Computer Support for Risk Management in Critical Infrastructures

Andrzej Bialas

Abstract The paper deals with a methodology for the assessment and management of risk in critical infrastructures. A ready-made risk manager, which supports information security- and business continuity management systems, was adapted to a new application domain—critical infrastructure protection and was used in the EU Ciras project as one of its three basic pillars. First, the author reviewed security issues in critical infrastructures, with special focus on risk management. On this basis the assumptions were discussed how to adapt the ready-made risk manager for this domain. The experimentation tool was configured, including risk measures and system dictionaries. The operations of the tool were illustrated by examples from a case study performed in a previous work. The case study dealt with the collaborating railway- and energy critical infrastructures. The aim of this research is to assess the usefulness of such approach and to acquire knowledge for future project works.

Keywords Critical infrastructure · Risk management · Interdependencies · Bow-tie model · Risk management software

1 Introduction

The paper is an expanded and updated version of the paper "Experimentation tool for critical infrastructures risk management" [1], presented at the 3rd International Conference on Innovative Network Systems and Applications within multi-conference 2015 Federated Conference on Computer Science and Information Systems.

Critical infrastructures (CIs) are understood as large scale infrastructures whose degradation, disruption or destruction would have a considerable impact on the citizens' health, safety, security or well-being or would threaten the functioning of

A. Bialas (✉)
Institute of Innovative Technologies EMAG, Leopolda 31, 40-189 Katowice, Poland
e-mail: andrzej.bialas@ibemag.pl

M. Grzenda et al. (eds.), *Advances in Network Systems*, Advances in Intelligent Systems and Computing 461, DOI 10.1007/978-3-319-44354-6_12

governments and/or economies. Such infrastructures are, for example, energy-, oil-, gas-, finance-, transport-, telecommunications-, and health sectors. CIs provide products and services of key importance for today's modern societies. They form an extensive, complex network of processes and assets to facilitate exchange of different services between particular infrastructures and, first and foremost, to provide services for the economy, government and citizens. The networking brings many benefits but it is accompanied by new risks which may disturb processes and breach assets engaged in these processes. Due to CIs mutual relationships, not only services are exchanged but also threats are propagated—disruptions in a certain CI may cause dire effects in others. The most important threats and hazards are: natural disasters and catastrophes, technical disasters and failures, espionage, international crime, physical- and cyber terrorism. There are a number of programmes and activities which are part of a new, holistic approach to CI protection. They all come under the term critical infrastructure protection (CIP).

The protection of critical infrastructures has become a serious issue in well developed countries, including the European Union (EU) countries. The European Council (EC) Directive [2] lays down the specifics about the CIP related needs on the EU and member state levels. The Directive formulates the rules of the CI identification based on casualties-, economic- and public criteria, risk analysis and management programmes. Additionally, it defines the term ECI (European critical infrastructure) as a critical infrastructure located in member states, whose disruption or destruction would have a significant impact on at least two member states. There are two ECI sectors distinguished in this document:

- energy (electricity, oil, gas),
- transport (road transport, rail transport, air transport, inland waterways transport, ocean and short-sea shipping and ports).

In 2006 the EPCIP programme was launched (European Programme for Critical Infrastructure Protection), concerning critical infrastructures on both European and national level. The revised and more practical implementation of EPCIP can be found in the EU document [3].

An important issue is the CI resilience, which is understood as an ability of a system to react to and recover from unanticipated disturbances and events.

Critical infrastructures protection programmes are based on risk management. The issue of risk management in CIPs remains a challenge. This is proven by dozens of EU or worldwide CIP R&D projects which focus on risk methodologies and tools (FP6, FP7, Horizon 2020, CIPS).

The paper features some researches that are preliminary activities of the Ciras[1] project [4] which was launched by the international consortium comprising ATOS, CESS, and EMAG—the author's organization. The Ciras project aims at the

[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).

development of a methodology and tool to properly select security measures in the critical infrastructure domain. The project uses three main inputs:

- an extensive review of the state of the art of the risk management methodologies, especially those for critical infrastructure protection,
- conclusions from the organized Ciras stakeholders' workshops,
- an OSCAD-Ciras feasibility study presented in the paper.

The Ciras approach is based on the FP7 ValueSec [5] methodology. The ValueSec decision making process assumes that the proposed security measure (countermeasures) should be:

- able to sufficiently mitigate the risk volume in order to provide security on an accepted level and to provide benefits for stakeholders,
- cost-effective in order not to diminish the efficiency of operations and not to produce unnecessary costs,
- free of social, psychological, political, legal, ethical, economical, technical, environmental, etc. restrictions (called there "qualitative criteria").

To provide data for a decision maker, the Ciras Tool will be equipped with three components corresponding to the above mentioned issues:

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

This three pillars approach has been implemented in the Ciras Tool for the critical infrastructure protection domain. This domain is more complicated than the application domains considered in the ValueSec (mass event, mass transportation, communal security planning, air transport security, cyber smart grid attack).

The paper deals with the RRA component and is focused on how to develop or implement it, satisfying the project requirements. RRA should be relatively simple, able to properly manage the risk in critical infrastructures by selecting security measures with right cost-benefits parameters and free of intangible restrictions. The OSCAD[2] software platform [6] was considered one of the candidates for the RRA component. The paper presents researches which allow to assess whether this platform is able to satisfy the project requirements and whether it can be used as the RRA component of the Ciras Tool. Because the answer to this question is not straightforward, the author performed researches and experiments presented in this paper. To do this, first the experimentation tool, called OSCAD-Ciras, was developed, next a case study was planned, performed and concluded.

The aim of the research presented in the paper is to develop a simple configurable risk management tool for CIs which will be able: to analyze causes and

[2]developed at the Institute of Innovative Technologies EMAG within a project co-financed by the National Centre for Research and Development (NCBiR).

consequences of hazardous events, to process all risk-relevant data, and to consider interdependencies.

The motivation for researches presented in the paper is to get input for the Ciras project. During the experimentations the standard OSCAD software was adapted to the CI application domain according to the requirements specified in the paper [7]. The key issue was if these requirements can be implemented on the ready-made software or some software modifications or extensions are needed. During the case study, the OSCAD platform was properly configured and equipped with the near real data related to the project domain. The case study example concerns the railway CI interrelated with the energy CI. This way the CI dedicated OSCAD-Ciras experimentation tool was developed. The aim of the experimentation is to acquire indispensable knowledge about the usability of this risk manager to work as the RRA component of the Ciras Tool. 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 the implementation. This information is supplemented by cost-benefits- and qualitative criteria related factors. RRA should be able to exchange information with the CBA and QCA components during the decision process dealing with the security measures selection.

Section 2 of the paper includes an introduction to risk management in critical infrastructures. Section 3 summarizes the preferred features of the risk management tool discussed in the work [7]. Section 4 presents the functionality of the OSCAD software platform, while Sect. 5 gives the specifics of OSCAD's adaptation to be a CI risk manager and draws some conclusions for future works.

2 Resilience and Risk Management in Critical Infrastructures Protection

Critical infrastructure is a heterogeneous, distributed, adaptive, and very complex socio-technical system which encompasses hardware, software, liveware, environmental, management, and organizational elements. The basic objective of a CI is to provide products and/or services for the society. In order to reach this objective, this complex socio-technical system must be well harmonized, the disturbances within the system must be under control, the system has to work smoothly, and the assets needed to perform the job have to be well protected. The CI countermeasures, selected on the basis of risk, should be properly managed and composed into CIP programmes.

Some critical infrastructures (systems) collaborate with each other, e.g. electricity, rail transport, gas, oil, telecommunications Thus they constitute a more complex structure, called a system-of-systems (SoS). SoS includes different mutual dependencies (i.e. interdependencies) that exist within particular CIs. An interdependency [8] is a mutual relationship between two infrastructures (systems) where the state of each infrastructure influences or is correlated to the state of the other [9].

The CIs failures are usually causally linked, which means that the impacts of incidents may pass across different CIs. In addition, certain CI-specific effects are observed:

- a cascading effect is based on a sequence of component failures [10]. The first failure shifts its load to one or more nearby components. Then these components fail and, in turn, shift their loads to other components. This sequence is repeated;
- an escalating failure happens when there is a disruption in one infrastructure which causes an independent disruption in another infrastructure [8]. The effects of hazardous events may escalate outside the area where they occur and exacerbate the consequences of a given event (in the form of increasing the severity or the time for recovery of the second failure);
- common cause failures are failures implied by a single shared cause and coupling to other systems mechanisms. They may occur almost concurrently.

The interdependencies and related phenomena are not the key issues in this paper but they are taken into account during the risk assessment and management.

Critical infrastructures operators take care about the CI resilience. They apply strategies to deal with disruptive events, mitigate the magnitude of events, shorten their duration, react properly, minimize impacts, recover from a potentially disruptive event, etc. The CI preparedness is very important too, along with the ability to anticipate an event, absorb a threat, adapt the infrastructure to different situations, maintain critical operations and functions in the face of a crisis (robustness), manage resources needed for reaction and recovery, etc.

To ensure the CI resilience, a systematic approach is needed. At the beginning, the critical infrastructure is structurally analyzed and specified. The most critical elements and the most vulnerable points are identified, as well as the internal and external relationships (interdependencies). All these results form a static picture of the CI. Using this model, different scenarios can be considered to reveal dynamic properties of the given CI. This analysis can be considered as the simulation of different phenomena, like propagation of dire effects, identifying the impact of certain threats, common failures, assessing the effectiveness of the reaction to a given threat or disturbance, performing the CI recovery process, etc. This analysis yields a set of the most dangerous and prioritized risk scenarios, which can be further analyzed on a more detailed level. Generally, due to the CIs complexity, it is impossible to analyze all identified risk scenarios. For this reason only the most serious ones are chosen to be encompassed by the risk management process.

To ensure the preparedness and incident response ability, it is necessary to identify the risk source, risk character and value. What is more, it is important to apply the right countermeasure and embed it into the risk management framework, sometimes supported by tools.

Due to CIs complexity, interdependencies, specific effects, different abstract levels applied to manage CIs, and other factors, the comprehensive approach to risk management in critical infrastructures still remains a challenge.

Different risk management methodologies and tools are a subject of current R&D on the national and international levels, including the EU level. The following knowledge sources contain very comprehensive reviews of the R&D results:

- the report [11] of the Institute for the Protection and Security of the Citizen, EC Joint Research Centre (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, like Ciras project [4];
- the EURACOM report [12]; it features a study of 11 risk assessment methodologies related to the energy sector;
- the book [9]; in its Appendix C it provides a comparison of the features of about 22 commonly used risk analysis methods;
- the ISO 31010 standard [13] characterizes about 30 risk assessment methods for different applications;
- the ENISA website [14] includes an inventory of risk management/assessment methods, mostly ICT-focused.

A very exhaustive review of the state of the art is provided in [15]. The objective of this document was to select the most favourable methods/tools features for implementation during the Ciras project. The document summarizes the assessment of 14 methods (from 46 preselected), 22 tools (from 150 preselected) and considers 19 projects and 8 frameworks.

Usually, each of these methods/tools is focused on a restricted domain and does not address properly the holistic view and resilience. Therefore, it is an open question how to consider CIs interdependencies in the risk management process.

3 Basic Features of Risk Manager for Critical Infrastructures

The paper [7] discusses the basic requirements of the risk manager to be applied in critical infrastructure protection. This section provides a short overview of these issues.

3.1 Conceptual Model of the Risk Manager

The implementation of the bow-tie risk concept in the tool brings obvious advantages for CI risk management [7]. The method allows to identify risk pathways and barriers in CIs to prevent or react to undesired consequences or stimulate desired ones.

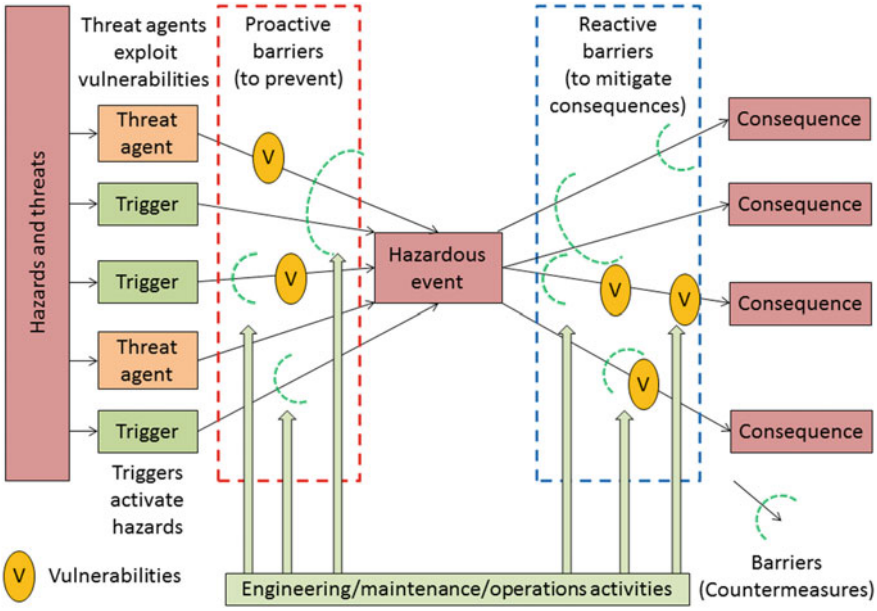


Fig. 1 General concept of the bow-tie analysis

The bow-tie conceptual model [10, 13] contains multiple and complex causes of the given hazardous event as well as its diversified and multidirectional consequences (Fig. 1).

The triggered hazards or threats, which exploit certain vulnerabilities, can degrade proactive barriers (countermeasures) existing in the system. This situation may result in an event which is hazardous for assets. Such an event usually has diversified and multidirectional consequences. To mitigate them, reactive barriers are applied. These barriers can be weakened or even removed by vulnerabilities. Generally, barriers are identified with different kinds of countermeasures. The countermeasures are applied with respect to the risk value and are monitored and maintained—according to the risk management principles. The bow-tie model is focused on risk assessment and can be used to reassess the risk after new or updated barriers are applied.

The bow-tie analysis is based on this model. For each knot representing a hazardous event, certain causes are identified along with related preventive barriers. Next all potential consequences of the hazardous event are listed, with respect to the reactive barriers. Management activities (engineering, maintenance, trainings, monitoring) support both groups of barriers.

The bow-tie model includes the cause analysis and the consequences analysis. These analyses can be implemented in less or more complex ways [13], e.g. with the use of FTA (Fault tree analysis) [16] or ETA (Event tree analysis) [17].

This model does not have any analysis of interdependencies, therefore it is necessary to supplement it in this respect.

3.2 Risk Related Data and the Risk Register

The tool should support a CI owner in elaborating and maintaining a risk register serving as an inventory of hazardous events. The listed items (data records) should include at a minimum: related hazards/threats, a possible corresponding hazardous event, probability of the event and its consequences. The risk management process is performed during the CI life cycle, so the risk register can be continuously updated. There are some data associated with each item of the risk register, like assets, societal critical functions (SCF) which ensure the basic needs of a society (e.g.: life and health, energy supply, law and order, national security), hazards, threats, vulnerabilities, countermeasures, etc.

3.3 Risk Assessment Parameters and Assessment Process

Risk measures, such as event likelihood and consequences, depend on the applied methodology and are broadly described in literature [9, 10].

The likelihood of a hazardous event can be assessed with the use of a predefined scale, e.g.: fairly normal, occasional, possible, remote, improbable. The consequence severity can be assessed in different dimensions with the use of enumerative scales, e.g.: negligible, minor, major, catastrophic damages. The risk is a function of both likelihood and consequences usually expressed by a risk matrix, as presented in [7].

3.4 Considering the CI Specific Issues

The risk assessment/management methods/tools (Sect. 2) are focused on the given environment which has certain protected assets and processes. However, they do not consider interdependencies between other environments. The interdependencies have be included in the risk management process as they are essential for the CI protection.

Please note that the given hazardous event may be invoked by internal factors as well as external factors, including these coming from other CIs. Apart from this, the hazardous event may cause internal damages and/or may cause problems in the coupled external infrastructures. The risk assessment methodology should be able to take into account the CI specific phenomena mentioned in Sect. 2.

4 OSCAD Software as the Implementation Platform

The OSCAD software was originally elaborated to support business continuity management according to ISO 22301 and information security management according to ISO/IEC 27001. It is used to control factors which disturb business processes or breach information assets in an institution (business, public) and which may bring about negative consequences, to minimize losses when an incident occurs, and to support the organization in its recovery processes.

OSCAD is open and flexible. Therefore, after certain modifications, it can be implemented in different application domains, e.g.: flood protection [18], railway safety management systems [19] and coal mining [20]. The paper discusses the possibility to adapt OSCAD to the CI risk management domain.

The OSCAD platform offers an extensive functionality, though from the risk management perspective, only the following will be useful:

- system dictionaries—allowing to predefine threats, vulnerabilities, countermeasures, categories of assets, risk measures parameters, like likelihood and consequences,
- configuration facilities—to describe the given CI, to define risk matrix, to set analytical parameters, etc.,
- asset and process inventory—to specify the CIs protected assets and/or processes, whose breaches and disturbances are to be considered during the risk assessment process,
- risk assessment and management facilities—the core functionality discussed in this paper.

OSCAD is equipped with tools which analyze causes of hazardous events:

- AORA—Asset Oriented Risk Analyzer,
- PORA—Process Oriented Risk Analyzer,

and tools which analyze their multidimensional consequences:

- ABIA—Asset Oriented Business Impact Analyzer,
- PBIA—Process Oriented Business Impact Analyzer.

The selection of countermeasures is based on the assessed risk value and their total investment/maintenance costs. After selecting for implementation a given countermeasure or a set of measures, the risk is reassessed with respect to the acceptance level assumed for the organization.

5 Implementation of Risk Manager Requirements on the OSCAD Software

The following section presents the author's proposals how to implement the above-listed requirements into the existing OSCAD [6] software platform.

5.1 Bow-Tie Model Implementation on the OSCAD Software Platform

The bow-tie conceptual model is not directly implemented in OSCAD. However, the OSCAD risk analyzing tools can be used to compose it.

The cause analysis part of the bow-tie model is implemented on the basis of AORA or PORA. AORA is responsible for the analysis of each threat-vulnerability pair which can breach the given asset. PORA does the same with respect to the given process.

The consequences analysis part of the bow-tie model is implemented on the basis of ABIA or PBIA. For a given asset (process), which is under a hazardous event, multi-dimensional consequences can be assessed with the use of the loss matrix.

Both parts of the bow-tie model are not coupled directly by the hazardous event, but by the threatened asset (or process) related to this event.

Figure 2 shows examples of analyses composing the bow-tie conceptual model. The left part of the figure presents the "Risk analysis" menu of the OSCAD experimentation tool, called here OSCAD-Ciras. The right side of the figure presents the list of performed analyses. Please note that two analyses, corresponding to the same asset (or process), compose the bow-tie model, e.g.:

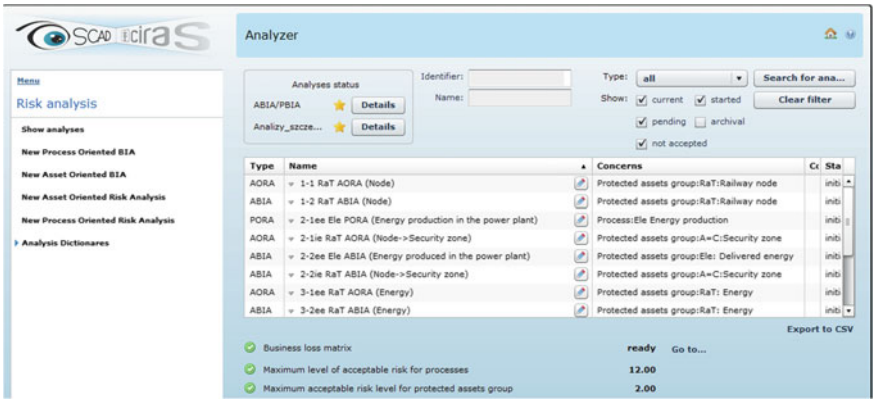


Fig. 2 OSCAD risk analyses composing the bow-tie model. OSCAD risk manager elaborated in the EMAG Institute. (Screen shot prepared by the author, 2015)

- "1-1 RaT AORA (Node)" (left part of the bow-tie model),
- "1-2 RaT ABIA (Node)" (right part of the bow-tie model).

Both above mentioned analyses create a pair related to the railway node. Please note that this node can be considered as an element of the Railway transport (RaT) European critical infrastructure (ECI) [2] (see Sect. 5.2).

The following preliminary naming convention for risk assessments is assumed:

- iteration number (1-primary, 2-secondary, 3-third iteration, etc.) followed by "-",
- index of assessment (1 for AORA/PORA, 2 for ABIA/PBIA),
- optional suffix for secondary effects assessment identified during BIA: "ie" or "ee" (see Sect. 5.3),
- CI acronym, e.g. "RaT",
- kind of assessment acronym with the asset in the parentheses, e.g. "AORA (Node->Security zone)".

Remark 1 In the OSCAD tool both asset oriented (AORA-ABIA) and process oriented (PORA-PBIA) analyses can be performed.

5.2 *Representation of the Risk Register and Risk Related Data in OSCAD*

The basic risk-related data are assets being part of critical infrastructures which need protection.

The general ECI (European CI) taxonomy specified in the EC Directive [2] is implemented in OSCAD as a hierarchical structure. The assets belonging to the given ECI are preceded by a label standing for 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).

The left part of Fig. 3 shows the assets hierarchy, while the right part points at the instance "Katowice—South" of the asset group "RaT:Railway node".

All CI assets can be specified hierarchically according to the stakeholders' needs with respect to the number of hierarchy levels. It is possible to create, around the given primary asset, a group of related secondary assets (technical, personal, immaterial, playing role of countermeasures, etc.). This group of assets can be composed in the assets inventory module. The assets can be defined on the general or detailed levels.

Remark 2 OSCAD-Ciras allows to consider the given critical infrastructure on different abstract levels, e.g. on the CI operator level, on the CI particular components levels.

For each of the protected assets, the AORA analysis can be performed. PORA can be done for the processes in a similar way. Using the OSCAD process

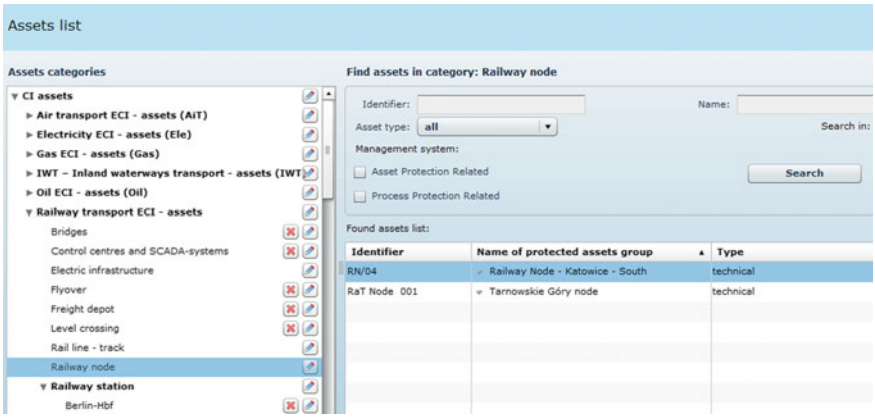


Fig. 3 Hierarchical structure of protected assets—taxonomy proposed in [2]. (OSCAD screen shot prepared by the author, 2015)

inventory, processes and their subprocesses can be defined on the general or more detailed levels. The paper does not focus on the process-oriented approach.

In critical infrastructures multilayered protection systems are usually applied. In the bow-tie model different barriers (countermeasures) are marked, representing this kind of protection. To perform a risk analysis for different barriers, security zones, etc., which play the role of countermeasures, an auxiliary category is defined: A = C (countermeasures considered as assets), for example "A = C:Security zone" can be added to the "Railway node", and an additional risk analysis for it can be performed (risk analysis in OSCAD is focused on assets or processes, not on countermeasures). This feature allows to take into account internal escalation effects during the risk analysis. This issue will be explained latter.

Remark 3 Certain assets playing the role of countermeasures are distinguished in OSCAD-Ciras (A = C category). This way the countermeasures can be encompassed by the risk assessment process and it is possible to analyze the internal escalation effects.

Generally, a hazardous event can be considered a specific representation of the threat [10]. The formula assumed in OSCAD and specifying the threats scenario is:

[*Threat agent*] exploiting [*vulnerability*] causes [*adverse action*] to [*asset*] or [*process*],

and parameters in square brackets have to be refined.

To put it simply, a threat agent, representing a force which initiates the scenario, is identified as the hazard trigger. Assuming that the phrase "exploiting [*vulnerability*]" concerns threats only, the following remark can be specified.

Remark 4 In the OSCAD-Ciras tool threats and hazards have the same representation—they are simply the "OSCAD threats" in system dictionaries.

The threat specification includes terms essential for the risk analysis. Threats specified during the AORA/PORA analyses play the role of risk register items. OSCAD has the incident management functionality (registering, assessment, solving, lessons learnt, statistics). The incidents which have already occurred are assigned to the threat items too. For this reason, the predicted risk scenarios and occurred incidents (materialized risk scenarios) are consistent. OSCAD is able to build statistics of incidents. This auxiliary option related to real-time risk management, not discussed here, can be used for more advanced applications in the future.

To sum up, OSCAD defines the risk register as a set of risk scenarios resulting from AORA or PORA and compatible with the incident inventory.

OSCAD has predefined lists of threats, vulnerabilities and countermeasures. Though they are flat, a special grouping mechanism is applied as the hierarchical grouping dictionary. On the upper hierarchy level these threats can be ordered first according to critical infrastructures taxonomy, and then according to their character. For OSCAD-Ciras the following threats categories are assumed: Behavioural/Social, Natural/Force majeure, Organizational, Technological. For the given threat (T), relevant vulnerabilities (V) are given, and to the given pair threat-vulnerability, recommended countermeasures (C) can be assigned.

Figure 4 presents the hierarchical structure of the grouping dictionary and some examples concerning railway transport:

- four vulnerabilities are assigned to the threat "Bomb in the station hall": "Improper response", "Insufficient protection", "Large areas and facilities" and "Low awareness",
- for the threat-vulnerability pair "Bomb in the station hall"-"Large areas and facilities", the following countermeasures are predefined: "Fences", "Intensified security zone inspections".

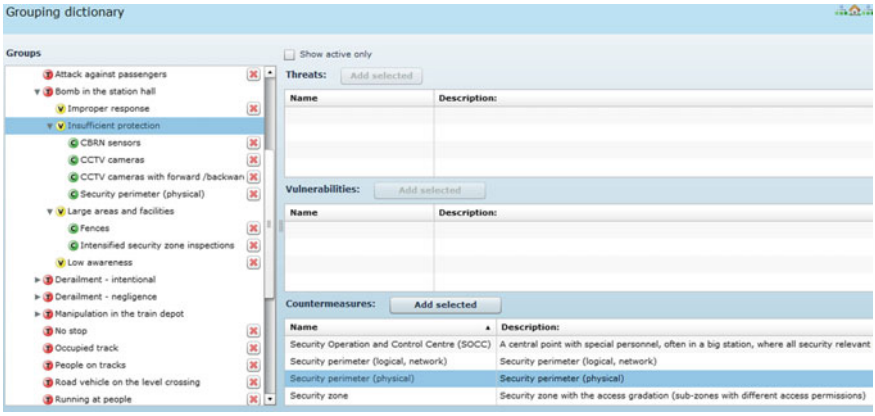


Fig. 4 Grouping dictionary with data relevant to rail transport. (OSCAD screen shot prepared by the author, 2015)

Remark 5 The OSCAD-Ciras tool is very flexible in creating dictionaries of threats, vulnerabilities and countermeasures (different levels of detail, predefined categories, domain-specific dictionaries, grouping of the predefined items). These predefined relations speed up the countermeasures selection during the risk management process.

5.3 Risk Assessment Parameters and Assessment Process in OSCAD

For the AORA and PORA analyses two issues should be defined: likelihood of the event and its consequences. For the experimentation purpose the likelihood and consequences measures were elaborated on the common literature basis. The scales of measures are discussed in [7] and summarized in Tables 2 and 1 of this publication.

Figure 5 shows the implementation of the likelihood scale of measure from [7]/Table 2 in OSCAD-Ciras.

Figure 6 shows the implementation of the scale of measure of consequences presented in [7]/Table 1 in OSCAD-Ciras.

The risk value (AORA/PORA) is calculated with the use of a simple formula:

$$\text{Risk value} = \text{Event likelihood} * \text{Event consequences} \quad (1)$$

The scales of measures should be defined for the ABIA/PBIA analyses as well.

The measures of multidimensional consequences of the hazardous event (Fig. 7) are key issues for the ABIA/PBIA analyses. Three categories of consequences are distinguished:

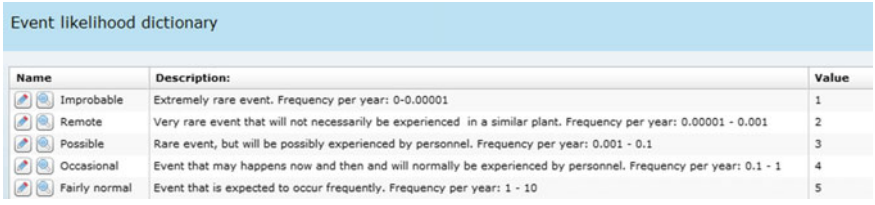
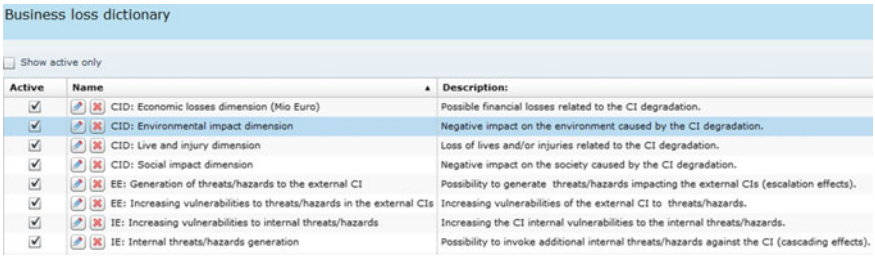


Fig. 5 Event likelihood scale of measure. (OSCAD screen shot prepared by the author, 2015)

Fig. 6 Event consequences scale of measure. (OSCAD screen shot prepared by the author, 2015)


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).

Fig. 7 Event impacts measures with CID, IE and EE categories

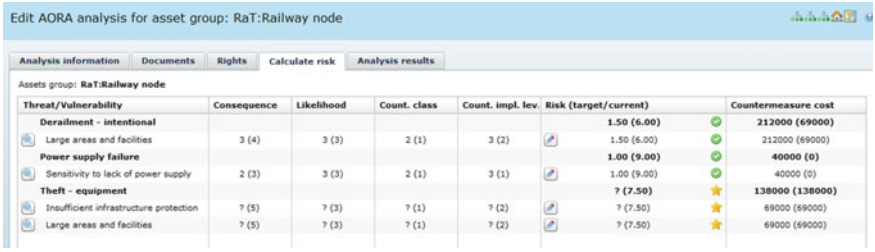
- CID (CI degradation) category, which expresses different kinds of damages within the given CI, like economic losses, environmental impact, loss of lives and injuries of people, social impact;
- IE (Internal escalations) expresses new internally generated threats or new or increased vulnerabilities which influence the considered CI, caused by the hazardous event,
- EE (External escalations) expresses generated threats which impact the external CIs or new or increased vulnerabilities in the external CIs, caused by the hazardous event.

Business loss categories (CID, IE, EE) and their subcategories are used to construct the later discussed BIA matrix, which is the basic tool for the ABIA/PBIA assessment process (Fig. 10).

The implementation of the bow-tie model is presented by the pair AORA-ABIA with respect to the given asset (here: railway node of the RaT infrastructure). The process approach (PORA-PBIA), though possible, is not discussed here.

The aim of AORA is to identify and assess the risk value related to a hazardous event in a railway node as a part of the railway critical infrastructure. Please note that AORA is focused on the assessment of causes of the hazardous event. Its example is shown in Fig. 8.

Please note three threats ("Derailment—intentional", "Power supply failure", "Theft—equipment") and the related vulnerabilities. For each pair


Edit AORA analysis for asset group: RaT:Railway node

Analysis information | Documents | Rights | Calculate risk | Analysis results

Assets group: **RaT:Railway node**

Threat/Vulnerability	Consequence	Likelihood	Count. class	Count. impl. lev.	Risk (target/current)	Countermeasure cost
Derailment - intentional					**1.50 (6.00)**	**212000 (69000)**
Large areas and facilities	3 (4)	3 (3)	2 (1)	3 (2)	1.50 (6.00)	212000 (69000)
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 protection	? (5)	? (3)	? (1)	? (2)	? (7.50)	69000 (69000)
Large areas and facilities	? (5)	? (3)	? (1)	? (2)	? (7.50)	69000 (69000)

Fig. 8 Example of the AORA analysis for a railway node. (OSCAD screen shot prepared by the author, 2015)

threat-vulnerability, which has certain influence on the asset, the risk value can be determined according to the above presented formula. Inherent risk ("risk before") is in parentheses, while current risk ("after measures applications")—without parentheses. The same rule applies to the cost of countermeasures. Each pair threat-vulnerability is considered a risk register item.

If the risk value is greater than the risk acceptance level, extra (other) countermeasures can be selected (Fig. 9).

The OSCAD-Ciras risk manager allows to consider up to five security measures alternatives (A–E). The decision maker chooses one as the target variant for implementation. Each alternative should be a coherent and applied together package of countermeasures. Examples of such packages are: "CCTV cameras", "Fences", "Police guards", "Security zone" (Fig. 9). The OSCAD risk manager has more features, not discussed here, like setting the assurance class for the countermeasure, along with its status of implementation, cost, etc.

The aim of ABIA is to identify and assess multidirectional impacts of the hazardous event breaching the given asset, e.g. the above mentioned railway node belonging to RaT ECI.

The loss matrix (Fig. 10) is the basic ABIA tool. For each CID, IR, EE subcategory, there are some losses are assessed with the use of 5 levels. A number of subcategories and levels are configurable. As a result of these operations, the CI degradation is assessed.

Additionally, we can identify new threats (or vulnerabilities) caused by a hazardous event:

- in the same infrastructure (IE category); they usually concern assets which are also countermeasures (A = C category); the AORA-ABIA pair must be performed with respect to the breached asset (a barrier), e.g. with respect to a

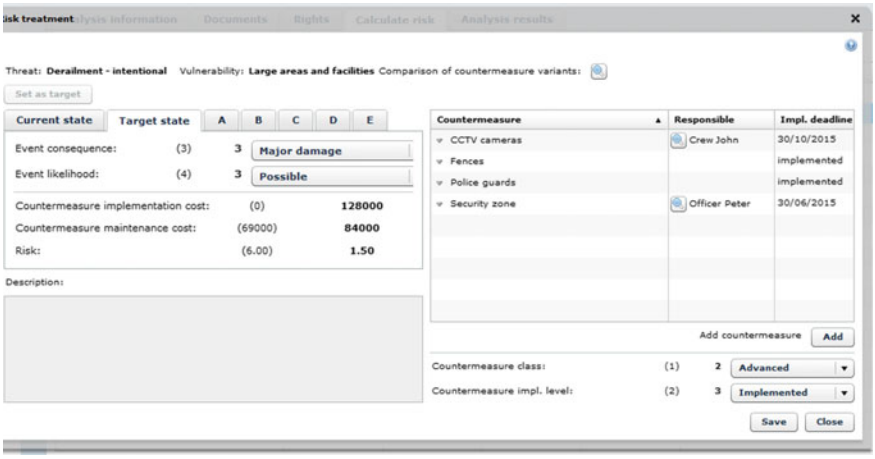


Fig. 9 CI risk management—countermeasures selection in OSCAD-Ciras. (Screen shot prepared by the author, 2015)

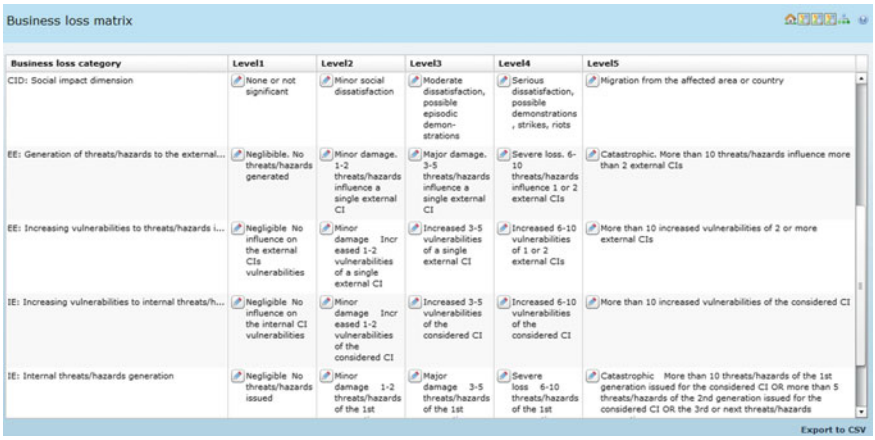


Fig. 10 The loss matrix as the basic BIA tool. (OSCAD screen shot prepared by the author, 2015)

breached security zone (A = C), to identify internal secondary effects resulting from the breach;

- in the dependent infrastructures (EE category); similarly, threats/vulnerabilities which influence external CIs are identified; this requires an extra AORA-ABIA pair for external CIs with respect to the affected asset (EE category).

5.4 Considering the CI Specific Issues in OSCAD-Ciras

OSCAD-Ciras does not have a specific tool to analyze interdependencies, particularly the strength of coupling between CIs. This task must be solved outside the system. One of the ways to do it is to prepare a map of interdependent CIs. With this map it is possible to further analyze the risk within a set of interdependent infrastructures.

OSCAD-Ciras is equipped with facilities allowing to explicitly distinguish CI internal and external causes of hazardous events, internal non-escalating consequences, consequences generating hazards/threats in the same infrastructure, and consequences generating external hazards/threats for other collaborating infrastructures.

Remark 6 Before the risk assessment/management process starts in OSCAD-Ciras, the interdependencies should be known from the perspective of the assessed CI. It should be clear which CIs depend on the given CI (they can be affected) and on which CIs the given CI depends (which CIs can affect the given CI).

6 Conclusions

The paper presents a part of preliminary researches related to the Ciras project. It is focused on the OSCAD-Ciras experimentation tool whose validation is presented in the paper [21]. The presented validation experiment encompasses the following simple scenarios:

1. A hazardous event is triggered in the railway CI causing damages in an important railway node. Apart from the RaT CI degradation (CID), the node security zone is breached (IE) and the coal transport for the neighbor power plant (Ele CI) is blocked in the node (EE).
2. The damaged security zone makes the node more vulnerable to thefts and vandalism. To assess this situation, a pair of AORA-ABIA is launched to check secondary effects (internal escalation) within the railway node.
3. The blocked coal transport (external threat to Ele CI) implies an extra pair AORA-ABIA for Ele CI to check if power production was disturbed (vulnerability: reduced stock of fuel). It is revealed that the power production disturbance affects the railway CI (a negative, backward impact caused by breaching the railway node).
4. The railway power supply is assessed by the next pair of AORA-ABIA, and no extra external escalation is detected because the railway uses redundant power lines.

This short feasibility study confirms the possibility to adapt the ready-made OSCAD platform to CI risk management according to the previously [7] identified requirements. This paper is focused on the experimentation tool, exemplifying it by data examples from the mentioned feasibility study. The ready-made OSCAD software platform was configured and filled in with the data related to the railway CI collaborating with the electricity CI. The data include: assets, threats, vulnerabilities, countermeasures, risk assessment parameters, and formulas.

The OSCAD-Ciras tool offers extensive software support for the risk management process in critical infrastructures. It was the basis of the validation experiment [21] which confirmed the possibility to use it as the RRA component in the Ciras framework. Apart from the data setup, configuration, small GUI modification, no software changes were needed by now. However, for better integration of the RRA, CBA and QCA pillars, such changes will be necessary in the future. They will encompass new web services to exchange information and the GUI extension (see Fig. 9), e.g.:

- to obtain investment costs, future costs and future benefits related to the countermeasures and/or security alternatives from the CBA component,
- to obtain score values related to the countermeasures and/or security alternatives from the QCA component.

These two issues have been solved by the project consortium and are out of scope of this paper.

During the presented preliminary Ciras research, knowledge is gathered about the risk management process in critical infrastructures. It was checked if the proposed approach is useful and how far the CI specific phenomena can be considered. The pros, cons and limitations were identified. All these issues are important to define the final shape of the three pillar based Ciras tool by the consortium members.

The novelty of the paper is to introduce the categorization of the hazardous event consequences, to distinguish the direct CI degradation (CID) and the internal (IE) and external (EE) escalation/cascading effects being the CI specific phenomena. Apart from this, the CID impacts can be assessed in a certain number of predefined time horizons (not discussed here).

The main contribution of the paper is the development of a configurable risk management tool for critical infrastructures. The paper presents how the previously elaborated requirements are implemented on the ready-made software platform. The research includes: domain data identification, elaboration of the software dictionaries, risk manager configuration and validation on the elaborated scenarios.

The paper proposes a new risk assessment method which considers interdependencies between CIs. The research presented in the paper gives substantial contribution to the CIRAS project. During the experiments there was knowledge acquired about the shape of the key component responsible for risk assessment (RRA) of the CIRAS Tool.

These issues need further researches, especially the definition of adequate risk measures. Please note that AORA and ABIA operate on “consequences”. Their definitions must be harmonized. Different variants of these problem solutions are analyzed by the author and by other project team members.

The second open question is how to manage particular risk assessments (pairs of AORA-ABIA). Please note that the launch of a new pair for secondary effects depends on the results of previous assessments—it has dynamic character. The research on the process oriented risk assessment (PORA-PBIA) is also an open issue.

Acknowledgements The author thanks the colleagues from the CIRAS project consortium for discussing the presented concept.

References

1. Białas, A.: Experimentation tool for critical infrastructures risk management. In: Proceedings of the 2015 Federated Conference on Computer Science and Information Systems (FedCSIS), pp. 775–780 ISBN 978-1-4673-4471-5 (Web). IEEE Catalog Number: CFP1385 N-ART (Web)
2. 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

3. Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure. European Commission. Brussels, Aug 28 2013, SWD(2013) 318 final
4. Ciras project, http://cirasproject.eu/ (access date: November 2015)
5. ValueSec project, www.valuesec.eu (access date: November 2015)
6. OSCAD project, http://www.oscad.eu/index.php/en/ (access date: Nov 2015)
7. Bialas, A.: Critical infrastructures risk manager—the basic requirements elaboration. In: Zamojski, W., Mazurkiewicz, J., Sugier, J., Walkowiak, T., Kacprzyk, J. (eds.) Theory and Engineering of Complex Systems and Dependability, Proceedings of the Tenth International Conference on DepCoS-RELCOMEX, June 29–July 3 2015, Brunów, Poland. Advances in Intelligent Systems and Computing, vol. 365, pp. 11–24. Springer, Cham (2015). doi:10.1007978-3-319-19216-1_2
8. Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K.: Identifying, understanding and analyzing critical infrastructure interdependencies. IEEE Control Syst. Mag., 11–25 (2001)
9. Hokstad, P., Utne, I.B., Vatn, J. (Eds): Risk and Interdependencies in Critical Infrastructures: A Guideline for Analysis (Springer Series in Reliability Engineering). Springer, London (2012). doi:10.1007/978-1-4471-4661-2_2
10. Rausand, M.: Risk Assessment: Theory, Methods, and Applications. Series: Statistics in Practice (Book 86). Wiley (2011)
11. Giannopoulos, G., Filippini, R., Schimmer, M.: Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art. European Union (2012)
12. Deliverable D2.1: Common areas of Risk Assessment Methodologies. Euracom (2007)
13. ISO/IEC 31010:2009—Risk Management—Risk Assessment Techniques
14. ENISA: http://rm-inv.enisa.europa.eu/methods. Accessed June 2015
15. Baginski, J., Bialas, A., Rogowski, D. et al.: D1.1—State of the Art of Methods and Tools, CIRAS Deliverable. Responsible: Institute of Innovative Technologies EMAG (February 2015), Dissemination level: RE/CO (i.e. available only for: beneficiaries, stakeholders and European Commission)
16. EN 61025 Fault tree analysis (FTA) (IEC 61025:2006), CENELEC (2007)
17. EN 62502 Event tree analysis (ETA) (IEC 62502:2010), CENELEC (2010)
18. Białas, A.: Risk assessment aspects in mastering the value function of security measures. In: Zamojski, W., Mazurkiewicz, J., Sugier, J., Walkowiak, T., Kacprzyk, J. (eds.) New results in dependability and computer systems. Advances in Intelligent and Soft Computing, vol. 224. Springer, Cham, pp. 25–39. http://link.springer.com/chapter/10.1007%2F978-3-319-00945-2_3#page-1 doi:10.1007/978-3-319-00945-2_3
19. Bialas, A.: Computer support for the railway safety management system—first validation results. In: Zamojski, W., Mazurkiewicz, J., Sugier, J., Walkowiak, T., Kacprzyk, J. (eds.): Proceedings of Ninth International Conference on DepCoS-RELCOMEX. June 30—July 4, 2014, Brunow, Poland. Advances in Intelligent Systems and Computing, vol. 286. Springer, Cham (2014), pp. 81–92. doi:10.1007/978-3-319-07013-1
20. Białas, A.: Business continuity management, information security and assets management in mining, Mechanizacja i Automatyzacja Górnictwa, No 8(510), Instytut Technik Innowacyjnych EMAG, Katowice (2013). English version: pp. 125–138
21. Białas, A.: Research on critical infrastructures risk management. In: Rostański, M., Pikiewicz, P., Buchwald, P. (eds.) Internet in the information Society 2015—10th International Conference Proceedings. Scientific Publishing University of Dąbrowa Górnicza (2015), pp. 93–108