- a Qualitative Criteria Assessment (QCA) component.

The CIRAS approach is based on the methodology elaborated in the FP7 (Seventh Framework Programme) ValueSec project [11]. Both the ValueSec and CIRAS methodologies support the decision making process using these three pillars, but the domains of applications and the pillars implementation approaches are different. Please note that the critical infrastructure domain, due to its specific phenomena caused by interdependencies, is much more complex than the ValueSec application domains (mass event security, mass transportation security, communal security planning, air transport security, protection against cyber-attacks on a smart grid). The CIs complexity influences the shape of the RRA, CBA and QCA components as well as the components collaboration within the framework implemented in the CIRAS Tool.

Research was performed by the project team members to elaborate the CIRAS methodology and to design and implement it in the CIRAS Tool. The project uses four main inputs:

- an extensive review of the state of the art of risk management, cost-benefits, and decision support methodologies and tools, especially those for critical infrastructure protection,
- conclusions from the CIRAS stakeholders' workshops,
- experience gained by the CIRAS team members from the ValueSec project, particularly concerning the pillars implementation.

This paper deals with a part of this research focused on the RRA component implementation. The problems addressed are:

- how to find and adapt a tool to be the RRA component,
- how to develop a new tool, according to the project requirements, if the above is not possible.

The RRA component should satisfy the project requirements:

- the basic requirements for CI risk management tools identified in [12], and
- the project specific requirements identified by the consortium with the stakeholders' help, *i.e.,* RRA should be able to properly manage the risk in critical infrastructures by selecting security measures with the right cost-benefits parameters and free of vague restrictions, should be able to easily integrate with other CIRAS components of the tool, and should be relatively simple.

The research presented in this article was focused on the feasibility of the OSCAD-based RRA. OSCAD (proprietary name) [13] is a ready-made software platform to be adapted and configured to different domains of application. The CIRAS consortium considered it a candidate for the RRA component.

This paper presents research which allowed to assess whether OSCAD can fulfil the project requirements and whether it can be used as the RRA component of the CIRAS Tool.

As a result of the experiment a novel approach is proposed how to deal with internal and external impacts of a hazardous event which occurred in the given CI. It allows to distinguish three main categories of impacts: direct CI damages, event escalation by breaching internal security barriers and causing secondary damages, event escalation from the given CI on the dependent CIs. The elaborated structured risk management method for critical infrastructures is embedded into the CI resilience process. The method is implemented in the OSCAD-CIRAS experimental tool. The tool allows to assess critical infrastructure damages in several time horizons and to assess several security measures alternatives with respect to the risk reduction and cost-benefits parameters.

1.3. State of the Art

During the CIRAS project a review [4,14–16] of laws, standards, frameworks, methods and tools was performed and summarized in [17].

The review confirms that the risk management issue in critical infrastructures is much more complicated than in other domains of application. It is specific due to the following factors:

- unprecedented CIs complexity, even when compared to very large business organizations or technical facilities,
- continuous evolution and enhancement of critical infrastructures,
- mutual interrelations between different infrastructures (interdependencies),
- problem diversity—the risk management issue is related to many other issues, like: complex systems architectures, interdependencies, complex interactions, behavioral aspects, reliability theory, vulnerability analysis, resilience, emerging behavior,
- knowledge of architecture and functioning principles of complex systems is fuzzy and the data incomplete,
- different abstraction levels applied to manage CIs and cross-sectoral relations,
- high-impact and low-probability events may occur,
- increased needs for communication and coordination among the CI operators.

The review shows that a significant number of risk assessment methods and tools can be applied in the critical infrastructure domain. Usually, they were developed for different organizations to solve their technical or organizational risk-related problems within the limited environments, and initially they were not dedicated to critical infrastructures. Later, many of them were adapted to CI needs. Usually, they are very mature, sector-specific, represent the detailed approach to the risk issue and can be easily applied on the lower level of the CI hierarchy. Their basic features are: threats and vulnerabilities categorization and identification, and the evaluation of impacts. Only few tools are able to operate on the higher CI hierarchy level. This group is still extended.

Risk management methods are very diverse and their shapes and abstraction levels depend on the levels of CIs where they are used. For example, a CI operator needs a more detailed approach than a policy maker working on the system-of-systems level, and the tool implemented for the CI asset level is more detailed than the tool for the CI operator. Generally, a higher CI level requires a more general approach.

The asset level methods and tools are adapted to higher levels but this generates problems how to handle cross-sectoral dependencies. This issue has been examined by many researchers. The challenge is how to adapt risk assessment methods used on the CI lower level to the higher level (complex system) needs.

The interdependency methodologies, supporting risk management methodologies, are growing in a parallel manner to each other. They are based on modeling and simulation techniques [6]. They are crucial to ensure the CI resilience, and in this sense they also support risk management methodologies. Many general purpose risk managers are not able to use input from the interdependencies analysis.

The review confirms that it is very hard to point out a tool which can be applied in the CIRAS Tool. There are many tools which satisfy certain basic requirements and are able to assess and manage the risk in critical infrastructures, however they do not address sufficiently the CIRAS project requirements, especially those related to the following issues:

- cross-sectoral risk management,
- cooperation with the CBA and QCA components (using cost, benefit, and vague factors in the risk management process),
- operations on the alternative packages of countermeasures,
- easy integration (connectivity, source code availability, commonly used technologies).

During the review the OSCAD was analyzed in comparison with other tools. This is a general purpose tool (software platform) which, when developed, was not intended especially for CIs. The tool is very flexible. Its functionality satisfies the basic CI risk management requirements and there is also a chance to meet the CIRAS project requirements. The paper presents research allowing to explain these issues.

1.4. Paper Content

The paper presents the following: a risk management study (Section 2) including the experimentation platform requirements, risk assessment method description, implementation of the requirements on the ready-made software platform, experiment plan workout, and the experimentation process. Section 3 includes the experimentation summary, and Section 4—the paper summary.

2. Risk Management Case Study

The case study is focused on the analysis how particular project requirements can be fulfilled by the OSCAD-based RRA, and shows step by step how this component has been developed according to the proposed risk management method.

2.1. General Requirements for Experimental Risk Manager

Basic requirements for the CI risk management tool were discussed in [12]. Summarizing this discussion, the following requirements were proposed:

(1) The CI specific phenomena, such as common cause failures, cascading and escalating effects, as well as interdependencies between CIs [5] should be considered in the risk management process.

(2) The bow-tie risk concept [4,18] is recommended for implementation as the conceptual model of the risk assessment tool. It embraces both causes of the given hazardous event and its diversified and multidirectional consequences.

(3) The CI risk register, as the managed inventory of hazardous events used in CIP programmes, should include at a minimum: related hazards/threats, corresponding hazardous event, probability of the event and its consequences. There are some other data associated with the risk register items, such as assets, societal critical functions, vulnerabilities, countermeasures, *etc.*

(4) Risk measures and the assessment process should be defined for the given application domain. A common method is to assess the likelihood (probability, frequency) of a hazardous event, and to assess the consequence severity in different dimensions. Risk is the function of both, usually expressed by a risk matrix.

The following issues are relevant with respect to the CIRAS project requirements:

(1) The RRA component should be able:

- to assess risk before a measure is implemented and reassess the risk for a certain number of security measures alternatives considered for implementation,
- to consider cross-sectoral dependencies,
- to take into account cost-benefits factors and qualitative criteria dealing with the security measures alternatives.

(2) RRA should exchange information with the CBA and QCA components during the decision process dealing with the security measures selection.

(3) RRA component should consider the CI specific phenomena, analyze causes and impacts of hazardous events, and manage the risk register data.

The data exchange between the components cannot be fully demonstrated, because the components have not been integrated yet.

2.2. Implementation Platform

The OSCAD software platform was chosen as the research platform [13]. Initially, this platform was designed to support business continuity management in accordance with ISO 22301 and information security management in accordance with ISO/IEC 27001. The software can identify different disturbances of business processes and/or breaches of information assets in different companies and organizations. OSCAD helps to reduce their losses, caused by incidents, and can support the recovery process too. OSCAD is an open and flexible tool, therefore it can be adapted to protect assets or processes in different application domains, e.g.,: flood protection [19], railway safety management systems [20] and coal mining [21]. The risk management functionality of OSCAD is of key importance to the protection of critical infrastructures.

OSCAD is equipped with risk assessment tools which analyze the causes of hazardous events (pairs: threat-vulnerability with respect to the asset or process):

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

AORA is used to calculate risk levels of critical assets and risk reduction levels after security measures implementation. The analysis is conducted for the given asset with the related threats which exploit the asset vulnerabilities. The impact and likelihood values of threats and the current values of security measures are used to determine the inherent risk level. After applying new security measures, the risk level is reassessed and the gain in risk reduction can be determined. The PORA analysis is similar, however, it is focused on causes of the processes disturbances.

Moreover, OSCAD is equipped with tools which are able to analyze multidimensional impacts of hazardous events:

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

ABIA is used to assess possible impacts of assets loss for an organization (here CI). The assessment is made according to different loss categories such as: fatalities and qualitative costs (political, social, legal), damages of infrastructure, revenue loss, external costs in other organizations. High loss levels indicate that security measures should be applied to reduce risk. PBIA is similar, however it concerns impacts for an organization (here CI), when the processes are disturbed.

As a result of the adaptation, the OSCAD-CIRAS tool prototype was developed [22]. The OSCAD adaptation performed by the author encompasses the elaboration of the domain specific system dictionaries, e.g., assets, threats, vulnerabilities, countermeasures, risk measures, software configuration, *etc.* OSCAD-CIRAS can be used as an experimental tool to acquire knowledge and experience which will then be used as an input to the CIRAS project.

2.3. Requirements Implementation on the Ready-Made Software Platform

The paper extends the works presented in [23] and deals with risk management experiments conducted with the use of the ready-made open OSCAD software platform, which was adapted to fulfill the basic CIs requirements with respect to risk management. It was assumed that one OSCAD-CIRAS instance, at minimum, can be implemented in one infrastructure. OSCAD-CIRAS is able to co-operate with similar systems working in other infrastructures. This co-operation is focused mainly on communication during the risk management process [2]. The presented experiment concerns the railway transport CI co-operating with the electricity CI. To simplify the experiment, both CIs are implemented in one OSCAD-CIRAS.

Risk management items implemented in OSCAD-CIRAS comply with the taxonomy included in the EC Directive [8], which distinguishes two groups of CIs: ECI (European CI), embraced by the EC Directive, and others (non-ECI). Assets and other items belonging to the given CI are preceded by a label being the abbreviation of a CI name: Ele (Electricity), Oil (Oil), Gas (Gas), RoT (Road Transport), RaT (Rail Transport), AiT (Air Transport), IWT (Inland Waterways Transport), Sea (Ocean and Short-Sea Shipping and Ports).

Based on the discussed below requirements a structured risk management method was developed and presented in Subsection 2.4 (Figure 6).

2.3.1. Interdependencies and CI-specific Issues—Input from Resilience Analysis

Critical infrastructure is a complex socio-technical system which interacts with similar systems working in other application domains. These interactions are considered on different layers (e.g., on the CI operator layer, sector layer, intra sector layer) [6].

The risk management process should be extended beyond a single infrastructure, because a hazardous event occurring within the given CI impacts this CI but may also cause problems for other interacting CIs, and similarly, the given CI may be impacted by hazardous events which occurred in external CIs. The risk management process should be able to consider interdependencies. This issue still remains a challenge.

OSCAD-CIRAS does not have a specialized functionality to analyze resilience, including interdependencies, and for this reason it should be supported externally to get the relevant information. The resilience analysis, producing necessary input, precedes and supports the risk assessment process.

The first kind of input concerns information about interdependencies obtained from the resilience analysis, more specifically from its static part focused on the system of systems analysis. During the dependency analysis [6], the following factors are taken into account:

- shared resources, shared services,
- common assets, components, policies,
- common causes of potential impacts, like: fire, flooding, virus attack, network attack, communication unavailability.

Diagrams, called dependency networks are obtained in the course of the interdependency analysis. The dependency network diagram represents homogenous dependencies between input and output. It will be shown in Figure 1 by an example related to the CIs presented later in the case study. The left part presents a scheme of collaborating infrastructures—rail transport (RaT), electricity (Ele) and others.

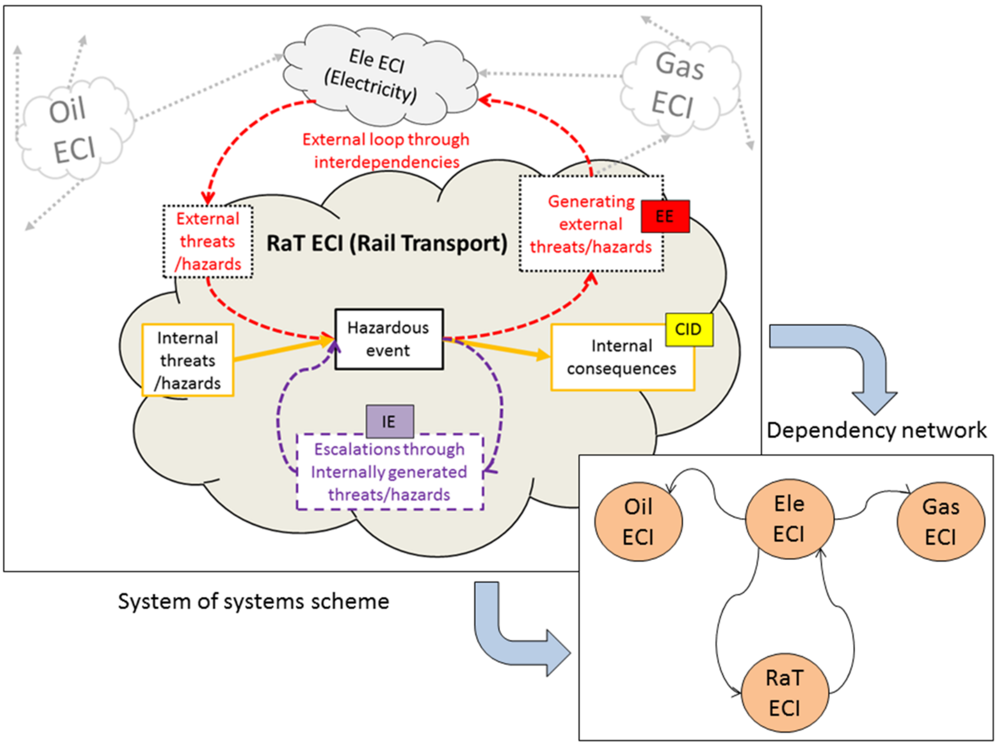

Ele ECI (Electricity)
Oil ECI
Gas ECI
External loop through interdependencies
External threats /hazards
RaT ECI (Rail Transport)
Generating external threats/hazards
EE
Internal threats /hazards
Hazardous event
CID
Internal consequences
IE
Escalations through Internally generated threats/hazards
Dependency network
System of systems scheme
Oil ECI
Ele ECI
Gas ECI
RaT ECI

Figure 1. Two collaborating infrastructures (RaT, Ele) as the validation context—system-of-systems scheme and dependency network diagram.

The example of a dependency network, presented in the right part of Figure 1, shows that RaT ECI depends on Ele ECI and *vice versa*, and, additionally the Gas and Oil infrastructures depend on Ele.

The objective of the method presented here is to distinguish three main categories of impacts (Figure 1):

- CID (CI Degradation) category—different kinds of damages within the given CI;
- IE (Internal Escalations)—new internally generated threats or new or increased vulnerabilities which influence the considered CI, caused by the hazardous event; this allows to consider secondary effects of the given event;
- EE (External Escalations)—generated threats which impact the external CIs, or new or increased vulnerabilities in the external CIs, caused by the hazardous event.

Please note that the EE category impacts propagate across infrastructures due to existing dependencies. For example, an impact can propagate from RaT to Ele, from Ele to Gas and to Oil.

The second kind of input from the resilience analysis concerns information about critical risk scenarios. Please note that the paper presents the typical approach to risk assessment, including the identification and prioritization of threats, identification of vulnerabilities relevant to these threats and the impact assessment. This is a relatively simple approach, but it can be unsuccessful if all possible scenarios are taken into account in the risk management process—only the most critical scenarios are selected. The dynamic resilience analysis [6], preceding the risk management process, returns these very critical scenarios, such as the CI collapsing scenarios. It is assumed that to identify these scenarios, structural analyses of the collaborating CIs and dynamic resilience analyses were made.

It is assumed for the presented method and tool that the critical scenarios and interdependencies are known prior to initiating the risk assessment.

Apart from critical scenarios and interdependencies, the resilience analysis provides information about the most critical nodes, the most vulnerable nodes, strength of coupling between the nodes, and a lot of other information useful in the risk management process.

2.3.2. Bow-Tie Risk Assessment Concept Implementation

The bow-tie conceptual model [18] embraces both multiple and complex causes of the given hazardous event and its diversified and multidirectional consequences (impacts). It means that it is composed of two elements: causes analysis and consequences analysis. These features are the basis for the method presented here.

The consequences analysis part of the bow-tie model is implemented on the ABIA or PBIA basis. Later, they are called BIA (in short). For a given asset (process), which is under the hazardous event, impact can be assessed with the use of the loss matrix.

In OSCAD-CIRAS two causes analyses are possible: AORA or PORA, later called RA (in short). AORA allows to analyze each threat-vulnerability pair which can breach the given asset, while PORA does the same with respect to the given process. First, the BIA type analysis is performed, next the RA analysis (Figure 6).

2.3.3. Critical Infrastructure Risk Register and Related Issues

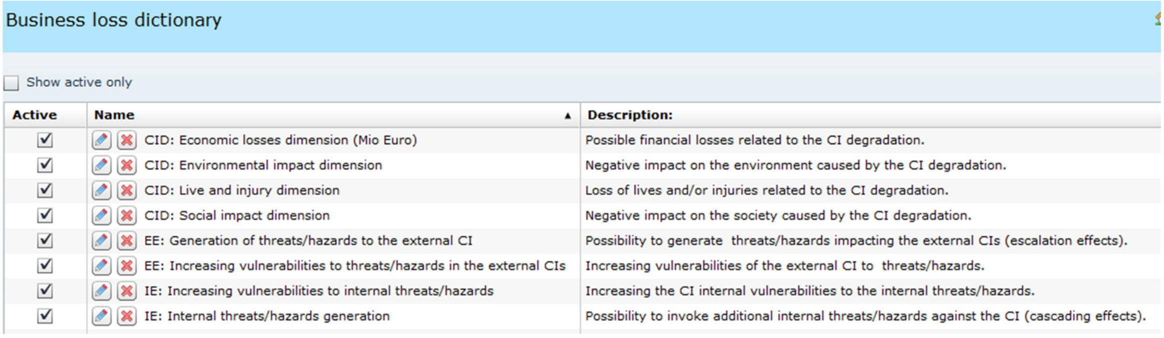
OSCAD-CIRAS distinguishes primary assets which are to be protected and secondary assets related to them. For example, RaT:Node, representing the railway node, can be considered a primary asset. It can be impacted when a hazardous event occurs, for this reason it should be protected. This complex asset embraces many diversified secondary assets (rails, level crossings, buildings, signaling equipment, ICT equipment, people, countermeasures, *etc.*).

The asset destruction implies multidirectional impacts on the CI where the event occurs and on other, dependent infrastructures. This is a subject of the BIA analysis. For the given protected asset there are threats and vulnerabilities considered, because they imply hazardous events which may cause full or partial damages on an asset. This is a subject of the RA analysis.

The risk register contains information about assets (and/or processes) impacted during a hazardous event, consequences, event frequency, threats, vulnerabilities, and assessed multidirectional impacts.

2.3.4. Risk Measures and the Assessment Process

The measures of multidimensional impacts of the hazardous event, used during BIA analyses, encompass three above mentioned main categories of impacts (CID, IE, EE). For each of them several loss categories are defined (four for CID, two for IE, and two for EE—eight categories in total)—see Figure 2. All categories and their number are user-defined.



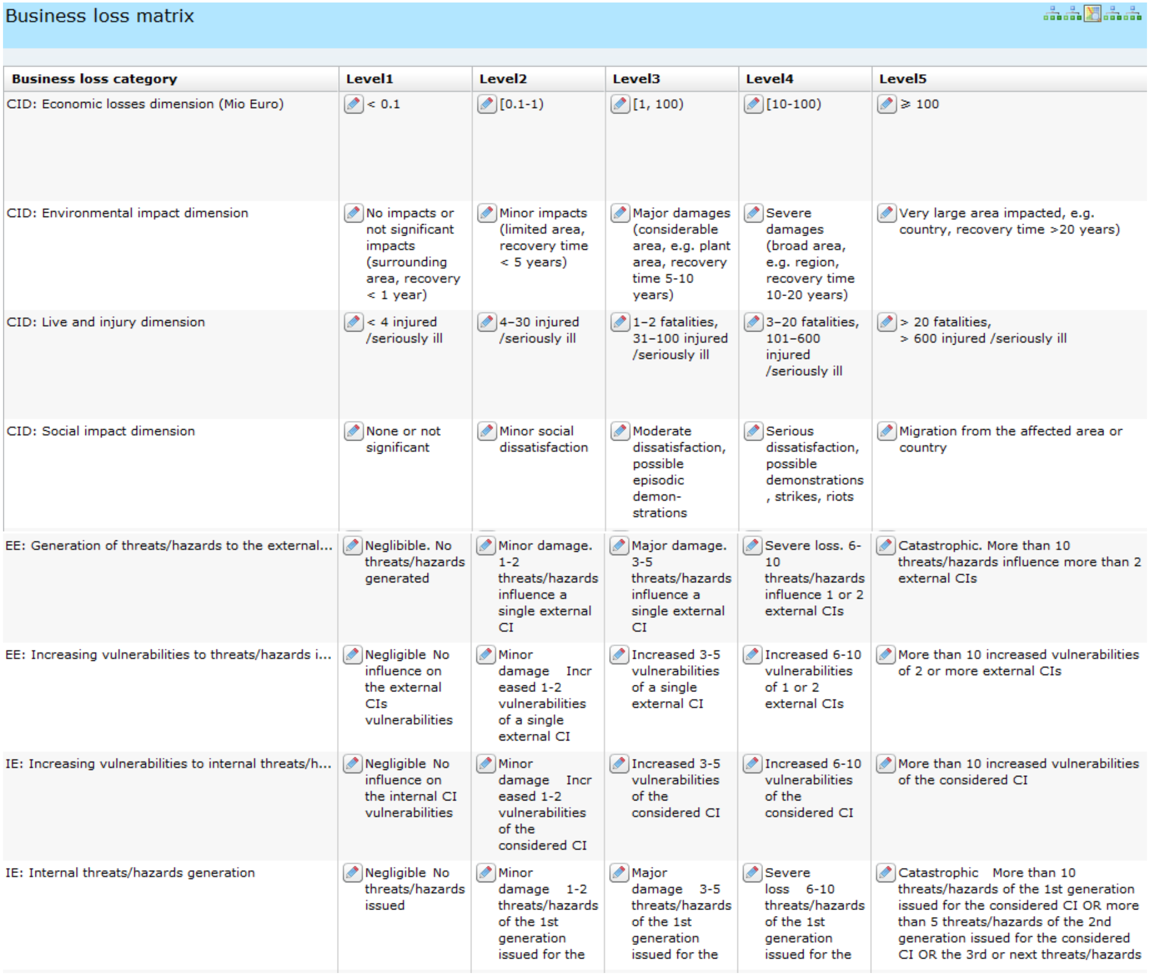
Business loss dictionary

☐ Show active only

Active	Name ▲	Description:
☑	CID: Economic losses dimension (Mio Euro)	Possible financial losses related to the CI degradation.
☑	CID: Environmental impact dimension	Negative impact on the environment caused by the CI degradation.
☑	CID: Live and injury dimension	Loss of lives and/or injuries related to the CI degradation.
☑	CID: Social impact dimension	Negative impact on the society caused by the CI degradation.
☑	EE: Generation of threats/hazards to the external CI	Possibility to generate threats/hazards impacting the external CIs (escalation effects).
☑	EE: Increasing vulnerabilities to threats/hazards in the external CIs	Increasing vulnerabilities of the external CI to threats/hazards.
☑	IE: Increasing vulnerabilities to internal threats/hazards	Increasing the CI internal vulnerabilities to the internal threats/hazards.
☑	IE: Internal threats/hazards generation	Possibility to invoke additional internal threats/hazards against the CI (cascading effects).

Figure 2. Event multidirectional impacts measures (CID, IE, EE) in OSCAD-CIRAS [23].

For all loss categories the same number of loss levels are defined (here: five): from Level 1 (the lower level) to Level 5 (the upper). Each level gets a clear interpretation. This way the loss matrix, *i.e.*, the basic BIA tool, is defined and shown in Figure 3. The "CID: Economic losses dimension (Mio Euro)", "CID: Live and injury dimension" and "CID: Social impact dimension" loss categories were defined according to the propositions from [4], others by the author.



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 demonstrations	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 Increased 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 Increased 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. Business loss matrix used for BIA analyses.

The BIA analyzer operates on three main categories of impacts (CID, IE, EE) and their loss categories shown in Figure 3. For each CID, IE, EE impact category the worst case value of loss categories is selected as a partial BIA result, marked as CIDval, IEval, and EEval. The BIA aggregated result, depending on the chosen calculation model, is defined by very simply functions:

- for the worst case model (WCM):

$$\text{BIAvalue} = \text{Worst Case of}\,(\text{CIDval, IEval, EEval}) \tag{1}$$

- for the total model (TM):

$$\text{BIAvalue} = \text{CIDval} + \text{IEval} + \text{EEval} \tag{2}$$

- for the product model (PM):

$$\text{BIAvalue} = \text{CIDval} \times \text{IEval} \times \text{EEval} \tag{3}$$

In the example discussed in the paper, BIA considers three main categories of losses (CID, IE, EE) and five levels of losses (1 to 5). It means that the range of the BIA aggregated results can be: 1 to 5 for WCM, 3 to 15 for TM, and 1 to 125 for PM. The kind of the calculation model is configurable. The WCM model is chosen due to its simplicity.

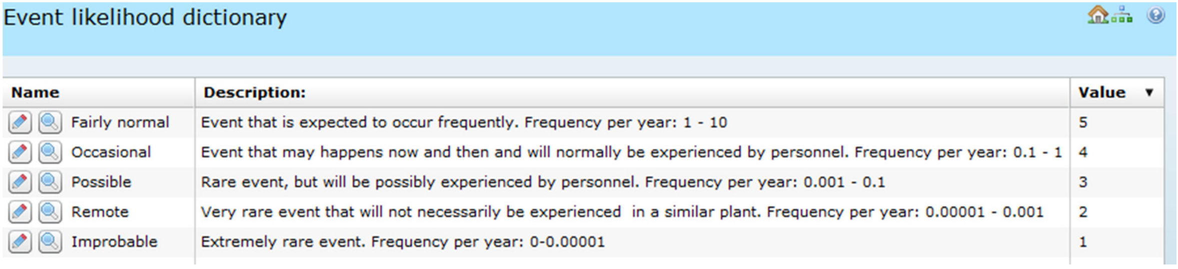
For the RA analysis the risk value is expressed as:

$$\text{Risk} = \text{Event likelihood} \times \text{Event consequences} \tag{4}$$

The RA "Event likelihood" measures, based on [12,18], are presented in Table 1, and their implementation in the OSCAD-CIRAS dictionary is shown in Figure 4. The number of likelihood measures is fully configurable – here five levels are assumed.

Table 1. Event likelihood measures.

Level of measure	Frequency per year	Description
Fairly normal 5	1–10	Event that is expected to occur frequently
Occasional 4	10^{-1}–1	Event that may happen now and then and will normally be experienced by personnel
Possible 3	10^{-3}–10^{-1}	Rare event, but will be possibly experienced by personnel
Remote 2	10^{-5}–10^{-3}	Very rare event that will not necessarily be experienced in a similar plant
Improbable 1	0–10^{-5}	Extremely rare event



Event likelihood dictionary

Name	Description:	Value ▼
Fairly normal	Event that is expected to occur frequently. Frequency per year: 1 - 10	5
Occasional	Event that may happens now and then and will normally be experienced by personnel. Frequency per year: 0.1 - 1	4
Possible	Rare event, but will be possibly experienced by personnel. Frequency per year: 0.001 - 0.1	3
Remote	Very rare event that will not necessarily be experienced in a similar plant. Frequency per year: 0.00001 - 0.001	2
Improbable	Extremely rare event. Frequency per year: 0-0.00001	1

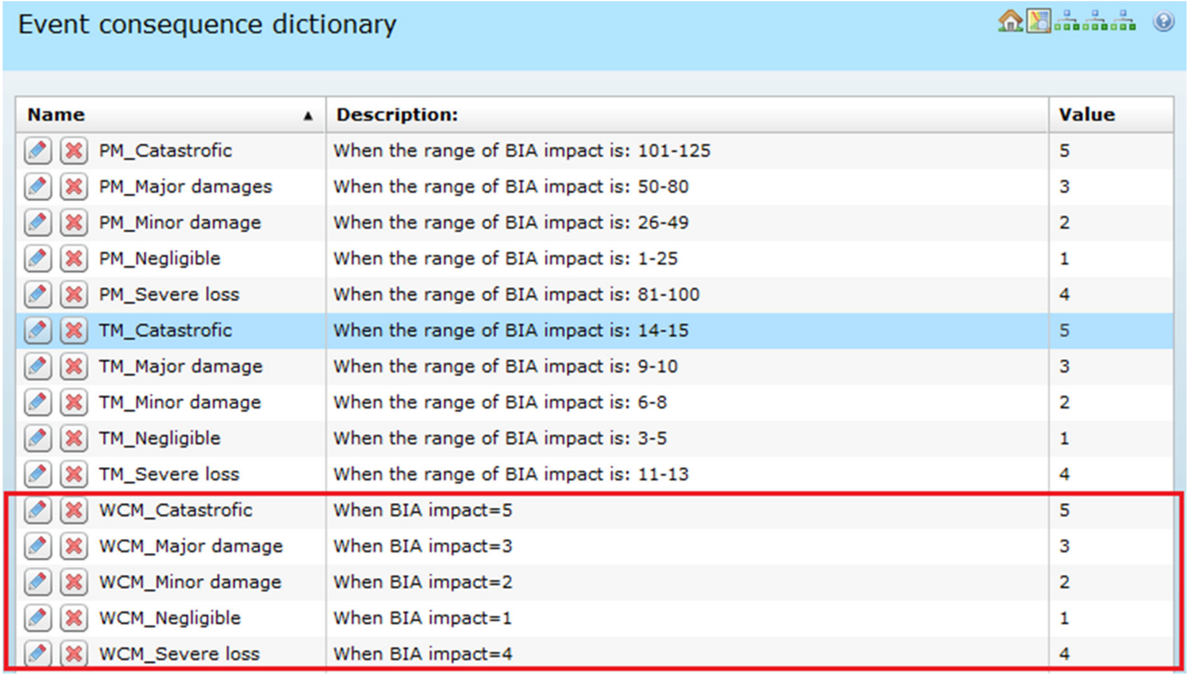
Figure 4. Event likelihood measure in OSCAD-CIRAS [23].

The RA "Event consequences" measures are derived from the loss matrix categories. It is possible because the BIA analysis precedes the RA one, and the measures of both are harmonized. Table 2 is an example of mapping the BIA aggregated results (BIAval) on the RA consequences measures with respect to the used calculation model.

Table 2. The RA consequences derived from BIA aggregated results depending on the used BIA calculation model (an example).

RA consequences	Mapping the BIA Aggregated Results on the RA Consequences for Different Calculation Models		
	for Worst Case Model (WCM)	for Total Model (TM)	for Product Model (PM)
Negligible damage 1	1	3–5	1–25
Minor damage 2	2	6–8	26–49
Major damage 3	3	9–10	50–80
Severe loss 4	4	11–13	81–100
Catastrophic 5	5	14–15	101–125

The contents of Table 2 are implemented in the consequences dictionary (Figure 5). For further BIA examples the measures with the "WCM_" prefixes are used, and the RA consequences are measured in the range from 1 to 5.



Event consequence dictionary

Name ▲	Description:	Value
PM_Catastrofic	When the range of BIA impact is: 101-125	5
PM_Major damages	When the range of BIA impact is: 50-80	3
PM_Minor damage	When the range of BIA impact is: 26-49	2
PM_Negligible	When the range of BIA impact is: 1-25	1
PM_Severe loss	When the range of BIA impact is: 81-100	4
TM_Catastrofic	When the range of BIA impact is: 14-15	5
TM_Major damage	When the range of BIA impact is: 9-10	3
TM_Minor damage	When the range of BIA impact is: 6-8	2
TM_Negligible	When the range of BIA impact is: 3-5	1
TM_Severe loss	When the range of BIA impact is: 11-13	4
WCM_Catastrofic	When BIA impact=5	5
WCM_Major damage	When BIA impact=3	3
WCM_Minor damage	When BIA impact=2	2
WCM_Negligible	When BIA impact=1	1
WCM_Severe loss	When BIA impact=4	4

Figure 5. Event consequences measures for different BIA calculation models implemented in the system dictionaries.

2.4. Risk Assessment Method Implemented in OSCAD-CIRAS

The risk assessment method proposed in the paper takes into account previously specified requirements, including the CIRAS RRA requirements, and the abilities of the OSCAD software platform [13].

This method is embedded into the process, which ensures the resilience of the given CI, e.g., RaT ECI. The general scheme of the risk assessment process is presented in Figure 6. The risk assessment processes run concurrently in each of the collaborating infrastructures.

The risk assessment process running in the given CI gets from the resilience analysis a set of basic critical risk scenarios, dependency network diagram and any other risk-relevant information. There are three risk scenarios repositories:

- for basic risk scenarios, obtained from the resilience analysis;
- for externally generated hazards for the given CI; the EE-related risk scenarios are identified outside the CI;
- for internally generated hazards for the given CI, causing secondary impacts (the IE-related risk scenarios).

The assessment process starts from the basic scenario of the highest criticality obtained from the resilience analysis. First, BIA (a consequences analysis) is performed, and its results encompass the following:

- CI internal damages (CID)—CIDval,
- generated internal hazards (IE)—IEval,
- generated external hazards (EE)—EEval.

The aggregated BIA result is identified as the function of CIDval, IEval, EEval, according to the calculation model (here, for WCM: BIA result is the maximal value of CIDval, IEval, EEval).

Next, RA (a causes analysis) is launched to identify threat/vulnerability pairs leading to the hazardous event. Their likelihood is assessed. OSCAD requires the event consequences input as well. In this case, the BIA-derived value is introduced by default. During the risk management process, the risk is reassessed after the countermeasure implementation (the risk after), and if the countermeasure affects the event consequences, e.g., data backup, the default value (from BIA) can be corrected manually.

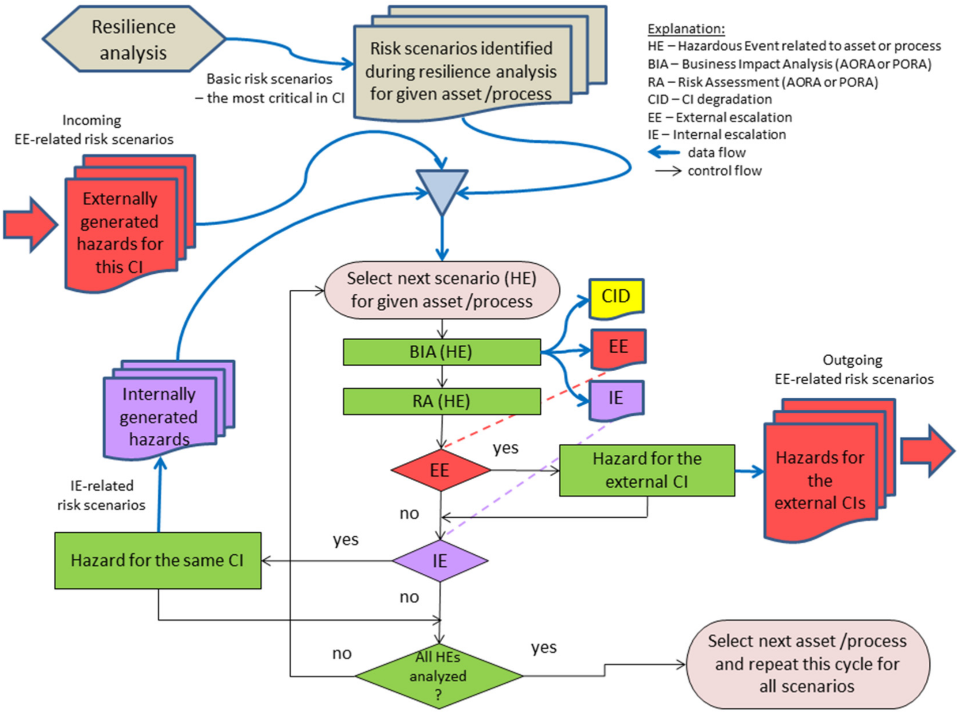

Resilience analysis
Basic risk scenarios – the most critical in CI
Risk scenarios identified during resilience analysis for given asset /process
Explanation:
HE – Hazardous Event related to asset or process
BIA – Business Impact Analysis (AORA or PORA)
RA – Risk Assessment (AORA or PORA)
CID – CI degradation
EE – External escalation
IE – Internal escalation
data flow
control flow
Incoming EE-related risk scenarios
Externally generated hazards for this CI
Select next scenario (HE) for given asset /process
BIA (HE)
RA (HE)
CID
EE
IE
Outgoing EE-related risk scenarios
Hazards for the external CIs
Internally generated hazards
IE-related risk scenarios
EE
yes
Hazard for the external CI
no
yes
Hazard for the same CI
IE
no
no
All HEs analyzed ?
yes
Select next asset /process and repeat this cycle for all scenarios

Figure 6. General scheme of the risk assessment process in a critical infrastructure.

After completing the BIA/RA pair, its results are analyzed. When the EE impact occurs, the warning about the generated hazard (embracing causes and consequences: new threats and/or increased vulnerabilities, external impact, risk and impact values, *etc.*) is formed as the EE-related risk scenario and sent to the potentially impacted CI to be considered in the risk assessment process. The risk communication process (an important part of the whole CIs risk management framework) is responsible for exchanging such warnings between the collaborating and dependent infrastructures. This EE-related risk scenario is placed in the external hazards repository of the warned CI.

Next, the IE impact is analyzed. When the impact occurs, the IE-related risk scenario is defined (a record embracing the causes and consequences: new threats and/or increased vulnerabilities within the considered CI, secondary impact, risk and impact values, *etc.*) and added to the internal hazards repository. Moreover, this newly generated internal hazard is assessed (BIA-RA). 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, which is placed in the repository and then analyzed (BIA/RA). These analyses focus on internal escalation and are repeated until no internal secondary effects occur. Then, the next basic risk scenario is taken into account and analyzed in the same way. When all basic scenarios are finished, next the hazards externally generated for this CI are analyzed similarly as the basic ones. The whole process stops when all basic and externally generated for this CI are analyzed.

2.5. Scenario of the Validation Experiment

The validation deals with the railway and energy collaborating infrastructures and encompasses one basic risk scenario: a catastrophe in an important railway node. To simplify the experiment, both CIs are analyzed in the same OSCAD-CIRAS. They are distinguished by prefixes RaT and Ele.

Let us assume that this critical risk scenario is downloaded from the basic repository for the risk assessment process.

Figure 7 shows four pairs of analyses of the validation experiment. Each pair, composed with BIA-RA, represents a bow-tie idea. The following numeration rule of the particular pairs of analyses is assumed: the basic scenario (called here the 1st iteration) has no postfix, for the second, third, *etc.*, expressing the escalated impacts, the iteration number is followed by a postfix expressing the kind of impact (ie, ee), *i.e.*, 1, 2ie, 2ee, and 3ee.

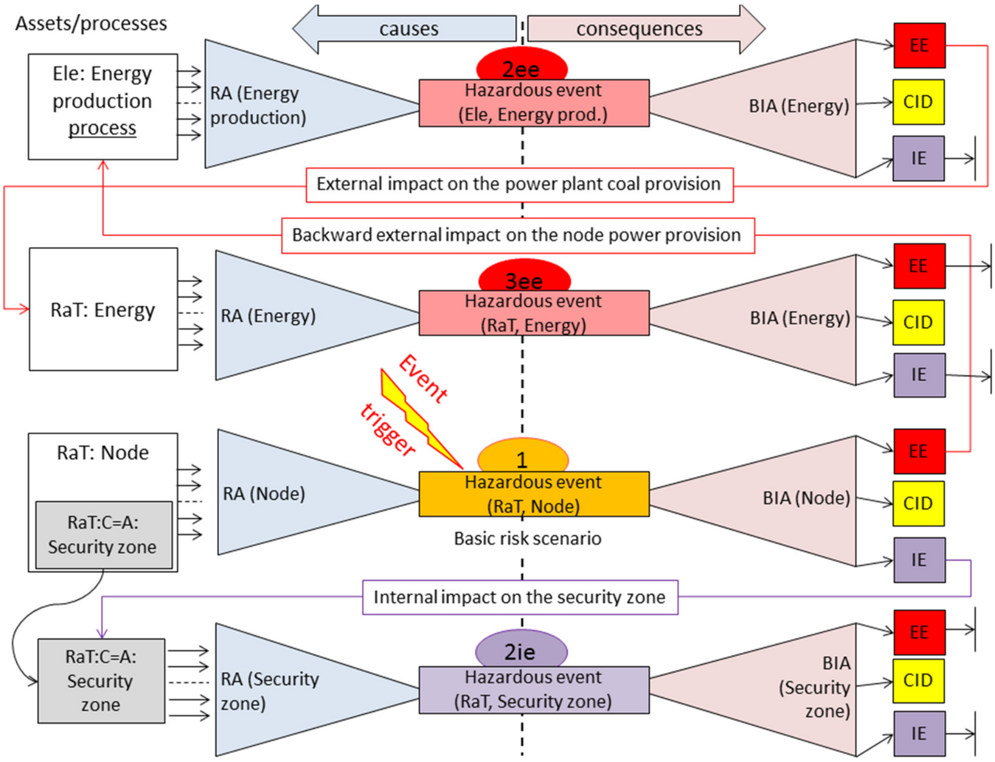

Assets/processes
causes
consequences
Ele: Energy production process
RA (Energy production)
2ee
Hazardous event (Ele, Energy prod.)
BIA (Energy)
EE
CID
IE
External impact on the power plant coal provision
Backward external impact on the node power provision
RaT: Energy
RA (Energy)
3ee
Hazardous event (RaT, Energy)
BIA (Energy)
EE
CID
IE
Event trigger
RaT: Node
RaT:C=A: Security zone
RA (Node)
1
Hazardous event (RaT, Node)
Basic risk scenario
BIA (Node)
EE
CID
IE
Internal impact on the security zone
RaT:C=A: Security zone
RA (Security zone)
2ie
Hazardous event (RaT, Security zone)
BIA (Security zone)
EE
CID
IE

Figure 7. Validation scenario shown with the use of the bow-tie concept.

The scenario is initiated by the event trigger which occurred in the RaT:Node (please note the naming convention: CIname:AssetName) primary asset and caused a hazardous event, e.g., intentional derailment seriously impacting the railway node area.

1st iteration

The "1 BIA(RaT:Node)" analysis identifies multidimensional impacts of this event. Please note that the impacted asset or process is within the brackets. The internal degradation (mostly financial consequences) which is caused by an intentional derailment is assessed (CID). BIA proves that this event:

- impacts the external infrastructure Ele as the coal transport for the power plant is stopped for a long time (EE-related risk scenario generated); normally this should imply sending this scenario to OSCAD-CIRAS working in Ele CI, but here both CIs are simulated in one OSCAD-CIRAS instance;
- breaches the security zone (countermeasure) which is a secondary asset of RaT:Node; IE-related risk scenario is generated and placed in the internal repository.

The "1 RA(RaT:Node)" analysis identifies causes of the hazardous event and the related risk. Because secondary effects are revealed, they should be further analyzed, causing the next iteration, instead of taking a new basic scenario.

2nd iteration

Due to the external escalation (EE), extra analyses for Ele CI (energy production in the power plant) are performed:

- "2ee BIA(Ele:Energy)" identifies the CI degradation caused by an externally generated threat; it does not identify any internal impacts (IE), but identifies backward external impacts to the RaT infrastructure (energy provision for the RaT:Energy); this implies the 3rd iteration;
- "2ee RA(Ele:Energy production process)" identifies how coal delivery disturbance impacts the energy production process (here the process-oriented approach is applied).

Due to the internal escalation (IE), extra analyses of the security zone are needed:

- "2ie BIA(RaT:Node→Security zone)",
- "2ie RA(RaT:Node→Security zone)".

Please note that a secondary asset is preceded by "→". The related BIA identifies secondary CI degradation caused by a breach in the security zone (here: theft) but does not identify any further IE or EE impacts.

3rd iteration

Due to the external threat generated by Ele for RaT:Energy, two extra analyses are performed:

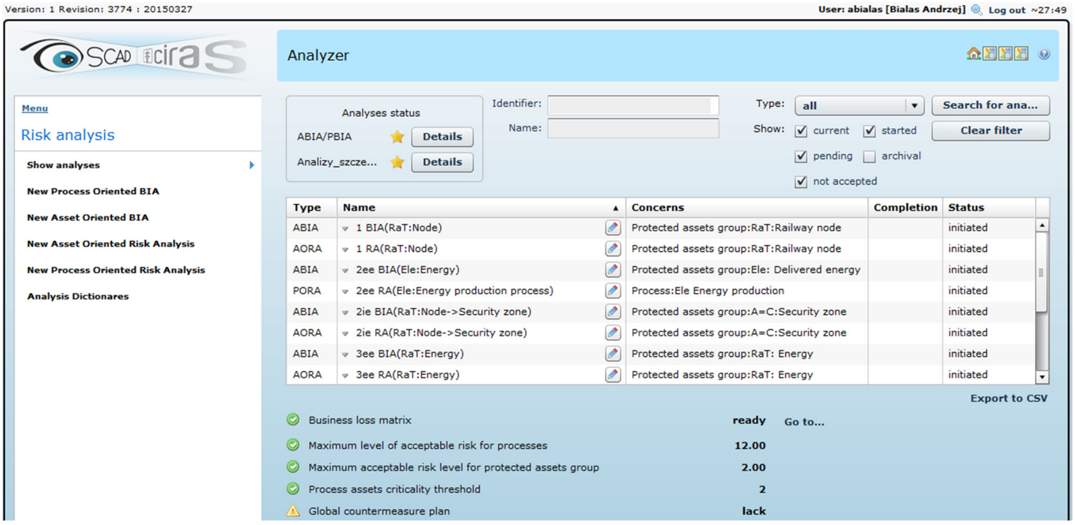
- "3ee BIA(RaT:Energy)",
- "3ee RA(RaT:Energy)".

The additional CI internal degradation is assessed, and no internal/external escalations are detected. In the 3rd iteration both RaT and Ele infrastructures achieve a stable state and therefore no further analyses are needed. Particular analyses were performed during the validation process.

2.6. Running the Validation Experiment

The validation experiment embraces eight analyses (four BIA, four RA) performed in OSCAD-CIRAS according to the scenario shown in Figure 7.

The left side of Figure 8 presents the OSCAD-CIRAS menu/submenu depending on the context of the operation, here: 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 the details of each analysis.



Version: 1 Revision: 3774 : 20150327

User: abialas [Bialas Andrzej] ~27:49

Analyses status
ABIA/PBIA ★ Details
Analizy_szcze... ★ Details

Identifier:
Name:

Type: all
Show: ☑ current ☑ started ☑ pending □ archival ☑ not accepted

Type	Name	Concerns	Completion	Status
ABIA	1 BIA(RaT:Node)	Protected assets group:RaT:Railway node		initiated
AORA	1 RA(RaT:Node)	Protected assets group:RaT:Railway node		initiated
ABIA	2ee BIA(Ele:Energy)	Protected assets group:Ele: Delivered energy		initiated
PORA	2ee RA(Ele:Energy production process)	Process:Ele Energy production		initiated
ABIA	2ie BIA(RaT:Node->Security zone)	Protected assets group:A=C:Security zone		initiated
AORA	2ie RA(RaT:Node->Security zone)	Protected assets group:A=C:Security zone		initiated
ABIA	3ee BIA(RaT:Energy)	Protected assets group:RaT: Energy		initiated
AORA	3ee RA(RaT:Energy)	Protected assets group:RaT: Energy		initiated

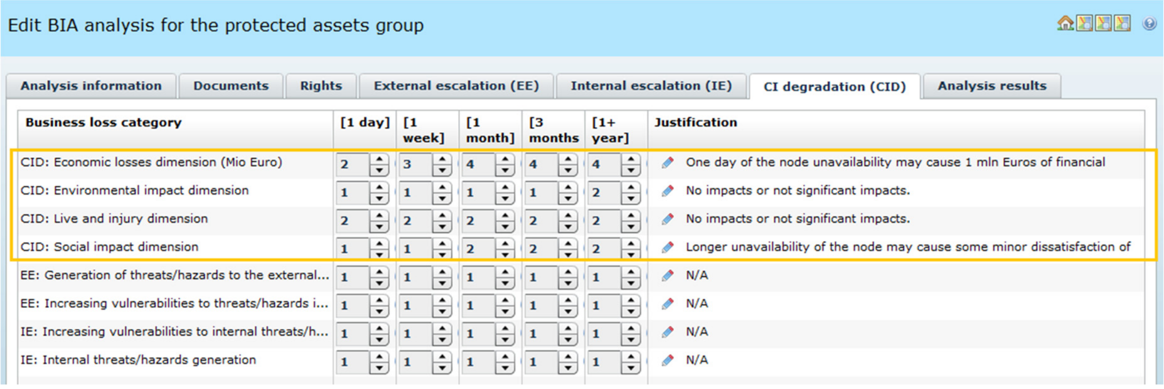
✓	Business loss matrix	ready
✓	Maximum level of acceptable risk for processes	12.00
✓	Maximum acceptable risk level for protected assets group	2.00
✓	Process assets criticality threshold	2
⚠	Global countermeasure plan	lack

Figure 8. OSCAD-CIRAS presenting performed analyses.

The four of eight performed analyses are exemplified in the following subsections.

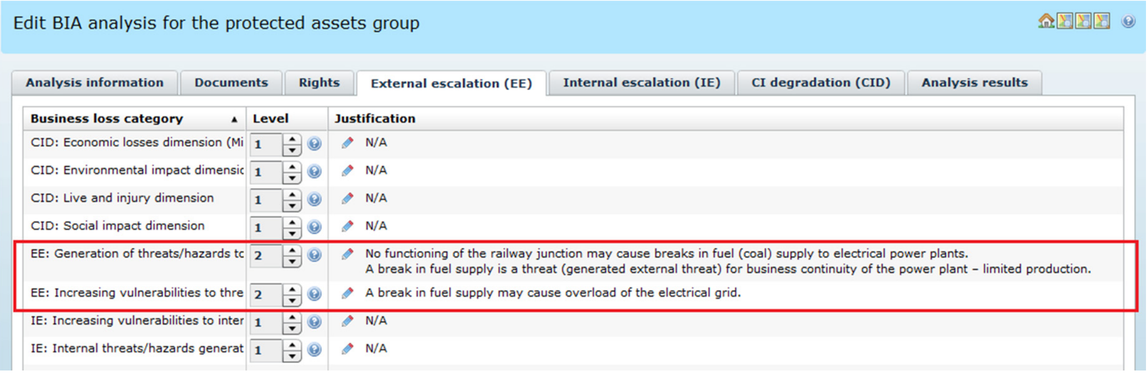
2.6.1. Identifying Impact of the Railway Node Crash—"1 BIA(RaT:Node)"

This BIA analysis assesses multidirectional impacts when the railway node crashes. "1 BIA(RaT:Node)" embraces three main impact categories, represented by three OSCAD-CIRAS tabs: CID (Figure 9), EE (Figure 10), IE (Figure 11).



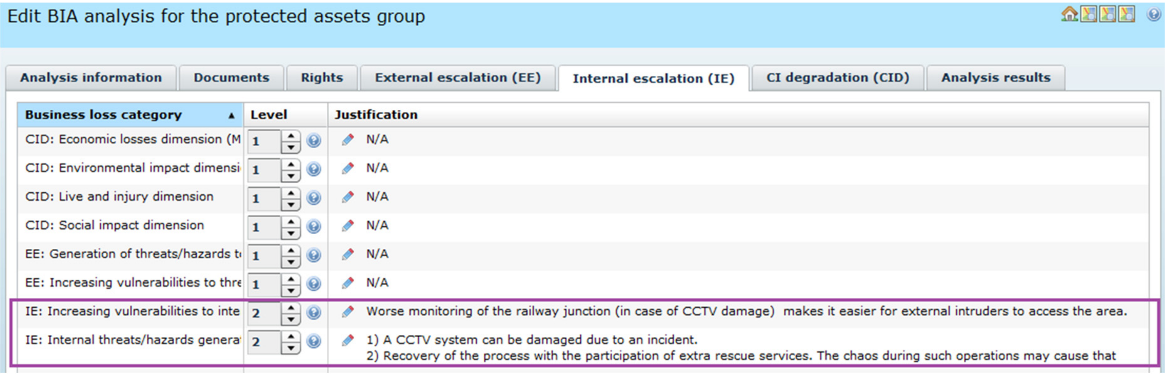
Business loss category	[1 day]	[1 week]	[1 month]	[3 months	[1+ year]	Justification
CID: Economic losses dimension (Mio Euro)	2	3	4	4	4	One day of the node unavailability may cause 1 mln Euros of financial
CID: Environmental impact dimension	1	1	1	1	2	No impacts or not significant impacts.
CID: Live and injury dimension	2	2	2	2	2	No impacts or not significant impacts.
CID: Social impact dimension	1	1	2	2	2	Longer unavailability of the node may cause some minor dissatisfaction of
EE: Generation of threats/hazards to the external...	1	1	1	1	1	N/A
EE: Increasing vulnerabilities to threats/hazards i...	1	1	1	1	1	N/A
IE: Increasing vulnerabilities to internal threats/h...	1	1	1	1	1	N/A
IE: Internal threats/hazards generation	1	1	1	1	1	N/A

Figure 9. The BIA analysis for the railway node—internal degradation tab.



Business loss category ▲	Level	Justification
CID: Economic losses dimension (Mi	1	N/A
CID: Environmental impact dimensic	1	N/A
CID: Live and injury dimension	1	N/A
CID: Social impact dimension	1	N/A
EE: Generation of threats/hazards tc	2	No functioning of the railway junction may cause breaks in fuel (coal) supply to electrical power plants. A break in fuel supply is a threat (generated external threat) for business continuity of the power plant – limited production.
EE: Increasing vulnerabilities to thre	2	A break in fuel supply may cause overload of the electrical grid.
IE: Increasing vulnerabilities to inter	1	N/A
IE: Internal threats/hazards generat	1	N/A

Figure 10. The BIA analysis for the railway node—external escalation tab.



Business loss category ▲	Level	Justification
CID: Economic losses dimension (M	1	N/A
CID: Environmental impact dimensi	1	N/A
CID: Live and injury dimension	1	N/A
CID: Social impact dimension	1	N/A
EE: Generation of threats/hazards t	1	N/A
EE: Increasing vulnerabilities to thre	1	N/A
IE: Increasing vulnerabilities to inte	2	Worse monitoring of the railway junction (in case of CCTV damage) makes it easier for external intruders to access the area.
IE: Internal threats/hazards genera	2	1) A CCTV system can be damaged due to an incident. 2) Recovery of the process with the participation of extra rescue services. The chaos during such operations may cause that

Figure 11. The BIA analysis for the railway node—internal escalation tab.

The tool offers a possibility to assess CID-type losses in a certain number (here: five) of time horizons (Figure 9). Please note that CIDval = 4 (worst case value).

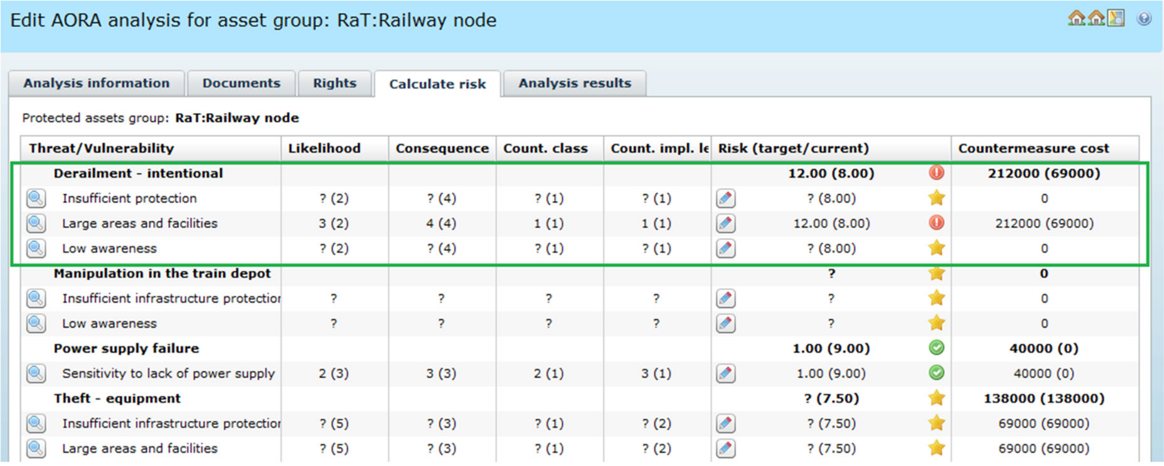
Figure 10 presents the assessment of the external impact of the crash in the railway node. The disturbance in the Ele critical infrastructure is possible because coal transport failed (limited production, network overloading). Please note that EEval = 2.

Figure 11 presents the assessment of the internal impact of the crash in the railway node. The crash may breach the node protection system (security zone, CCTV) raising vulnerabilities to other threats. This may cause negative secondary effects. Please note that IEval = 2.

Assuming that the worst case model is used, BIAvalue = max(4,2,2) = 4.

2.6.2. Causes of the Railway Node Crash—"1 RA(RaT:Node)"

Figure 12 exemplifies the "1 RA(RaT:Node)" analysis, mentioned in the validation scenario (Figure 7). Apart from the train derailment (a green frame), some other node risk scenarios are listed, like: manipulation in the train depot, power supply failure, theft of equipment, but they are not discussed here.



Edit AORA analysis for asset group: RaT:Railway node

Protected assets group: **RaT:Railway node**

Threat/Vulnerability	Likelihood	Consequence	Count. class	Count. impl. le	Risk (target/current)		Countermeasure cost
Derailment - intentional					**12.00 (8.00)**	❗	**212000 (69000)**
Insufficient protection	? (2)	? (4)	? (1)	? (1)	? (8.00)	★	0
Large areas and facilities	3 (2)	4 (4)	1 (1)	1 (1)	12.00 (8.00)	❗	212000 (69000)
Low awareness	? (2)	? (4)	? (1)	? (1)	? (8.00)	★	0
Manipulation in the train depot					**?**	★	**0**
Insufficient infrastructure protectior	?	?	?	?	?	★	0
Low awareness	?	?	?	?	?	★	0
Power supply failure					**1.00 (9.00)**	✓	**40000 (0)**
Sensitivity to lack of power supply	2 (3)	3 (3)	2 (1)	3 (1)	1.00 (9.00)	✓	40000 (0)
Theft - equipment					**? (7.50)**	★	**138000 (138000)**
Insufficient infrastructure protectior	? (5)	? (3)	? (1)	? (2)	? (7.50)	★	69000 (69000)
Large areas and facilities	? (5)	? (3)	? (1)	? (2)	? (7.50)	★	69000 (69000)

Figure 12. The RA analysis for the railway node.

The event triggered in the railway node is classified as "intentional derailment". The derailment is possible due to the following exploited vulnerabilities:

- "Large areas and facilities" of the railway node – difficult to monitor,
- "Insufficient infrastructure protection",
- "Low awareness".

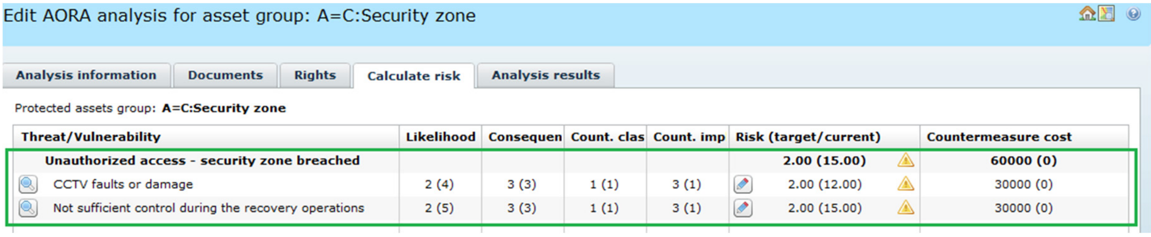
For each pair threat-vulnerability the risk is assessed. Each pair has consequences from BIA (BIAvalue = 4). Please note the pair: "Derailment—intentional"—"Large areas and facilities". The implementation of the countermeasures package (security zone, CCTV cameras, additional fences, police guards), not shown here, decreases the likelihood from "Possible" (3) to "Remote" (2), with the same consequences (4), and the risk from 12 to 8 (max. value is 5 × 5 = 25.0). Please note that the countermeasures cost rises from 69,000 Euros to 212,000 Euros (for the given package of countermeasures the cost is assigned).

Certain parameters, like countermeasure class or implementation level, are not used in the paper.

2.6.3. Causes of Breaching the Node Security Zone—"2ie RA(RaT:Node→Security Zone)"

During the IE assessment (Figure 11) a breach of the node security zone was identified implying two analyses:

- “2ie BIA(RaT:Node → Security zone)”—to assess impact related to this event, like: “Significant financial losses possible in case of long-lasting disturbance in functioning of security zone”, neither IE nor EE are detected—BIA not shown;
- “2ie RA (RaT:Node → Security zone)”—presented in Figure 13.


Edit AORA analysis for asset group: A=C:Security zone

Protected assets group: **A=C:Security zone**

Threat/Vulnerability	Likelihood	Consequen	Count. clas	Count. imp	Risk (target/current)	Countermeasure cost
Unauthorized access - security zone breached					**2.00 (15.00)** ⚠	**60000 (0)**
CCTV faults or damage	2 (4)	3 (3)	1 (1)	3 (1)	2.00 (12.00) ⚠	30000 (0)
Not sufficient control during the recovery operations	2 (5)	3 (3)	1 (1)	3 (1)	2.00 (15.00) ⚠	30000 (0)

Figure 13. The RA analysis for the breached security zone.

The breached security zone becomes more vulnerable because the CCTV system was damaged and the node was not properly watched due to the recovery process in the node (resources shortage). For this reason, unauthorized access is more realistic.

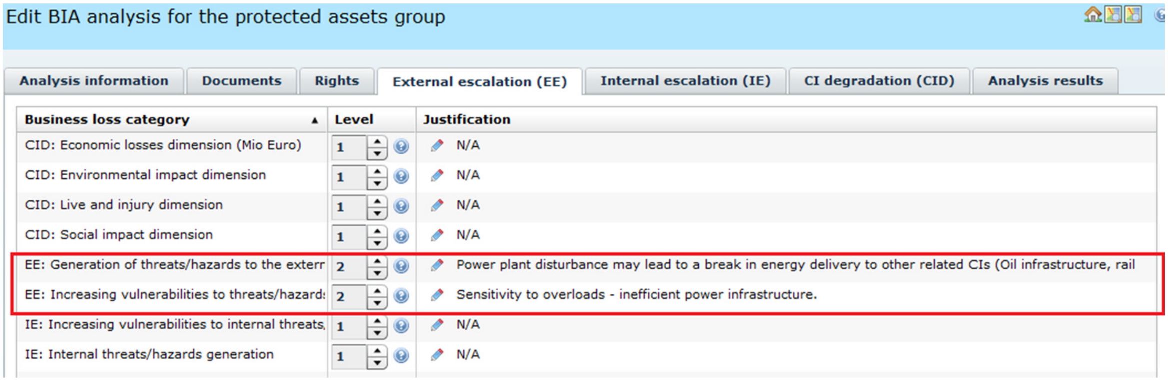
Please note that the security zone plays twofold role, therefore in the system dictionary a special category A = C (Asset as countermeasure) was defined.

The security zone is a barrier, a countermeasure, and an asset belonging to the set of assets representing the railway node. In OSCAD-CIRAS it is possible to asses risk for this node similarly to other assets.

2.6.4. Identifying Impact of Energy Delivery Disturbance—“2ee BIA (Ele:Energy)”

While EE was assessed for the basic scenario (Figure 10), the disturbance of the fuel (coal) delivery for the power plant was detected, implying two other analyses to be done for the Ele infrastructure:

- “2ee BIA(Ele:Energy)” was made, which revealed the possibility of the energy delivery problem (Figure 14); this may impact railways, therefore “3ee BIA(RaT:Energy)” and “3ee RA(RaT:Energy)” are launched (not shown).
- “2ee RA(Ele:Energy)”; the process-oriented risk analysis (PORA) is applied to exemplify that the process approach is possible in OSCAD-CIRAS; the analysis is focused on the causes of the “Energy production process in the power plant” disturbance.


Edit BIA analysis for the protected assets group

Business loss category ▲	Level	Justification
CID: Economic losses dimension (Mio Euro)	1	N/A
CID: Environmental impact dimension	1	N/A
CID: Live and injury dimension	1	N/A
CID: Social impact dimension	1	N/A
EE: Generation of threats/hazards to the exterr	2	Power plant disturbance may lead to a break in energy delivery to other related CIs (Oil infrastructure, rail
EE: Increasing vulnerabilities to threats/hazard:	2	Sensitivity to overloads - inefficient power infrastructure.
IE: Increasing vulnerabilities to internal threats,	1	N/A
IE: Internal threats/hazards generation	1	N/A

Figure 14. BIA for the energy asset provided by the power plant (EE tab).

The implied, but not shown here “3ee BIA (RaT:Energy)” and “3ee RA (RaT:Energy)” conclude that the disturbance of the railway energy system can be serious, still the probability is low thanks to the implemented redundancy.

Please note that the event "Energy delivery problem" can be considered a common cause event, because it impacts all energy dependent infrastructures. The validation scenario is simplified and considers only one dependent infrastructure (RaT).

3. Results and Discussion

The paper presents the validation experiment related to risk management in critical infrastructures with the use of the ready-made OSCAD software platform adapted for this application domain as the OSCAD-CIRAS tool.

To develop this CI-dedicated experimental tool, the following input was considered:

- the general requirements for the CI risk manager [12], elaborated on the basis of publications, laws, standards and tool reviews,
- the CIRAS project requirements.

The objective was to perform a case study and to acquire knowledge for the CIRAS project. The question is to what extent the requirements are satisfied by OSCAD-CIRAS, *i.e.,* whether OSCAD-CIRAS is able to work as the risk reduction assessment (RRA) component within the CIRAS Tool. The ready-made OSCAD was configured, equipped with the domain data (dictionaries, measures, different parameters, *etc.*), and the validation was performed according to the elaborated plan. As a result, the OSCAD-CIRAS experimentation tool was worked out.

3.1. Meeting Basic Requirements

Reviewing the basic requirements (Section 2.1.), the following conclusions are possible.

(1) OSCAD-CIRAS takes into account the CI specific phenomena, such as common cause failures, cascading and escalating effects, as well as interdependencies between CIs, though OSCAD-CIRAS should be supported by a resilience analysis. During the validation experiment it was shown that OSCAD-CIRAS is able to consider the following:

- common cause initiating events; for the given hazardous event BIA is able to detect hazardous events, that are implied by the given hazardous event, in all dependent infrastructures by generating many outgoing EE-related risk scenarios; this possibility was mentioned in Figure 14 (Ele => RaT, Ele => Oil, Ele => Gas) but was shown only for one dependency path (Ele => RaT);
- cascade initiating events; apart from internally triggered hazardous events, the RA analysis considers external triggers incoming from other infrastructures as the incoming EE-related risk scenarios; the considered impacted CI depends on infrastructures which generate these scenarios; this possibility is represented by the following analyses:
- ▪ "2ee RA(Ele:Energy)"—a coal delivery problem may disturb the energy production process;
- ▪ "3ee RA (RaT:Energy)"—an energy delivery problem may disturb railway transport;
- cascade resulting events; BIA is able to detect any hazardous event resulting from the original event which impacts a dependent infrastructure; this was represented by: "1 BIA(RaT:Node)"/Figure 10, "2ee BIA(Ele:Energy)"/Figure 14 and "3ee BIA (RaT:Energy)" (not shown);
- escalating events; BIA performed in the first infrastructure is able to detect a hazardous event in the second impacted dependent infrastructure, and BIA performed for the second impacted infrastructure is able to detect a hazardous event in the third infrastructure, and so on; this was exemplified by the analysis chain for RaT => Ele => RaT (Figure 7—a red line).

(2) The bow-tie concept embracing the analysis of consequences and causes was implemented as the pairs of the RA-BIA analyses. It was exemplified by the analyses chain shown in Figure 7. Usually BIA precedes RA.

(3) The risk register is represented by the OSCAD-CIRAS data (assets—primary and secondary, processes, threats, vulnerabilities, risk scenarios, countermeasures, *etc.*)—some data are predefined (dictionaries), some created during the performed analyses.

(4) Risk measures are configurable: categories of losses, number of loss levels and their interpretation, number of time horizons, likelihood levels and their interpretation, e.g., in the frequency domain, calculation models and formulas for risk assessment.

3.2. Meeting CIRAS Project Requirements

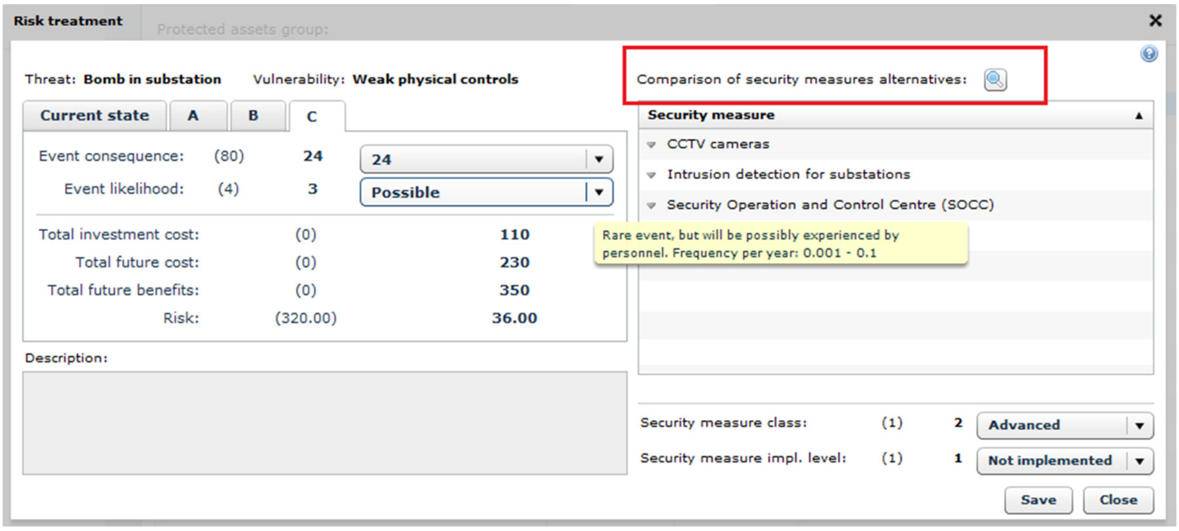
As for the CIRAS project requirements (Section 2.1), the following conclusions are possible.

(1) OSCAD-CIRAS is able:

- to assess risk before a measure is implemented and reassess the risk for a certain number of security measures alternatives considered for implementation,
- to take into account cost-benefits factors and qualitative criteria dealing with the security measures alternatives.

The validation scenario, simplified for the purposes of this article, was focused on the risk assessment before the countermeasure was implemented. However, the selection of measures in OSCAD-CIRAS, which is a part of the risk management process, needs additional explanation.

Figure 15 shows an example of security measures selection (the example slightly differs from the validation example) for the given threat-vulnerability pair. It is assumed that the "risk before" the measures implementation was assessed earlier (Current state tab). The decision maker who selects countermeasures for implementation may define several security measures alternatives (here three, marked A, B, C). Each alternative represents a coherent package of countermeasures, with their risk, cost, benefits, qualitative criteria and other parameters. Then the most advantageous alternative is selected for implementation.



Threat: **Bomb in substation** Vulnerability: **Weak physical controls**

Comparison of security measures alternatives:

Event consequence:	(80)	24	24
Event likelihood:	(4)	3	Possible
Total investment cost:	(0)		110
Total future cost:	(0)		230
Total future benefits:	(0)		350
Risk:	(320.00)		36.00

Rare event, but will be possibly experienced by personnel. Frequency per year: 0.001 - 0.1

Description:

Security measure
CCTV cameras
Intrusion detection for substations
Security Operation and Control Centre (SOCC)

Security measure class:	(1)	2	Advanced
Security measure impl. level:	(1)	1	Not implemented

Figure 15. OSCAD-CIRAS risk manager—considering security measures alternatives.

To support the decision maker in this process, some aggregated data from RRA, CBA and QCA are available on diagrams (note the button "Comparison of security measures alternatives", marked by the red frame). An example of a diagram, related to CBA parameters, is shown in Figure 16. Please note other tabs.

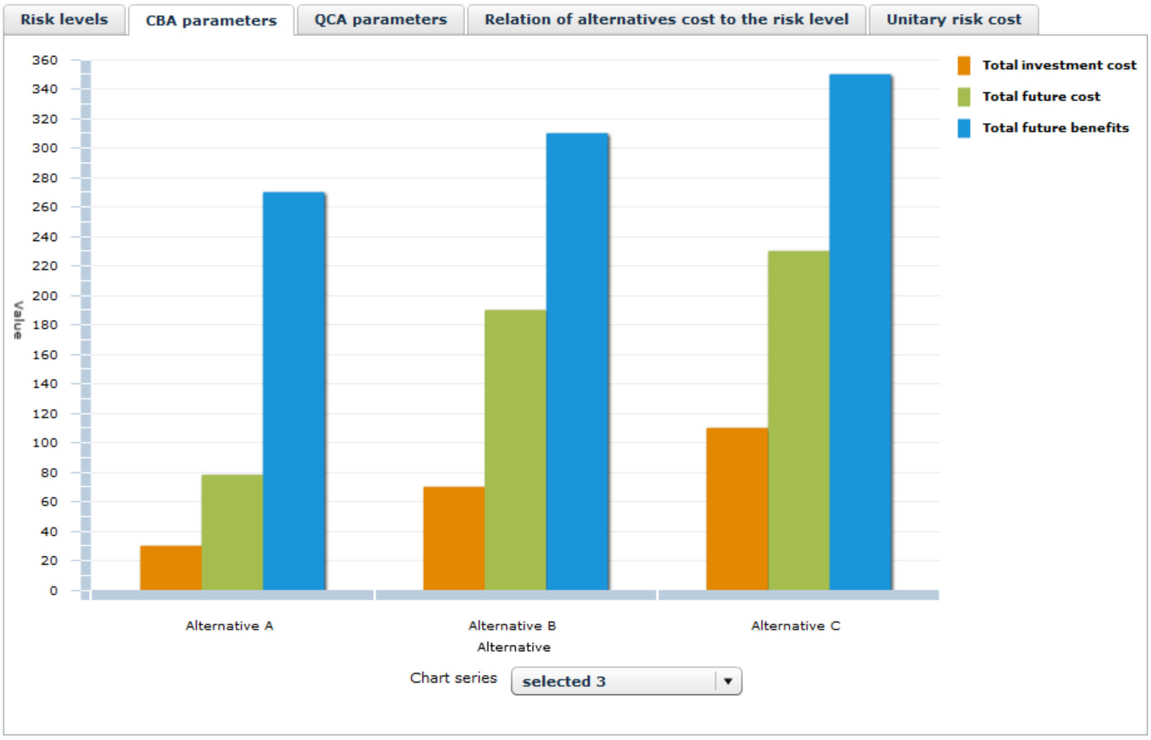


Figure 16. OSCAD-CIRAS risk manager—considering external cost-benefit parameters.

More detailed graphs, tables, reports related to particular alternatives will be available from the CIRAS tool level. Currently they are under development. OSCAD-CIRAS is able to exchange (through developed web services) information with the CBA and QCA components during the decision process dealing with the security measures selection

(2) Other issues related to the project requirements were discussed previously, like the ability to consider the CI specific phenomena and cross-sectoral dependencies, to analyze causes and impacts of hazardous events, and to manage the risk register data.

Reassuming, the validation process is based on the planned scenario which encompasses two critical infrastructures: railway transport (RaT) and electricity provision (Ele). Two kinds of escalation effects are demonstrated:

- those propagated through a CI internal path,
- those propagated through a path crossing one or more CIs.

The consequences of hazardous events in a given CI can impact the same CI again and/or the neighboring CIs, creating a complex sequence of impacts. The presented method allows to identify:

- direct consequences occurring within the considered infrastructure (called here: CI degradation);
- secondary effects caused by breaching internal barriers (CI safeguards) and occurring in this CI as the consequences of a hazardous event (called here: internal escalation); this escalation can propagate further causing additional hazardous events—internal or external;
- secondary effects occurring in the external CIs as the consequences of a hazardous event (called here: external escalation); they can propagate further, impacting other CIs or generating internal escalations.

The scenario depends on the new risks identified during the analysis. The presented method assumes (in the loss matrix for BIA analyses) that a new hazardous event (internal or external) can be triggered as a consequence of a previous hazardous event. Internally triggered events result from breaching the CI internal barriers. Events triggered within the external CIs can propagate thanks to existing CI interdependencies. The risk assessment results give information if the hazardous event will propagate internally and/or externally, or nowhere. It means that each risk situation may drive quite a different scenario in the same set of infrastructures. If, during the analysis of infrastructure A, it was detected that a breach in infrastructure B is possible (EE), then the risk analysis in infrastructure B is needed and will be added to the risk analyses scenario. Otherwise, the analysis in infrastructure B will not be added to this scenario. If, during the analysis of infrastructure A, it was detected that a security barrier can be breached (IE), then the analysis in infrastructure A is needed and will be added to the risk analyses scenario. Otherwise, it will not be added to this scenario.

For this reason, each scenario is here called a risk-driven scenario. It is assumed that interdependencies are known—all paths with possible propagation of impacts are known.

4. Conclusions

The objective of the paper is to develop a structured risk management method for critical infrastructures, embedded into the CI resilience process (Figure 6). The method distinguishes three categories of impacts composed into the BIA loss matrix:

- CID (direct CI degradation),
- IE (escalation by breaching internal security barriers),
- EE (escalation by breaching security barriers in external CIs).

The method is based on the commonly used risk management methodology, though it was enhanced by three above mentioned features which allowed to take into account the following issues (Section 3):

- how a hazardous event which occurred in the given CI impacts the dependent CIs; this allows to consider common cause initiating events, cascade resulting events, externally escalating events;
- how a hazardous event which occurred in external CIs impacts the given CI; this allows to consider cascade initiating events, externally escalating events;
- secondary impacts of a hazardous event which occurred in the given CI and lead to an internal escalation; this allows to analyze breaches in the multilayered protection system.

There are some extra features which make it possible to assess a critical infrastructure degradation in several time horizons (CID-type consequences). In addition, they can assess several security measures packages with respect to the risk reduction ability.

To elaborate, implement and validate this method, the research includes as well:

- the identification of CI domain-related data, like assets, processes, threats, vulnerabilities, common used countermeasures, *etc.*, and put them into the OSCAD system dictionaries,
- the risk parameters definition, *i.e.*,: scales of measures for likelihood, consequences, impacts categories and levels, loss matrix, calculation formulas configuration,
- the planning of the validation scenario (to be simple enough and be able to exemplify all features of the elaborated method),
- performing validation to assess the feasibility of the proposed solution.

The paper gives substantial contribution to the CIRAS project. The aim of the research presented in the paper is to acquire knowledge about the shape of the key component responsible for risk assessment (RRA) of the CIRAS Tool. The case study was based on the ready-made business continuity/information security management OSCAD software. During the research this software was adapted to the critical infrastructure application domain, according to the identified requirements. This way the dedicated OSCAD-CIRAS tool was developed. The near real data were prepared for the critical infrastructure domain and the software was configured. According to the planned validation scenario, the risk assessment within two collaborating infrastructures (railway, energy) was studied.

The case study gives information how to use OSCAD-CIRAS in the CIRAS project. The results of research confirm that OSCAD-CIRAS can be applied as the RRA component.

The acquired knowledge was used by the CIRAS project team. Currently all components (RRA, CBA, QCA) are integrated into the CIRAS Tool. The case study described in the paper is the basis for two CIRAS project use cases.

The CIRAS project considerably extends the risk reduction assessment by additional CBA (cost-benefits) and QCA (vague factors) assessments to obtain a full risk picture for the decision maker.

Acknowledgments: The author thanks his Colleagues from the CIRAS project consortium for reviewing this paper and discussing the presented concept. The author is grateful for their assistance during the OSCAD customization (installation, logo edition, preparing the OSCAD dictionaries).

Author Contributions: The presented validation experiment represent the author's own research.

Conflicts of Interest: The author declares no conflict of interest. The OSCAD is owned by the Institute of Innovative Technologies EMAG. 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 (obligatory for each paper concerning CIRAS).

References and Notes

1. Eusgeld, I.; Nan, C.; Dietz, S. "System-of-systems" approach for interdependent critical infrastructures. *Reliab. Eng. Syst. Saf.* **2011**, *96*, 679–686. [CrossRef]
2. ISO. *Risk management—Principles and guidelines*; ISO 31000:2009; International Organization for Standardization: Geneva, Switzerland, 2009.
3. IEC/ISO. *Risk Management—Risk Assessment Techniques*; IEC 31010:2009; International Electrotechnical Commission (in cooperation with ISO): Geneva, Switzerland, 2009.
4. Hokstad, P.; Utne, I.B.; Vatn, J. *Risk and Interdependencies in Critical Infrastructures: A Guideline for Analysis, Reliability Engineering*; Springer-Verlag: London, UK, 2012.
5. Rinaldi, S.M.; Peerenboom, J.P.; Kelly, T.K. Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Syst. Mag.* **2001**, *21*, 11–25. [CrossRef]
6. Giannopoulos, G.; Filippini, R. Risk Assessment and Resilience for Critical Infrastructures. In Proceedings of Workshop Proceedings, Ispra, Italy, 25–26 April 2012; Available online: http://publications.jrc.ec.europa.eu/repository/handle/JRC71923 (accessed on 29 February 2016).
7. Min, H.-S. J.; Beyeler, W.; Brown, T.; Jun Son, Y.; Jones, A.T. Toward modelling and simulation of critical national infrastructure interdependencies. *IIE Trans.* **2007**, *39*, 57–71. [CrossRef]
8. The Council of the European Union. Council Directive 2008/114/EC—on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. 2008. Available online: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008L0114 (accessed on 29 February 2016).
9. European Commission. Commission Staff Working Document—on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure. 2013. Available online: https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf (accessed on 29 February 2016).
10. CIRAS project web site. Available online: http://cirasproject.eu/content/project-topic (accessed on 22 December 2015).
11. ValueSec FP7 project web site. Available online: www.valuesec.eu (accessed on 22 December 2015).
12. Bialas, A. Critical infrastructures risk manager—the basic requirements elaboration. In *Theory and Engineering of Complex Systems and Dependability*; Zamojski, W., Mazurkiewicz, J., Sugier, J., Walkowiak, T., Kacprzyk, J., Eds.; Springer-Verlag: Cham, Switzerland; Heidelberg, Germany; New York, NY, USA; Dordrecht, The Netherland; London, UK, 2015; pp. 11–24.
13. EMAG. OSCAD project web site. Available online: http://www.oscad.eu/index.php/en/ (accessed on 21 December 2015).
14. Giannopoulos, G.; Filippini, R.; Schimmer, M. *Risk Assessment Methodologies for Critical Infrastructure Protection—Part I: A State of the Art*; Publications Office of the European Union: Luxembourg, 2012.

15. European Commission. EURACOM Deliverable D20: Final Publishable Summary, Version: D20.1. 2011. Available online: http://cordis.europa.eu/result/rcn/57042_en.html (accessed on 21 December 2015).
16. ENISA. Inventory of Risk Management/Risk Assessment Methods and Tools. Available online: http://rm-inv.enisa.europa.eu/methods (accessed on 21 December 2015).
17. Baginski, J.; Bialas, A.; Rogowski, D.; Flisiuk, B.; (Institute of Innovative Technologies EMAG, Katowice, Poland); Martin, J.; Garcia, A.; (ATOS S.A., Madrid, Spain); Klein, P.; (Center for European Security Strategies, Munich, Germany). State of the Art of Methods and Tools. 2015.
18. Rausand, M. Risk Assessment: Theory, Methods, and Applications. In *Statistics in Practice*; Wiley: Hoboken, NJ, USA, 2011.
19. Białas, A. Risk assessment aspects in mastering the value function of security measures. In *New Results in Dependability and Computer Systems*; Zamojski, W., Mazurkiewicz, J., Sugier, J., Walkowiak, T., Kacprzyk, J., Eds.; Springer-Verlag: Cham, Switzerland; Heidelberg, Germany; New York, NY, USA; Dordrecht, The Netherland; London, UK, 2013.
20. Bialas, A. Computer support for the railway safety management system—first validation results. In *Advances in Intelligent Systems and Computing*; Zamojski, W., Mazurkiewicz, J., Sugier, J., Walkowiak, T., Kacprzyk, J., Eds.; Springer-Verlag: Cham, Switzerland; Heidelberg, Germany; New York, NY, USA; Dordrecht, The Netherland; London, UK, 2014.
21. Białas, A. Business continuity management, information security and assets management in mining. *Mechanizacja i Automatyzacja Górnictwa* **2013**, *8*, 125–138. Available online: http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-891910b0-6f4e-4dfb-8bc3-345d940cc88b?q=fd72cbbb-7631-435b-9e4e-cf0b5ebdcc38$4&qt=IN_PAGE (accessed on 29 February 2016).
22. OSCAD-CIRAS. Available online on request using the author's e-mail.
23. Białas, A. Experimentation tool for critical infrastructures risk management. In Proceedings of the 2015 Federated Conference on Computer Science and Information Systems (FedCSIS), Lodz, Poland, 13–16 September 2015.