Critical Infrastructure Protection—How to Assess the Protection Efficiency

Andrzej Bialas

Abstract The paper presents a concept how to assess the effectiveness of critical infrastructure protection systems. At the beginning the main issues related to critical infrastructure protection are discussed, like resilience, interdependencies, dire phenomena caused by them, and risk management. Next, the state of the art is reviewed. It embraces frameworks, methods and tools related to infrastructures protection, especially risk management. The paper extends the researches of the EU CIRAS project beyond the risk management issue, proposing a method to assess the effectiveness of countermeasures selected for implementation. The concept is based on supplementing the risk management framework by incident management, incident statistics and effectiveness indicators presenting relevant parameters for decisions makers. To implement this concept, the CIRAS risk management software platform should be extended. Main categories of statistics and indicators dedicated for critical infrastructures are proposed. In the conclusion the concept is summarized and future works related to its validation is specified.

Keywords Critical infrastructure · Resilience · Risk management · Interdependencies · Incident management · Effectiveness indicators

1 Introduction

The paper concerns critical infrastructures (CIs) protection. CIs are 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. The examples of CIs are infrastructures providing services in the energy-, oil-, gas-, finance-, transport-, telecommunications- and health sectors.

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

W. Zamojski et al. (eds.), *Dependability Engineering and Complex Systems*,
Advances in Intelligent Systems and Computing 470,
DOI 10.1007/978-3-319-39639-2_3

The processes which provide these services are based on different assets: technological, IT hardware, software, environmental, personal, and organizational. 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 on multiple levels, which evolve over time [1].

The processes providing services are interrelated with other processes across different economy sectors. Special terms—dependencies and interdependencies—were introduced in the CI domain. Dependency defines a unidirectional relationship between two infrastructures, e.g. the telecommunications CI is dependent on the energy CI, because to function properly telecommunications needs energy. Interdependencies are much more complicated. They represent a set of different mutual and bidirectional relations existing in the set of co-operating infrastructures. The strength of coupling between particular CIs may vary.

Critical infrastructures are crucial for the functioning of a society and economy. The CIs processes may be disturbed, and their assets breached by different threats and hazards, such as: natural disasters and catastrophes, technical disasters and failures, espionage, international crime, physical- and cyber terrorism. This is deep motivation to develop critical infrastructure protection (CIP) programmes on the national or international levels. Creating and implementing these programmes is difficult due to the CIs complexity, existing interdependencies and cross-sectoral relations. Risk management is the key issue to create the CIP systems, because the identified risk is the basic factor during the selection of countermeasures which mitigate risk.

The existing risk management methods and tools, used to protect CIs, were mainly developed for business or public organizations, not especially for CIs—this is a conclusion from their review presented in Sect. 2. Critical infrastructures are much more complex than business organizations. Particular CIs do not embrace single organizations (CI operators) but their groups, and, moreover, they are connected to each other by a huge number of relationships, sometimes even unknown. Operational CIs are included in more general structures to be considered on the national or even on international levels.

The paper concerns the European CIRAS[1] project [2] related to “The Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme—CIPS”. CIRAS is performed by the international consortium, including the author’s organization:

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

[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).

The CIRAS method and tool are based on the FP7 ValueSec approach [3]. The countermeasures selected for implementation in critical infrastructures should satisfy the following requirements:

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

To satisfy these requirements the CIRAS Tool was equipped with dedicated components:

- Risk Reduction Assessment (RRA) which assesses risk before and after the countermeasure implementation,
- Cost-Benefit Assessment (CBA) which assesses cost and benefits factors (monetary, tangible) in the given time horizon after the countermeasure implementation,
- Qualitative Criteria Assessment (QCA) which assesses intangible factors that may occur after the countermeasure implementation.

CIRAS focuses on the countermeasures selection, which is the central issue of risk management. This selection is understood as a single act of the decision maker and continuous, security and safety management aspects are not considered here. CIRAS does not refer to other important issues related to CIP, e.g.: resilience, incident management, effectiveness of the applied countermeasures, and CIP management aspects like: planning, implementing, monitoring, correcting, improving.

This was the motivation to work on an extension of the CIRAS methodology towards the CIP management framework, which would be able to plan, implement, monitor and maintain the CI protection on the assumed level.

The objective of the paper is to propose a method and tool to assess the effectiveness of the CI protection system. This protection is based on the applied countermeasures and on the protection management activities. The protection effectiveness rises when the number of incidents and related losses decreases. In the paper it is assumed that the effectiveness of the CI protection system can be assessed with the use of statistics of incidents and effectiveness indicators. The statistics and indicators are the basis to define correction and improvement actions in the CI protection system. The incident management is important as well. It delivers data to build statistics, to feed indicators, and to allow immediate reaction to security problems.

When the protection decreases below the acceptance level the CI protection system needs corrections and improvements, and when it considerably increases above the acceptance level, it is possible to economize the protection cost.

The results of the author’s researches can be used as input to indicate directions of the CIRAS project in the future.

The paper includes the state of the art summary (Sect. 2), the concept of effectiveness assessment for countermeasures (Sect. 3), its implementation on the ready-made software platform (Sect. 4), and conclusions.

2 State of the Art

The review was focused on:

- CI-specific issues, like resilience, interdependencies and related effects,
- risk management methods and tools, especially those used in CIs,
- CIP frameworks and projects.

Critical infrastructure resilience concerns its ability to mitigate the magnitude or duration of hazardous events. The resilient CI is resistant to external and internal disturbances and can function on an acceptable efficiency level in the face of a hazardous event. It means that the CI is able to predict, absorb, react, adapt itself to critical situations, or recover after the disruptive event.

Resilience frameworks [4] are based on best practices and encompass methods and/or tools to perform the system analysis, interdependencies analysis and risk management. Building the CI resilience is a process which includes the following stages:

1. Structural analysis of the CI as a system of systems.
   It is focused on the CIs static model elaboration, i.e. most important nodes, most vulnerable nodes, dependencies and interdependencies (direct, indirect) are identified and expressed by criticality-, vulnerability-, dependency directed graphs or matrices.
2. Dynamic analysis of the CI.
   Based on the static model, the scenarios essential for the CI resilience are analyzed, like: recovering after the given event in the given time, identification of threats impacts, analyses of common failures, the system response to a failure or an incident. The event driven dynamics method is used. The qualitative approach is based on the concurrent event sequence diagrams. When the quantitative approach is applied, simulation tools are used. As a result, a set of the most dangerous risk scenarios is identified.
3. Prioritization of risk scenarios.
   The identified risk scenarios are ordered according to their harmful consequences and prepared to the risk management process in which the detailed analysis is conducted and countermeasures are selected.
4. Risk management.
   The selected and prioritized risk scenarios are analyzed, the risk value assessed, and the right countermeasures selected.

The existing frameworks are focused on the resilience building as a one-time act, not on the resilience maintenance over the time by continuous management activities.

Researches [5, 6] distinguish four basic kinds of interdependencies: physical, cyber, geographical, and logical ones. Because of interdependencies, dire effects of hazardous events propagate across the collaborating infrastructures causing CI-specific phenomena, like: cascading effects, escalating failures, common cause failures [5, 7]. Interdependencies and dependencies are expressed by matrices of relationships or by dependency graphs [4]. The interdependencies analysis is the key issue in building the CI resilience.

The first task of the CIRAS project concerned an exhaustive review of laws, standards, frameworks, methods and tools [8]. This review was based mainly on the following knowledge sources:

- the report [9] of the Institute for the Protection and Security of the Citizen, one of the EC Joint Research Centres (JRC); the report assesses and summarizes 21 existing risk management methodologies/tools on the EU and global level, identifies their gaps and prepares the ground for R&D in this field;
- the book [6]; Appendix C compares the features of about 22 commonly used risk analysis methods;
- the EURACOM report [10] features a desktop study of 11 risk assessment methodologies related to the energy sector;
- the ISO 31010 standard [11] describes about 30 risk assessment methods for different applications;
- the ENISA website [12] gives an inventory of risk management/assessment methods, mostly ICT-focused;
- projects performed on international and national levels (about 20 projects);
- frameworks used by the leading countries in this domain, e.g. [4, 10, 13–16].

From the CI protection perspective the risk management method/tool should: consider interdependencies and phenomena related to them, analyze consequences and causes of the given hazardous event, express the most important data included in the risk register understood here as the managed inventory of hazardous events, be flexible for configuration of different parameters, e.g.: likelihood, probability, frequency, consequences, their categories, scales of measures. The existing methods/tools were developed for single business organizations, not for a set of collaborating organizations, like CIs. Some methods/tools were adapted for the critical infrastructures requirements, especially for the lower level of the CI hierarchy (e.g. operator level). There is lack of risk management method/tools for the higher level (e.g. international level). The reviewed methods [8] do not address the CI specific phenomena in a satisfactory way. There is no method which would consider the cost, benefit, and intangible restrictions with respect to the CIs.

The CIs resilience- or risk management frameworks are defined on a very general level. There are no comprehensive critical infrastructure protection frameworks that would take into account all aspects important for CIs like: resilience, interdependencies, risk management in all important perspectives (planning, implementing, maintaining, improving). Particular frameworks focus on the selected aspects, e.g., risk management [16], resilience building or interdependencies [4]. The US Dept. of Homeland Security framework [13, 14] represents a comprehensive approach to the risk-based resilience building and maintenance, including feedback loops and iterative steps. One of the risk management activities is to measure effectiveness. Metrics and evaluation procedures are used to measure progress and assess the effectiveness of the efforts to secure and strengthen the resilience of a critical infrastructure. Measures of effectiveness, indicators are broadly used in information security or IT governance standards, like ISO/IEC 27001 [17] or COBIT [18]. None of the frameworks was based on the Deming cycle [19], which is a proven solution to manage and maintain quality, security, business continuity, etc.

3 Critical Infrastructure Protection Framework Effectiveness—Concept of Assessment

The effectiveness of a CI protection system rises when damages caused by incidents and protection costs decrease. The problem is that to decrease damages, the risk should be better reduced and this rises the protection cost too. A trade-off between different factors is needed, and these factors should be identified and monitored. Sampling all these parameters in an aggregated way supports the decision makers involved in the management of critical infrastructures protection systems.

The countermeasures should be properly selected to achieve the security/safety on the accepted level. The countermeasures selection is based on the ability to reduce risk. In the developed CIRAS Tool, the cost-benefits parameters and intangible factors are taken into account too. CIRAS does not go beyond the countermeasure selection. This is considered as a one-time act. There are no operations to maintain the achieved security over time—this issue is out of this project scope.

Please note that incidents within a protected system, like a CI, are still possible, due to a few factors:

- during risk assessment a mistake or an inaccuracy may occur; please note that methods and tools used in the CI domain are rather simple, while the domain is complex,
- new threats or vulnerabilities appear, previously unknown or omitted,
- changes in CI occur and for this reason the protection system does not match the situation after changes,
- risk is ignored (this option is not recommended).

For this reason the entire protection system which embraces a set of different but coherent countermeasures should be monitored, managed and corrected to minimize incidents and their impacts. The problem is solved in security management systems [17], IT governance systems [18] and in many other management systems related to business or public organizations, but not for critical infrastructures.

To solve this issue, the critical infrastructure and its protection system should be equipped with management facilities, especially with:

- an incident management system which should be able to identify the incident, to react, to do lessons learnt, and to derive corrections in the protection system,
- different incident assessment facilities and indicators, working like sensors, track parameters relevant to the effectiveness of the whole system and are able to monitor the effectiveness of the protection system.

To assess the effectiveness of the protection system, the number of incidents (materialized risk scenarios) and their consequences in different views should be observed. An incident management system provides these data, however, the data should be processed and presented in an aggregated way, e.g. as on-line statistics or graphs. Incidents observation and on-line reaction are close to the real-time risk management concept.

Indicators can be monitored on line to react immediately when something goes wrong, or can be analyzed in the assumed time horizons, e.g. yearly, to improve the existing protection system.

Statistics and indicators can be useful in periodical risk reassessment (a static approach). Risk prediction can be confronted with the occurred incidents (materialized risks) to elaborate more adequate predictions (and countermeasures) for the future. Information about the countermeasures past and future costs is also useful. This allows to optimize protection costs which influence the protection system effectiveness.

It is assumed that the effectiveness assessment of the CI protection system is based on different sources of information needed for decision makers and other people responsible for the CI protection. The basic sources of information showing this effectiveness are:

- incident statistics,
- indicators,
- the cost of the protection system.

The assessment results are the foundation of correction actions and continual improvement of the protection system.

4 Protection Framework Effectiveness Assessment—Implementation

To make a feasibility study of the above effectiveness assessment concept, the author proposes to use the OSCAD software platform [20]—the same as the one used in the RRA component in the CIRAS Tool.

The paper is continuation of researches focused on the OSCAD application in the CIRAS project. Current researches are focused on risk management. The paper [21] presents the requirement for the CI risk manager, [22] presents the experimentation tool based on these requirements, and [23] is focused on the validation experiment dealing with the risk management in the collaborating infrastructures. As a result the OSCAD-based RRA component is proposed which is currently adapted to and embedded into the CIRAS Tool. The experimentation risk manager is called here OSCAD-CIRAS. The paper proposes to go beyond the risk management research and to extend OSCAD-CIRAS by a new functionality to measure the effectiveness of the protection system.

The OSCAD software was originally developed as an integrated system to support:

- business continuity management according to ISO 22301 [24], to identify and mitigate different disturbances of business processes,
- information security management according to ISO/IEC 27001 [17], to identify and mitigate breaches of information assets.

OSCAD was developed for business or public organizations and it has three main functionalities:

- to perform risk management (preparedness),
- to manage incidents (reaction, recovery),
- to ensure continual improvement of the security-related management processes.

4.1 Information from Incident Management System Useful in the Effectiveness Assessment

OSCAD is equipped with a complex event/incident management system. Events are reported and evaluated. Some of them, bringing higher damages, are classified as incidents. The event circumstances and causes are specified. OSCAD helps to react when incidents occur. In this case, for serious incidents, ready-to-use emergency plans can be activated. Closed incidents are assessed again (lessons learnt) to plan corrective actions within the protection system. The incident reports are sampled in the database to produce statistics.

Figure 1 shows two simple statistics issued: events by weekdays and kinds of events (police interventions, non-classified, failures, other events). The example deals with the Railway Safety Management System [25]. Similar statistics will be created for CIs, however, to obtain reliable statistics, the data should be sampled over long time.

For critical infrastructures the examples of statistics can be created around the following:

- number of incidents of the given severity and category,
- losses from incidents of the given severity and category,

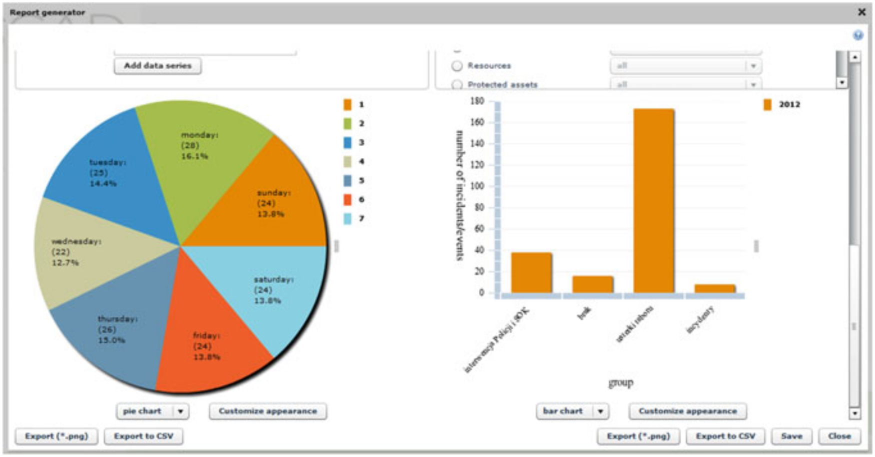

○ Resources all
○ Protected assets all

Fig. 1 Events by weekdays and kinds of events [25]. *Source* OSCAD. Prepared by the author, 2014

- number of unresolved incidents,
- total number of incidents,
- total losses caused by incidents.

The severity related to the damages caused by the event/incident can be defined similarly to the consequences severity used in the risk assessment. For example, events can be classified with the use of the enumerative scale [21]: Negligible damage, Minor damage, Major damage, Severe loss, Catastrophic.

Incidents are a subset of events of higher damages: Major damage, Severe loss, Catastrophic.

It is proposed that the categories of risk (threats) [22, 23] should comply with the categories of events/incidents. This way it is possible to compare predicted risks with incidents (materialized risks) and get extra information about the effectiveness of the protection system.

The incident statistics are a source of information to plan corrective actions in the CI protection system.

4.2 *Indicators Expressing the Effectiveness of the Protection System*

OSCAD-CIRAS can be equipped with indicators, including the user defined variables, which sample relevant values. The value of the given effectiveness indicator can be:

- entered manually by the user,
- downloaded automatically, e.g. from telematics applications, from ERP (Enterprise Resource Planning), from SCADA (Supervisory Control And Data Acquisition),
- calculated on the basis of the existing data (incident records, statistics) as aggregated values.

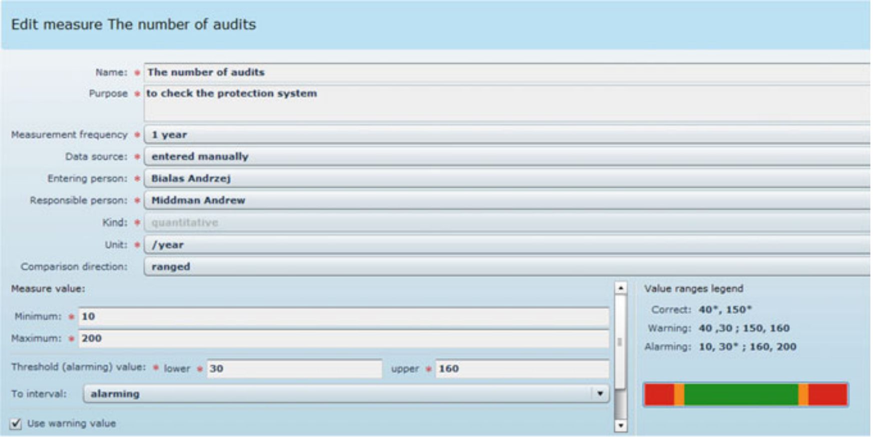
Indicators represent security, safety, reliability, resilience, technical and management issues. OSCAD is equipped with these mechanisms but the adequate indicators should be defined during the planned researches.

The first group of examples concerns the basic indicators or their families:

- average reaction time to an incident of the given severity and category,
- maximal reaction time to an incident of the given severity and category,
- average recovery time per incident category,
- average recovery cost per incident category,
- total recovery cost,
- number of audits, reviews, correction actions in the protection system,
- number of false alarms,
- number of incidents related to dangerous products, e.g. chemical, nuclear,
- number of deaths,
- number of persons seriously injured,
- number of incidents when RTO (Recovery Time Objective) was exceeded,
- number of precursors of incidents, near-failures,
- volume of compensation related to insurance,
- economic efficiency factors, e.g. volume of transported goods, produced energy, provided services per year,
- percentage of the state-of-the art countermeasures (modern, certified, automatic, etc.) in the protection system,
- percentage of CCTV cameras with video analysis with respect to the total number of cameras,
- number of security awareness activities, trainings for employees in the given time horizon.

The second group of indicators is defined to check the CI specific phenomena, e.g. internal and external escalation/cascading, common cause effects:

- number of incidents caused by external critical infrastructures through interdependencies,
- volume of losses due to incidents caused by external critical infrastructures through interdependencies,
- number of incidents invoked in external critical infrastructures through interdependencies,
- volume of losses due to incidents caused by external critical infrastructures through interdependencies,



Edit measure The number of audits

Name: * The number of audits

Purpose * to check the protection system

Measurement frequency * 1 year

Data source: * entered manually

Entering person: * Bialas Andrzej

Responsible person: * Middman Andrew

Kind: * quantitative

Unit: * /year

Comparison direction: ranged

Measure value:

Minimum: * 10

Maximum: * 200

Threshold (alarming) value: * lower * 30 upper * 160

To interval: alarming

☑ Use warning value

Value ranges legend

Correct: 40*, 150*

Warning: 40 ,30 ; 150, 160

Alarming: 10, 30* ; 160, 200

Fig. 2 Effectiveness indicator—an example. *Source* OSCAD-CIRAS. Prepared by the author, 2016

- number of internally escalated incidents,
- number of detected common cause failures.

Figure 2 presents the definition of an indicator in OSCAD-CIRAS which checks the protection system with respect to the yearly planned audits. In the example it is assumed that minimum 10 audits a year should be performed, and the total number of audits cannot exceed 200 per year. To watch the current number of audits the warning and alarm thresholds are defined. Exceeding the given threshold causes automatic generation of a task for the responsible person, and a warning or an alarm respectively. Apart from indicators which monitor the value in the range, there are indicators which show if the value is above (or below) the assumed threshold.

The third group of indicators is defined to check the cost and benefits parameters dealing with the entire CI protection system, like:

- total cost of the protection system per year,
- total investment cost related to the category of countermeasures per year,
- total operational cost related to the category of countermeasures per year,
- total benefits resulting from risk reduction.

These total indicators are calculated based on the parameters values assigned to the particular countermeasure during the OSCAD-CIRAS risk management process. These parameters, like investment cost, operation cost, future benefits, are provided for the CBA component.

The key issue is to define how often the statistics and indicators should be updated and reviewed. This feature is configurable.

It is possible to observe the QCA indicators, but this issue not discussed here. When a given incident is assessed, the QCA factors should be considered, i.e. whether the incident was caused by trespassing of the given qualitative criterion.

5 Conclusions

The paper presents a new concept and implementation of the effectiveness assessment of the critical infrastructure protection system. CI protection is based on the countermeasures which are selected according to the risk value.

The proposed method tries to assess countermeasures effectiveness in practice, observing the behavior of the protected CI. The effectiveness depends on the number of occurred incident, losses caused by them and the cost of applied countermeasures.

For this reason the OSCAD-CIRAS risk manager used in the CIRAS project is extended by an additional functionality related to:

- incident management—to gather data about incidents and to allow immediate reaction to incidents (real-time risk management aspects);
- incident statistics—to present synthetically information about incidents and damages;
- effectiveness indicators—to present more enhanced information related to incidents, their consequences, functioning of the CI and its protection system, protection cost and limitations (provided by the CBA and QCA components of the CIRAS Tool).

The proposed OSCAD-CIRAS extensions are based on the functionality existing in the software which still requires to be customized and configured. The paper shows how to do it. After that the validation experiment is planned. The validation will concern two collaborating and mutually dependent infrastructures: railway transport and energy production.

The proposed concept supports the CI protection system. The countermeasures are not only properly selected, but also monitored and managed. Synthetic information about behavior of the protected CI allows to provide corrections and improvements within the protection system.

References

1. Eusgeld, I., Nan, C., Dietz, S.: "System-of-systems" approach for interdependent critical infrastructures. Reliab. Eng. Syst. Safety **96**, 679–686 (2011)
2. Ciras project, http://cirasproject.eu/. Accessed January 2016
3. ValueSec project, www.valuesec.eu. Accessed January 2016
4. Giannopoulos, G., Filippini, R.: Risk Assessment and Resilience for Critical Infrastructures. Workshop Proceedings, 25–26 April 2012, Joint Research Centre—Institute for the Protection and Security of the Citizen. Ispra, Italy. https://www.google.pl/search?q=Risk+Assessment+and+Resilience+for+Critical+Infrastructures.+Workshop+Proceedings&ie=utf-8&oe=utf-8&gws_rd=cr&ei=s-h6VvXDMof2aJ-EqsgB. Accessed December 2015
5. Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K.: Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine. December, pp. 11–25 (2001)

6. 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
7. Rausand, M.: Risk Assessment: Theory, Methods, and Applications. Series: Statistics in Practice (Book 86). Wiley (2011)
8. 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, Dissem. level: RE/CO (i.e. available for: beneficiaries, stakeholders, Europ. Commission) (2015)
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. Accessed December 2015
13. NIPP 2013: Partnering for Critical Infrastructure Security and Resilience. The US Department of Homeland Security (2013). http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf. Accessed January 2016
14. Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach. U.S. Department of Homeland Security, DHS Risk Lexicon (2010). http://www.dhs.gov/sites/default/files/publications/NIPP%202013%20Supplement_Executing%20a%20CI%20Risk%20Mgmt%20Approach_508.pdf. Accessed January 2016
15. Stapelberg, R.F.: Infrastructure Systems Interdependencies and Risk Informed Decision Making (RIDM): Impact Scenario Analysis of Infrastructure Risks Induced by Natural, Technological and Intentional Hazards, Systemics, Cybernetics and Informatics, vol. 6, number 5 (2013)
16. ISO 31000:2009, Risk management—Principles and guidelines
17. ISO/IEC 27001:2013 Information technology—Security techniques—Information security management systems—Requirements
18. COBIT: http://www.isaca.org/cobit/pages/default.aspx. Accessed January 2016
19. Deming cycle: https://en.wikipedia.org/wiki/PDCA. Accessed January 2016
20. OSCAD project. http://www.oscad.eu/index.php/en/ . Accessed January 2016
21. 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, pp. 11–24. Springer, Cham, Heidelberg, New York, Dordrecht, London (2015). DOI:10.1007/978-3-319-19216-1_2
22. 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)
23. 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, pp. 93–108. Scientific Publishing University of Dąbrowa Górnicza (2015)
24. ISO 22301:2012 Societal security—Business continuity management systems—Requirements
25. 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, pp. 81–92. Springer Cham, Heidelberg, New York, Dordrecht, London (2014). ISBN 978-3-319-07012-4. DOI:10.1007/978-3-319-07013-1