Proceedings of the Federated Conference on
Computer Science and Information Systems pp. 1099–1106

DOI: 10.15439/2015F77
ACSIS, Vol. 5

Experimentation tool for critical infrastructures risk management

Andrzej Bialas
Institute of Innovative
Technologies EMAG,
ul. Leopolda 31,
40-189 Katowice, Poland
Email: andrzej.bialas@ibemag.pl

***Abstract*—The paper concerns a risk assessment and management methodology in critical infrastructures. The research objective is to adapt a ready-made risk manager, supporting information security- and business continuity management systems, to a new domain of application – critical infrastructure protection. First, a review of security issues in critical infrastructures was performed, with special focus on risk management. On this basis the assumptions were discussed how to adapt the OSCAD risk manager designed for the information security/business continuity applications. According to these assumptions, the OSCAD risk manager was adapted to its new domain of application, i.e. critical infrastructures. The aim of this work is to assess the usefulness of such a solution and to elaborate requirements for the advanced critical infrastructure risk manager to be developed from scratch.**

I. Introduction

CRITICAL infrastructures (CIs) consist of large scale infrastructures whose degradation, disruption or destruction would have a serious impact on health, safety, security or well-being of citizens or effective functioning of governments and/or economies. Typical examples of such infrastructures are energy-, oil-, gas-, finance-, transport-, telecommunications-, and health sectors. CIs provide products and services for the society. In order to function, CIs need many different assets. What is more, they are based on complex processes interrelated with other processes across different sectors. CIs are extremely important for effective functioning of today's societies, especially those of well-developed countries. Critical infrastructures ensure proper relationships between citizens and governments. Each society is very sensitive to any disturbance of a CI. Security and safety issues are very important, but due to the CIs complexity, multi-dimensional interdependencies, large scale and heterogeneity, the problems emerging in these areas are often hard to solve.

A CI can be disturbed by different kinds of threats and hazards. The most important are: natural disasters and catastrophes, technical disasters and failures, espionage, international crime, physical- and cyber terrorism. A new, holistic approach to CI protection is applied by programmes and activities which are understood as critical infrastructure protection (CIP). It is a common effort of the infrastructure owners and operators, manufacturers, users, R&D institutions, governments, international bodies and regulatory authorities. The aim of these efforts is to keep the performance of CIs in case of failures, attacks or accidents and minimize the recovery time and damages.

Well developed countries, including the EU countries, pay more and more attention to the protection of their critical infrastructures. The European Council (EC) Directive [1] specifies the CIP related needs on the EU and member state levels. It precisely defines the rules of the CI identification based on casualties-, economic- and public criteria, risk analysis and management programmes. The EC Directive defines the term ECI (European critical infrastructure). ECI means 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:

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

The European Programme for Critical Infrastructure Protection (EPCIP), aimed at both European and national infrastructures, was launched in 2006. The revised and more practical implementation of EPCIP is presented in the EU document [2].

Risk assessment is the basis for critical infrastructures protection programmes. Dozens of EU or worldwide CIP R&D projects which focus on risk methodologies and tools have been completed or are running (FP6, FP7, Horizon 2020, CIPS), which is a proof that the CIP issue is still a challenge.

The researches presented in the paper can be considered preliminary activities of the Ciras[1] project [3]. Ciras was

This work was not supported by any organization

[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).

launched by the international consortium (ATOS, CESS, EMAG) including the author's organization.

The motivation for researches presented in the paper is to elaborate the experimental OSCAD-Ciras tool to get an input for the Ciras project. Particularly, the following aims are planned to be accomplished:

- to implement the requirements [4] on the OSCAD software platform [5] elaborating the CI risk manager to be used as an experimental platform,
- to assess, using near real data, if the basic requirements of the risk manager can be implemented on the OSCAD software, and
- to summarize the whole experiment, acquiring indispensable knowledge about the usability of this risk manager and to identify directions of the future works.

Apart from the requirements identified during the stakeholders' workshop and the reviewed state of the art of the risk management methodology, the Ciras project will get input from the results of this OSCAD-Ciras feasibility study. This input will be used for the Ciras Toolset development.

The paper includes an introduction to risk management in critical infrastructures (section II), summarizes the preferred features of the risk management tool discussed in the work [4] (section III), presents the functionality of the OSCAD software platform (section IV), gives the specifics of OSCAD's adaptation to be a CI risk manager (section V), and finally draws some conclusions for future works.

II. Risk management in critical infrastructures protection

Critical infrastructure is a heterogeneous, distributed, adaptive, and, first and foremost, very complex socio-technical system. Such a system encompasses hardware, software, liveware, environmental, management, and organizational elements. The main objective of a CI is to provide products and/or services for the society. This aim can be accomplished when this complex socio-technical system is well harmonized and the disturbances within the system are under control – the system processes its work smoothly and the assets needed to perform this job are well protected. The CI countermeasures, selected on the risk basis, should be properly managed and composed into CIP programmes.

Collaborating critical infrastructures (systems), e.g. electricity, rail transport, gas, oil, telecommunications, constitute a more complex structure, called a system-of-systems (SoS).

Different mutual dependencies (i.e. interdependencies) between particular CIs exist within SoS too. An interdependency [6] is a bidirectional relationship between two infrastructures (systems) through which the state of each infrastructure influences or is correlated to the state of the other [7].

The CIs failures are usually causally linked – the impacts of incidents may pass across the CIs. Certain CI-specific effects are observed. A cascading effect is [8] a sequence of component failures: the first failure shifts its load to one or more nearby components – these components fail and, in turn, shift their loads to other components. This sequence is repeated. An escalating failure is when there is a disruption in one infrastructure which causes an independent disruption in another infrastructure [6]. The effects of hazardous events may escalate outside the area where they occur and exacerbate the consequences of a given event (generally in the form of increasing the severity or the time for recovery of the second failure). Different failures may have a common cause (failures implied by a single shared cause and coupling to other systems mechanisms) and may occur almost concurrently. 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.

The critical infrastructure protection concept comprises preparedness and response to serious incidents which occur within critical infrastructures. To ensure the preparedness and incident response ability, it is necessary to imply the risk source, character and value. In addition, the right countermeasure should be applied and embedded into the risk management framework, sometimes supported by tools.

The comprehensive approach to risk management in critical infrastructures still remains a challenge, due to CIs complexity, interdependencies, specific effects (common cause failures, cascading, escalating effects), different abstract levels applied to manage CIs, and other factors.

The risk management methodology and tools are a subject of current R&D on the national and international levels, including the EU level. Very comprehensive reviews of R&D results can be found in the following knowledge sources:

- the report [9] of the Institute for the Protection and Security of the Citizen, an 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 [3];
- the EURACOM report [10]; it presents a study of 11 risk assessment methodologies related to the energy sector;
- the book [7]; in its Appendix C there is a comparison of the features of about 22 commonly used risk analysis methods;
- the ISO 31010 standard [11] characterizes about 30 risk assessment methods for different applications;
- the ENISA website [12] includes an inventory of risk management/assessment methods, mostly ICT-focused.

A very exhaustive review of the state of the art is reported in [13]. 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, methods/tools are focused on the confined domain and they do not address properly the holistic view and resilience. The problem is how to consider CIs interdependencies in the risk management process. This requires to distinguish the internal and external causes of hazardous events as well as the internal and external consequences implied by these events.

The survey on the representative methodologies and tools for the CI risk management was made in [4]. Based on these researches, the most favourable features of the CI risk manager are specified in the next section.

III. Preferred Features of Risk Management Tools for Critical Infrastructures

The paper [4] discusses the basic requirements of the risk manager to be applied in critical infrastructure protection. This section gives a short overview of these issues.

A. Conceptual model of the risk manager

The implementation of the bow-tie risk concept in the tool is advantageous for CI risk management [4].

The bow-tie conceptual model [8] embraces both multiple and complex causes of the given hazardous event and 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. As a result, an event may occur which is hazardous for assets. The consequences of such an event are usually diversified and multidirectional. 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/updated barriers are applied.

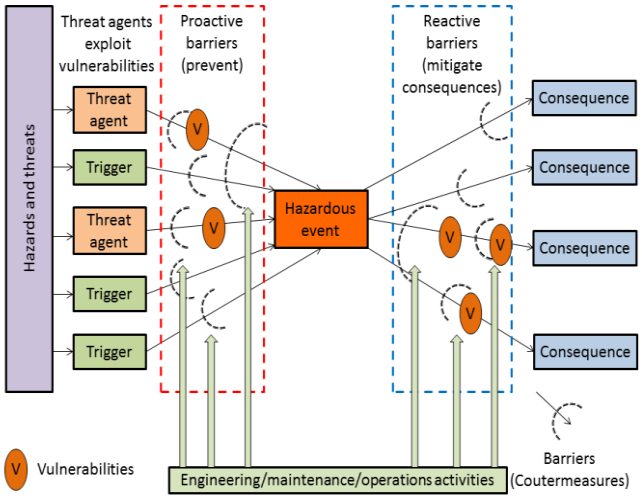


Fig. 1 Bow-tie model

The bow-tie model encompasses the cause analysis and the consequences analysis. These risk analyses can be implemented in less or more complex ways [11], e.g. using FTA (Fault tree analysis) [14] and ETA (Event tree analysis) [15].

There is no analysis of interdependencies in this model, therefore it is necessary to supplement the model in this respect.

B. Risk register and risk related data

The tool should support a CI owner in elaborating and maintaining a risk register as the managed 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. It is used in CIP programmes. There are some data associated with each item of the risk register, like assets, societal critical functions (SCF) ensuring the basic needs of a society (e.g.: life and health, energy supply, law and order, national security), hazards, threats, vulnerabilities, countermeasures, etc.

C. Risk measures and the assessment process

Risk measures depend on the applied methodology. A common method is to assess the likelihood (probability, frequency) of a hazardous event, e.g.: fairly normal, occasional, possible, remote, improbable, and to assess the consequence severity in different dimensions using the enumerative scales, e.g.: negligible, minor, major, catastrophic damages. The risk is the function of both, usually expressed by a risk matrix, as presented in [4].

D. Interdependencies and critical infrastructure specific phenomena

The risk assessment/management methods/tools (Section II) are focused on the given environment with protected assets and processes, and they do not consider interdependencies between other environments. The interdependencies ought to be considered in the risk management process because they are essential for the CI protection. The risk assessment methodology should be able to take into account the CI specific phenomena mentioned in Section II.

IV. Functionality of the OSCAD Software Platform

The identified requirements are experimentally implemented on the OSCAD[2] platform [5]. The OSCAD software was originally elaborated to support business continuity management according to BS 25999 (ISO 22301)

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

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) leading to negative consequences, to limit losses when an incident occurs, and to help in the recovery process.

The solution is open and flexible and thus, after certain modifications, possible to implement in other application domains, e.g.: flood protection [16], railway safety management systems [17] and coal mining [18].

OSCAD offers the following functions:

- general purpose functions: system management, document and tasks management, reporting, dictionaries, business continuity planning, auditing, etc.;
- functions allowing to assess the system effectiveness: acquiring data, assessing effectiveness, permanent improvement actions;
- external communications functions with ERP, SCADA, GSM.

Additionally, OSCAD offers risk management and incident management functions, which are discussed here in the CI context.

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

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

and tools analyzing their multidimensional consequences:

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

Countermeasures are selected based on the assessed risk value and their total investment/maintenance costs. Then the risk is reassessed with respect to the acceptance level.

The incident management functions allow for events acquisition. They also enable to assess their severity according to the elaborated criteria. Serious events, which are incidents, are managed according to standards. The incident statistics and corrective actions are prepared too.

V. Implementation of Risk Manager Requirements on the OSCAD Software

The section discusses the author's proposals how to implement the above-listed requirements into the existing OSCAD software platform.

A. Bow-tie model implementation in the OSCAD software platform

The bow-tie model is not directly implemented in the OSCAD software but its existing 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 analyzes each threat-vulnerability pair which can breach the given asset, while 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.

Examples of analyses pairs composing the bow-tie model are shown in Fig. 2. The "1-1 RaT AORA (Node)" and "1-2 RaT ABIA (Node)" create one of pairs related to the railway node belonging to the Railway transport (RaT) European critical infrastructure (ECI) [1].

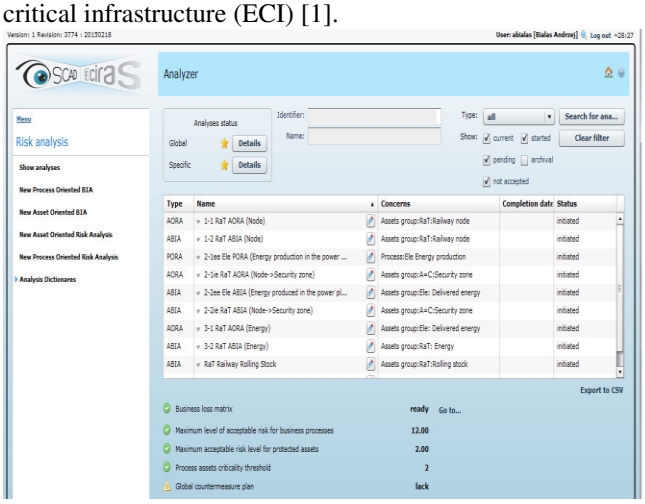


Fig. 2 OSCAD risk analyses composing the bow-tie model

The bow-tie model is rather asset-oriented, similarly to the risk analysis in CIs. For this reason AORA/ABIA may be more convenient for CIs. The given AORA analysis groups the threats related to the given asset. Threats and hazards have the same representation – they are simply the "OSCAD threats". The PORA/PBIA pair represents the process approach. It allows to see a CI from a point of a view of processes, not only assets. Process-oriented risk analyses in CIs need further research.

B. Risk register and risk related data – the OSCAD representation

The basic risk-related data are assets belonging to the critical infrastructures which need protection.

The general CIs taxonomy and assets are implemented in OSCAD. Two groups of CIs are distinguished: ECI (European CI), embraced by the EU Directive [1] and others (non-ECI). Currently only the ECI ones are implemented.

In OSCAD the protected assets dictionary is a simple flat list. For this reason, the assets belonging to the given CI 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). Figure 3 presents different assets, belonging to the ECI, distinguished according to their labels. Each protected asset can be the central point of any AORA or ABIA. They play a

role of primary assets. Please note three attributes CID (CI degradation), IE (Internal escalations), EE (external escalations) which express three types of consequences when the given asset is breached (this will be explained later, when ABIA/PBIA will be discussed).

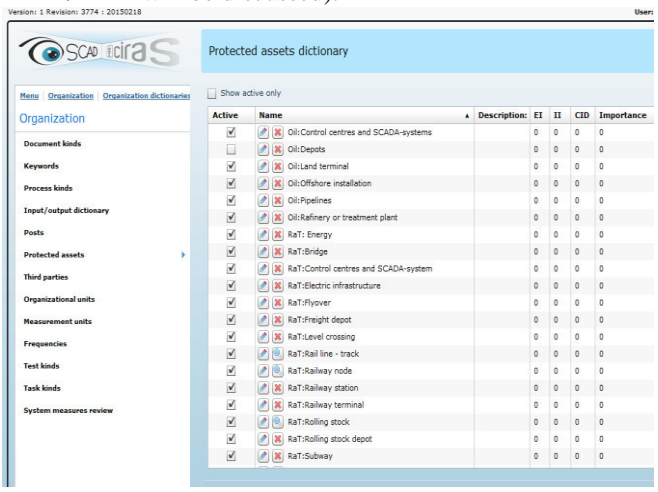


Fig. 3 Protected assets of ECIs in the OSCAD software

It is possible to create a group of the related secondary assets (technical, personal, immaterial, playing role of countermeasures, etc.) around the given primary asset. This group of assets can be defined in the assets inventory module (Fig. 4). The Railway node asset is represented by a node located in the city of Tarnowskie Góry (Upper Silesia, Poland).

For each of the protected assets, the AORA analysis can be performed. PORA can be done for the processes (not discussed here) in a similar way.

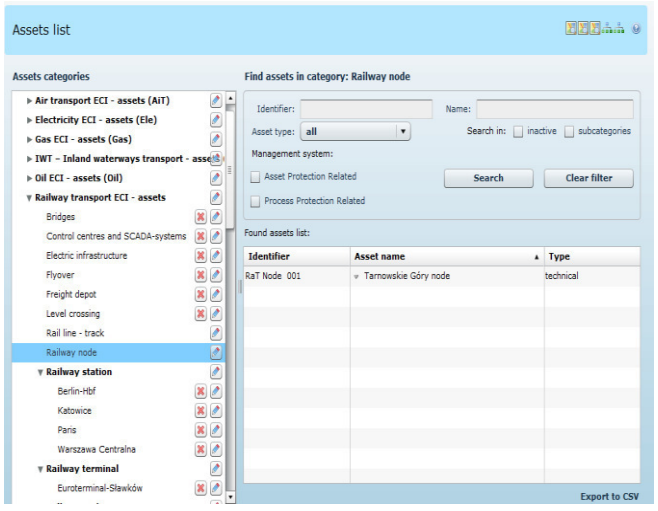


Fig. 4 Different assets belonging to the given protected assets category

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 when internal escalation effects are analyzed (will be explained further).

The general formula of the threats/hazards scenario is:

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

Assuming that a threat agent is identified as the hazard trigger, the common description of threats and hazards is possible in OSCAD. The threat specification includes key terms essential for the risk analysis. Threats specified during the AORA/PORA analyses are considered risk register items. OSCAD is equipped with 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 (not discussed here).

Summing up, the risk register is defined in OSCAD as a set of risk scenarios worked out during AORA or PORA, and compatible with the incident inventory.

OSCAD has predefined lists of threats, vulnerabilities and countermeasures. They are flat, but a special grouping mechanism is applied as the hierarchical grouping dictionary. On the upper hierarchy level threats can be ordered according to critical infrastructures, next according to these threats character (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 counter-measures (C) can be assigned. These predefined relations speed up the countermeasures selection.

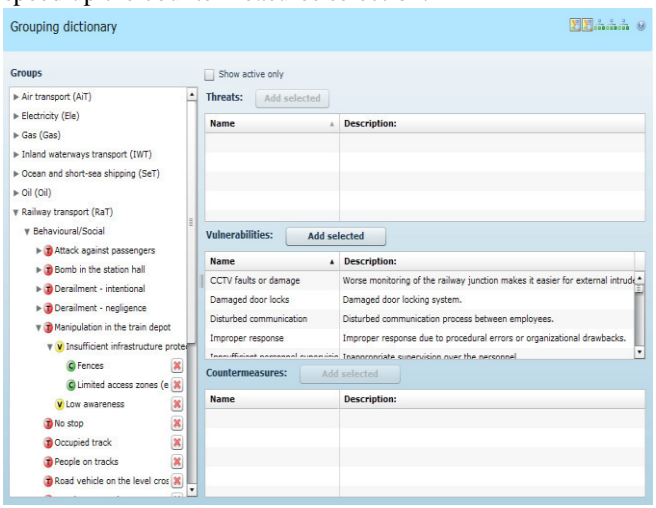


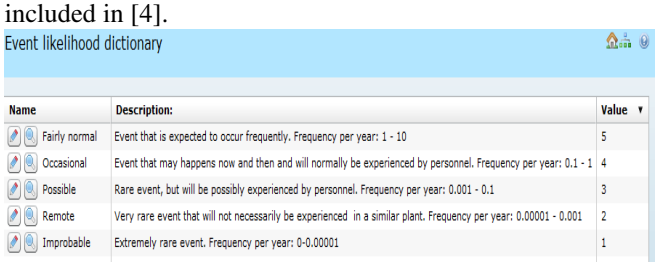
Fig. 5 Grouping dictionary with rail transport relevant data

Figure 5 presents the hierarchical structure of the grouping dictionary and some examples concerning railway transport.

C. Risk measures and assessment process in the OSCAD software

For the AORA and PORA analyses two issues should be defined: likelihood of the event (Fig. 6) and its consequences (Fig. 7).

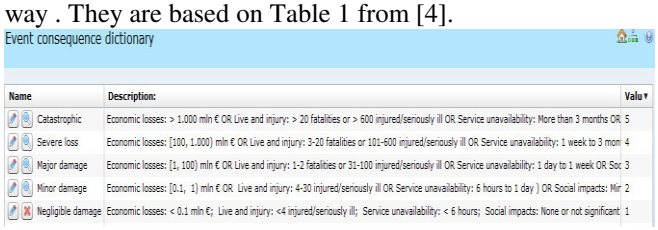
Event likelihood measures with their interpretation are direct implementation of the measures presented in Table 2 included in [4].


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

Fig. 6 Event likelihood measures

The consequences measures are implemented in the same way . They are based on Table 1 from [4].


Event consequence dictionary

Name	Description:	Valu
Catastrophic	Economic losses: > 1.000 mln € OR Live and injury: > 20 fatalities or > 600 injured/seriously ill OR Service unavailability: More than 3 months OR	5
Severe loss	Economic losses: [100, 1.000) mln € OR Live and injury: 3-20 fatalities or 101-600 injured/seriously ill OR Service unavailability: 1 week to 3 mon	4
Major damage	Economic losses: [1, 100) mln € OR Live and injury: 1-2 fatalities or 31-100 injured/seriously ill OR Service unavailability: 1 day to 1 week OR Soc	3
Minor damage	Economic losses: [0.1, 1) mln € OR Live and injury: 4-30 injured/seriously ill OR Service unavailability: 6 hours to 1 day) OR Social impacts: Mir	2
Negligible damage	Economic losses: < 0.1 mln €; Live and injury: <4 injured/seriously ill; Service unavailability: < 6 hours; Social impacts: None or not significant	1

Fig. 7 Event consequences measures

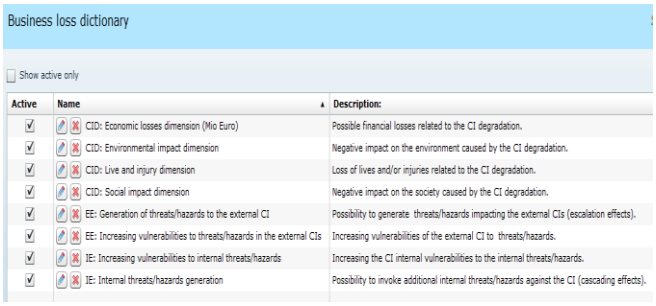
The risk value (AORA/PORA) is calculated with the use of the simple formula:

$$\text{Risk} = \frac{\text{Event likelihood} * \text{Event consequences}}{\text{Countermeasure class} * \text{Countermeasure impl.lev.}}$$

The "Countermeasure class", if used, i.e. when it is > 1, can express countermeasure assurance (basic, advanced). The "Countermeasure implementation level" expresses the stage of the implementation (not implemented, partially, fully implemented). These two additional parameters are used for more advanced applications.

The measures of multidimensional consequences of the hazardous event (Fig. 8) are key issues for the ABIA/PBIA analyses. Three groups of consequences are distinguished. The basic one is the CID (CI degradation) category which expresses different kinds of damages within the given CI. To consider the CI specific effects analyses, two additional categories are introduced:

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


Business loss dictionary

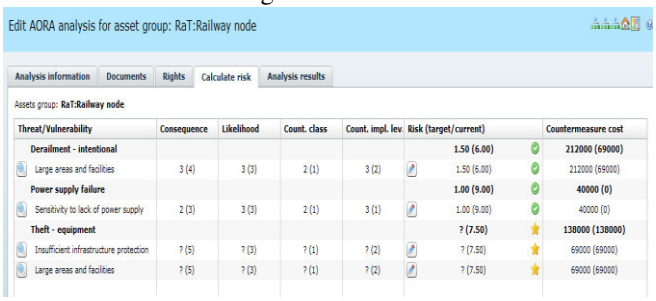
Show active only

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. 8 Event impacts measures with CID, IE and EE categories

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.

AORA is shown in Fig. 9.


Edit AORA analysis for asset group: RaT:Railway node

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

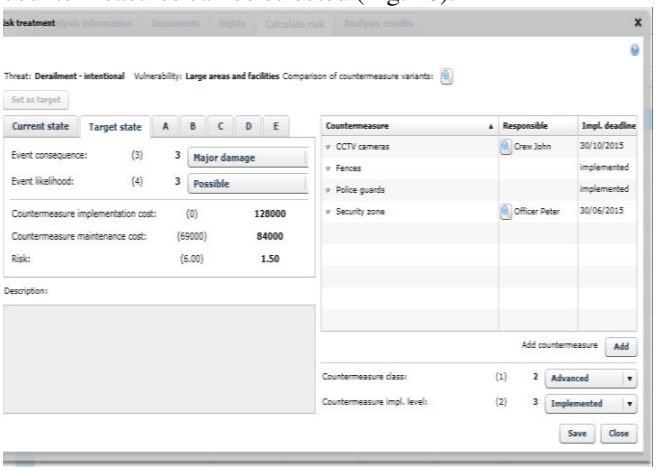
Assets group: RaT:Railway node

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. 9 Example of the AORA analysis for a railway node

Please note three threats (Derailment – intentional, Power supply failure, Theft – equipment) and vulnerabilities associated with them. For each pair threat-vulnerability, which influences the asset, the risk value can be determined according to the above presented formula. Inherent risk ("risk before") is in parentheses, while the 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 unaccepted, extra (other) countermeasures can be selected (Fig. 10).


Threat: Derailment - intentional Vulnerability: Large areas and facilities Comparison of countermeasure variants:

Set as target

Current state | Target state | A | B | C | D | E

Event consequence: (3) 3 Major damage

Event likelihood: (4) 3 Possible

Countermeasure implementation cost: (0) 128000

Countermeasure maintenance cost: (69000) 84000

Risk: (6.00) 1.50

Description:

Countermeasure	Responsible	Impl. deadline
CCTV cameras	Crew John	30/10/2015
Fences		implemented
Police guards		implemented
Security zone	Officer Peter	30/06/2015

Add countermeasure Add

Countermeasure class: (1) 2 Advanced

Countermeasure impl. level: (2) 3 Implemented

Save Close

Fig. 10 CI risk management – countermeasures selection

The risk manager can consider up to five variants of decisions with respect to the possible risk reduction and the cost of this reduction.

The next step is the consequences analysis of a given hazardous event embraced by ABIA. It is possible to apply ABIA in the case of each hazardous event, but in most cases it will be more convenient to perform ABIA according to assets.

The basic ABIA tool is the loss matrix (Fig. 11). For each subcategory of CID, IR, EE, losses are assessed with the use of 5 levels. A number of subcategories and levels are configurable. As a result, the CI degradation is assessed.

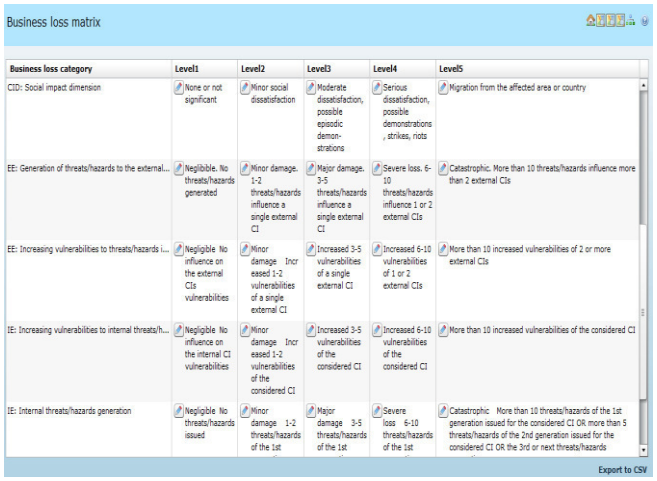


Fig. 11 Use of the loss matrix during BIA

Additionally, we can identify new threats (or vulnerabilities) caused by a hazardous event. These breaches usually concern assets which are also countermeasures (C=A category). Here AORA-ABIA must be performed with respect to the given asset to identify internal escalation or cascading consequences. Similarly, threats/vulnerabilities which influenced external CIs are identified. This requires extra AORA-ABIA for external CIs with respect to the influenced asset.

Fig. 12 presents an example of a risk assessment scenario driven by CIs phenomena:

1. In CI#n an external event occurs and triggers the hazardous event HE(#n,#m) impacting the primary asset #m which belongs to this infrastructure.
2. AORA(#m) identifies the risk related to this hazardous event, while ABIA(#m) – its multidimensional consequences. The internal degradation caused by the HE(#n,#m) is assessed (CID). ABIA identifies that this event breaches the security zone (#m->#k) which is a secondary asset of #m (IE) and influences the external infrastructure #p (EE).
3. Due to the internal escalation (IE) an extra analysis of the secondary asset (#m->#k), playing the role of a countermeasure, is required: AORA(#m->#k)-ABIA(#m->#k). The related ABIA identifies CI degradation caused by the security zone breaching but does not identify any further IE or EE impacts.
4. Due to the external escalation (EE) an extra analysis of asset #s of the CI#p is performed: AORA(#s)-ABIA(#s). The related ABIA identifies the CI degradation caused by an externally generated threat but does not identify any internal impacts (IE). Moreover, the backward external impacts to the infrastructure #n are identified.
5. Due to the external threat generated by the CI #p for the CI#n on its primary asset #z, an extra pair of analyses is issued: AORA(#z)-ABIA(#z). The CI internal degradation is assessed, and no internal/ external escalations are detected.

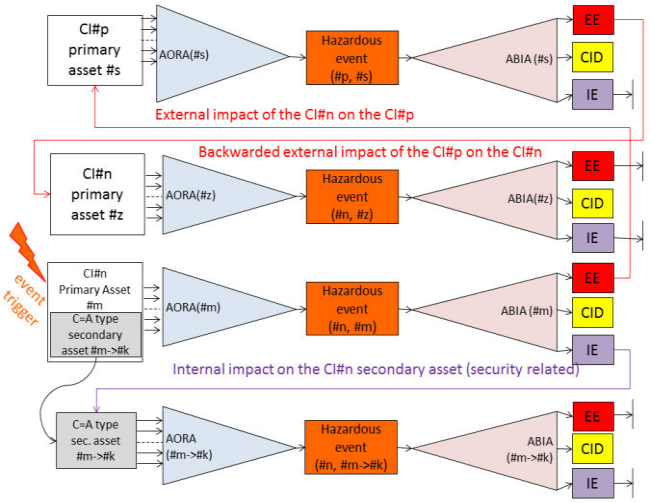


Fig. 12 Risk management in interdependent critical infrastructures

This scenario shows a general plan of analyses driven by the situations occurring in the interdependent CIs.

D. Interdependencies and critical infrastructure specific phenomena

There is no specific tool in OSCAD to analyze interdependencies, especially the strength of coupling inside CIs. This task should be solved outside the system, e.g. by preparing a map of interdependent CIs. Using this map it is possible to further analyze risk within a set of interdependent infrastructures, which was shown in Section V, subsection C.

There is a mechanism introduced that allows to explicitly distinguish CI internal and external causes of hazardous events, and to distinguish CI internal non-escalating consequences, consequences generating hazards/threats in the same infrastructure, and consequences generating external hazards/threats for other collaborating infrastructures.

VI. Conclusions

The short feasibility study provided in the paper confirms a possibility to adapt the ready-made OSCAD platform for CI risk management according to the previously [4] identified requirements.

The CI related data were prepared and implemented in the system. Some OSCAD functions and system messages were changed to better express the CI domain. No software changes were needed. Most of the required functionalities of the CI risk manager were successfully implemented. This way the OSCAD-Ciras tool was prepared for further researches.

The key advantage of the presented method, which allows to consider effects implied by interdependencies in risk management, is to distinguish the direct CI degradation (CID) and the internal (IE) and external (EE) escalation/cascading effects.

As far as more complicated CIs relationships are concerned, more iterations of analyses are needed. Here it is required to introduce identifiers of particular analyses, additional managing and reporting. The Ciras-OSCAD tool is currently used to elaborate use cases in the CIRAS project and to design the Ciras Toolset. The OSCAD tool can be integrated into the toolset but should be supported in the range of analyses and interdependencies management. More experiments based on the elaborated use cases are planned.

ACKNOWLEDGMENT

The author thanks the colleagues from the CIRAS project consortium for reviewing this paper and discussing the presented concept.

REFERENCES

[1] 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 (2008).

[2] 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

[3] Ciras project: http://Cirasproject.eu/content/project-topic (access date: June 2015).

[4] 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 Dependability and Complex Systems DepCoS-RELCOMEX, June 29 – July 3 2015, Brunów, Poland,* Advances in Intelligent Systems and Computing Vol. 365, 2015, Springer-Verlag: Cham, Heidelberg, New York, Dordrecht, London, pp. 11-24, DOI: 10.1007978-3-319-19216-1_2.

[5] OSCAD project: http://www.oscad.eu/index.php/en/ (access date: June 2015).

[6] Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K.: Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*. December, 11–25 (2001).

[7] Hokstad, P., Utne, I.B., Vatn, J. (Eds): *Risk and Interdependencies in Critical Infrastructures: A Guideline for Analysis* (Springer Series in Reliability Engineering). Springer-Verlag London (2012), DOI: 10.1007/978-1-4471-4661-2_2.

[8] Rausand, M., *Risk Assessment: Theory, Methods, and Applications*. Series: Statistics in Practice (Book 86), Wiley (2011).

[9] Giannopoulos, G., Filippini, R., Schimmer, M.: *Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art*. European Union (2012).

[10] Deliverable D2.1: Common areas of Risk Assessment Methodologies. Euracom (2007).

[11] ISO/IEC 31010:2009 – Risk Management – Risk Assessment Techniques.

[12] ENISA: http://rm-inv.enisa.europa.eu/methods (access date: June 2015).

[13] D1.1 State of the Art of Methods and Tools, Ciras report (Dissem. level: RE/CO), 2015.

[14] EN 61025 Fault tree analysis (FTA) (IEC 61025:2006), CENELEC (2007).

[15] EN 62502 Event tree analysis (ETA) (IEC 62502:2010), CENELEC (2010).

[16] 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, 2013, Springer-Verlag: Cham, Heidelberg, New York, Dordrecht, London, 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.

[17] 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 Dependability and Complex Systems DepCoS-RELCOMEX. June 30 – July 4, 2014, Brunow, Poland*, Advances in Intelligent Systems and Computing Vol. 286, Springer Cham, Heidelberg, New York, Dordrecht, London, 2014, ISBN 978-3-319-07012-4, DOI 10.1007/978-3-319-07013-1, pp. 81-92.

[18] Białas A.: Business continuity management, information security and assets management in mining, *Mechanizacja i Automatyzacja Górnictwa*, Nr 8(510), 2013, Instytut Technik Innowacyjnych EMAG, Katowice, English version: pp. 125-138.