European Commission

ESReDA

European Safety,Reliability & Data Association

Critical Infrastructures: Enhancing Preparedness & Resilience for the Security of Citizens and Services Supply Continuity

Proceedings of the 52nd ESReDA Seminar Hosted by the Lithuanian Energy Institute & Vytautas Magnus University
May 30-31, 2017, Kaunas, Lithuania

Edited by

Inga Žutautaitė, Mohamed Eid,
Kaisa Simola, Vytis Kopustinskas

EUR 28803 EN

Legal Notice

The scientific output expressed in this document does not imply a policy position of the European Commission. Neither do the contents of the document necessarily reflect the position of ESReDA. They are the sole responsibility of the authors concerned. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication. ESReDA seminar's proceedings are designed for free public distribution. Reproduction is authorized provided the source is acknowledged.

European Safety, Reliability & Data Association (ESReDA)

European Safety, Reliability & Data Association (ESReDA) is a European Association established in 1992 to promote research, application and training in Reliability, Availability, Maintainability and Safety (RAMS). The Association provides a forum for the exchange of information, data and current research in Safety and Reliability.

ESReDA membership is open to organisations, privates or governmental institutes, industry researchers and consultants, who are active in the field of Safety and Reliability. Membership fees are currently 1000 EURO for organisations and 500 EURO for universities and individual members. Special sponsoring or associate membership is also available.

ISBN 978-92-79-73870-8
52nd ESReDA Seminar Proceedings, May 2017

For more information and available ESReDA proceedings please consult:
http://www.esreda.org/

Table of contents

Preface

Critical Infrastructures Preparedness and Resilience is a major societal security issue in modern society. Critical Infrastructures (CIs) provide vital services to modern societies. Some CIs' disruptions may endanger the security of the citizen, the safety of the strategic assets and even the governance continuity.

The importance of CI's has been recognized by the European Commission by issuing directive 2008/114/EC on the identification and designation of European CIs and the assessment of the need to improve their protection. The European Programme for European Critical Infrastructure Protection (EPCIP) has been developed and running since 2006. The programme involves pilot projects analysing EU's gas and electricity systems and other CIs. The European Commission Joint Research Centre actively participates in EPCIP by providing technical support, dissemination and training activities.

The critical role that CIs play in the security of modern societies is a direct effect of the ever-increasing spread out of the information technology (IT) in every smallest task in man's daily-life. The continuous progress in the IT fields pushes modern systems and infrastructures to be increasingly intelligent, distributed and proactive. That increases the productivity, the prosperity and the living standards of the modern societies. But, it increases the complexity of the systems and the infrastructures, as well. The more complex a system is, the more vulnerable it will be and the more numerous the threats that can impact on its operability. The loss of operability of critical infrastructures may result in major crises in modern societies. To counterbalance the increasing vulnerability of the systems, engineers, designers and operators should enhance the system preparedness and resilience facing different threats. Much interest is currently paid to the Modelling, Simulation & Analysis (SM&A) of the CI in order to enhance the CIs' preparedness & resilience.

ESReDA as one of the most active EU networks in the field has initiated a project group (CI-PR/MS&A-Data) on the "Critical Infrastructure/Modelling, Simulation and Analysis – Data". The main focus of the project group is to report on the state of progress in MS&A of the CIs preparedness & resilience with a specific focus on the corresponding data availability and relevance. In order to report on the most recent developments in the field of the CIs preparedness & resilience MS&A and the availability of the relevant data, ESReDA held its 52nd Seminar on the following thematic: "Critical Infrastructures: Enhancing Preparedness & Resilience for the security of citizens and services supply continuity".

The 52nd ESReDA Seminar was a very successful event, which attracted about 50 participants from industry, authorities, operators, research centres, academia and consultancy companies. The seminar programme consisted of 18 technical papers, three plenary speeches and a specific round table on Cyber Security.

The editorial work for this volume was supported by the Joint Research Centre of the European Commission in the frame of JRC support to ESReDA activities. Thank is due to A. Liessens of JRC for the editorial work.

Dr. Inga Žutautaitė
Lithuanian Energy Institute

Dr. Vytis Kopustinskas, Dr. Kaisa Simola
EC Joint Research Centre

Dr. Mohamed Eid
Commissariat for Atomic Energy & Alternative Energies

Safety and Security of Critical Infrastructures with regard to nuclear facilities

Berg Heinz-Peter
Bültenweg 85
38106 Braunschweig, Germany

Abstract

Safety and security should have a high priority for operators of critical infrastructures keeping in mind that safety and security have a common purpose: the protection of people, society and the environment depending of the type of critical infrastructure. Cybersecurity has become an essential element of the overall security framework of all kinds of critical infrastructures. As the threat landscape changes and as new actors – from criminal organizations to nation states – get involved, the threat to critical infrastructures from cyber- attacks is increasingly perceived as a growing, real problem. As examples the current experiences and future activities in case of nuclear facilities in Germany under the IT Act recently set in force are discussed and results of international activities in this area are reported.

Keywords: Safety, (cyber)security, IT security, regulations, international projects.

1. INTRODUCTION

Critical infrastructure plays a key role in the functioning of the state and the lives of its citizens. As a result of events caused by the forces of nature or as a consequence of human activities, critical infrastructure can be destroyed, damaged, and its performance may be disrupted, affecting the economic development of the state. Therefore, the protection of critical infrastructure is one of the priorities of the government. Through the protection of critical infrastructure should be understood as all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to prevent threats, risks or weaknesses and limitations and neutralize their effects, including rapid restoration of infrastructure in the event of failure, (cyber)attacks and other incidents affecting the proper functioning.

As the threats changes and new actors – from criminal organizations to nation states – get involved, the threat to critical infrastructures from cyber- attacks is increasingly perceived as a growing, real problem.

A violation or sabotage to critical infrastructures can be driven by a physical attack (e.g. disconnection of a cable) or by an indirect attack from the cyberspace and in this paper we focus on the latter. According to the terminology in International

Electrotechnical Commission (2015), cybersecurity is defined as “actions required to preclude unauthorized use of, denial of service to, modifications to, disclosure of, loss of revenue from, or destruction of critical systems or informational assets”.

Nuclear power plants benefit from a sophisticated and comprehensive safety regime that has been established over the years. However, the security regime for nuclear power plants is far less developed than the safety regime. In general, nuclear safety and nuclear security have a common purpose: the protection of people, society and the environment from unintended releases of radiation material. Many of the principles to ensure protection are common, although their implementation may differ. For nuclear safety or security reasons protection shall be ensured by good design and appropriate operational practices of the respective facilities including nuclear waste disposal.

Recent complex attacks have been designed to target to instrumentation and control (I&C) systems with all the potential consequences for safety and security such attacks may carry (Institute for Security and Safety 2015). In that context, cybersecurity is understood as all processes and mechanisms by which any digital equipment, information or service is protected from unintended access, change or destruction. Cybersecurity has become an essential element of the overall security framework of nuclear facilities and it is establishing itself as a priority for operators and regulators.

2. GERMAN IT SECURITY ACT

The German IT Security Act (IT-Sicherheitsgesetz) has been in force since July 2015. Regulations which specify the areas of critical infrastructure covered by the act are needed for its implementation. An initial regulation relating to this entered into force in May 2016. It covers the critical infrastructure sectors of energy, information technology and telecommunications, as well as water and food.

The next regulation is expected in spring 2017 and will cover finance, transport and traffic, as well as health sectors. In each case, the sectors affected must full their obligations under the law six months after the regulations have entered into force.

Initial effects are already being seen as a result of the enactment of the IT Security Act. For example, individual companies in the areas covered are already meeting their statutory obligations for reporting IT security incidents and for protecting IT systems in accordance with state-of-the-art technology ahead of the deadline. Sector-specific working groups have been formed under co-operation of critical infrastructures.

The IT Security Act places the highest demands on the operators of critical infrastructures. In addition to the establishment of adequate safety measures corresponding to the state of the art, they must undergo an evaluation of these measures every 4 years. As a national cybersecurity authority, the goal of the Federal

Office for Information Security (BSI) is to promote IT security in Germany. BSI is first and foremost the central IT security service provider for the federal government.

Thus, in addition to the legal requirements for the establishment of appropriate technical and organizational measures for the protection of IT systems, the core element of the IT Security Act is the various reporting requirements on IT security incidents to BSI, which will function as a central reporting and supervisory authority. BSI provides the insights gained from these notifications, but also from various other information, to all operators of critical infrastructures so that they can adequately protect their IT. The obligation to report significant IT security concerns initially affects, as explained above, the energy sector and, thus, also the operators of nuclear power plants.

A first example with respect to critical infrastructures in 2013 which has been reported by BSI (2014) was the malfunction in the energy sector but not in the nuclear area. Anomalies were detected in the data streams in several Austrian control networks for the management of energy grids. These caused malfunctions for grid and power station operators as well as a number of data transmission disruptions. It is suspected that the malfunction was triggered by a command during commissioning a gas grid operator in southern Germany which also extended to the Austrian energy grid. This was then passed on to various different operators. Due to the unspecified processing of this message in individual network components the command was sent as an infinite loop, thereby triggering serious disruption of the grid management control. During the incident the grid’s stability could only be maintained at great expense. During the disruption considerable volumes of data were created, leading to log data overflows. Accordingly it has not yet been possible to finally determine the cause of the incident.

The recent BSI report (2016) provides a reliable and in-depth description of current developments in IT security. It outlines the current exposure in Germany, assesses vulnerabilities in IT systems and illustrates both means and methods of attack and finally provides information about the structures and framework conditions of IT security in Germany. The reporting period was characterised by a continued increase in the professionalisation of attackers and their methods of attack. The number of known malicious program versions increased further in 2016 and, in August 2016, the recorded figure was over 560 million. At the same time, current conventional defence measures are continuing to lose their effectiveness. This affects all users – private, corporate, state and administrative. The threat from ransomware has increased in Germany significantly since the end of 2015. Ransomware is defined as malicious programs which restrict or prevent access to data and systems and only release these resources upon payment of ransom money.

Malicious programs are generally installed with the involvement of the user, meaning that technical protective measures are circumvented and attackers are able to penetrate protected networks. IT security must be considered and implemented as an overarching concept which also comprises user involvement.

3. SAFETY AND SECURITY ASPECTS FOR NUCLEAR FACILITIES

Many elements or actions serve to enhance both safety and security simultaneously. For example, the containment structure at a nuclear power plant serves to prevent a significant release of radioactive material to the environment in the event of an accident, while simultaneously providing a robust structure that protects the reactor from a terrorist assault. However, all these actions are, of course, ineffective in the case of cyber- attacks as described in the event of malicious software later on in this section. Therefore, the Federal Government has issued the Directive for the Protection of IT Systems in Nuclear Installations (BMU 2013).

The following definitions are provided by International Atomic Energy Agency (2009):

- nuclear safety as “the achievement of proper operating conditions, prevention of accidents and mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation hazards”,
- nuclear security, on the other hand, as, “the prevention and detection of and response to theft, sabotage, unauthorized access, illegal transfer, or other malicious acts involving nuclear material, other radioactive substances, or their associated facilities”.

Although safety and security are considered complementary, typical differences exist and are shown in Table 1.

Table 1: Typical differences between safety and security.

SAFETY	SECURITY
The nature of an incident is an inherent risk	The nature of an incident is caused by a human act
Non intentional	Intentional
No human aggressor	Human aggressor
Quantitative probabilities and frequencies of safety-related risks are available	Only qualitative (expert-opinion based) likelihood of security-related risks may be available
Risks are of a rational nature	Threats may be of a symbolic nature
Information is generally open	Information must be kept confidential

There are certainly similarities in the approaches to protection under safety and under security: both rely on in-depth-defences; both place priority on prevention, early detection, and prompt action; and both require extensive emergency planning.

However, the different starting points of safety and security at times have implications for how measures are implemented and who implements them. Moreover, nuclear safety and security management must be considered throughout the lifetime of the facility, which begins with the facility design and continues through commissioning, operation, decommissioning and dismantling. An interaction between safety and security is necessary before making changes to plant configurations, facility conditions or security to ensure that potential adverse effects have been adequately considered and managed (Berg and Seidel, 2014). One possibility of a unified approach is shown in Figure 2.

Observations from the near past show the evidence that cyber threats have been also directed on software-based instrumentation and control (SB I&C) systems of industrial processing plants. For instance, the Stuxnet attack targeted the instrumentation and control of a nuclear facility. As a consequence, there is an urgent need to analyse and protect SB I&C performing functions important to safety according to cybersecurity.

Cybersecurity as a component of nuclear security is the range of measures enacted to prevent, detect, or respond to the theft of nuclear material or the sabotage of a nuclear facility that could result in catastrophic consequences through cyber-attacks.

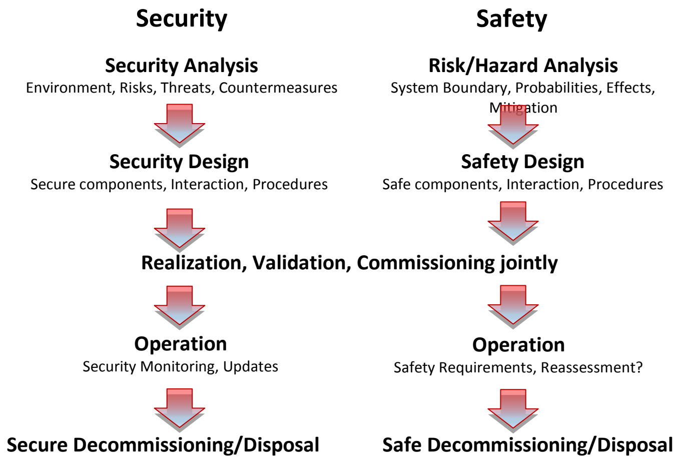

Security
Safety
Security Analysis
Environment, Risks, Threats, Countermeasures
Risk/Hazard Analysis
System Boundary, Probabilities, Effects, Mitigation
Security Design
Secure components, Interaction, Procedures
Safety Design
Safe components, Interaction, Procedures
Realization, Validation, Commissioning jointly
Operation
Security Monitoring, Updates
Operation
Safety Requirements, Reassessment?
Secure Decommissioning/Disposal
Safe Decommissioning/Disposal

Figure 2: One possible unified approach according to Schoitsch and Bleier (2013).

In order to implement and maintain cybersecurity a plant specific cybersecurity plan is to be developed which involves e.g. prescriptions to following aspects:

- The high level documents such as on DBT and the plant security policy the cybersecurity plan is to be embedded,
- Roles and responsibilities for cyber security,
- Reporting and documentation requirements,
- Interfaces of the cybersecurity plan to other documents on plant specification,
- SB I&C asset management,
- Graded approach to SB I&C security and risk assessment,

- Implementation of cybersecurity controls (these are protective measures of technical or administrative nature),
- Lifecycle qualification procedure.

It is obvious that the implementation of a cybersecurity feature (a SB I&C system internal property to support cyber security) or control some of the above mentioned security requirements needs a strategy to meet the above mentioned requirements and recommendations in accordance with the safety objectives. Therefore the mutual impact on safety and security has to be analyse and if necessary resolved. Some examples where a potential conflict has to be resolved are given by the International Electrotechnical Commission (2016):

- The implementation of a cybersecurity feature or control shall not adversely impact the performance, effectiveness, reliability or operation of safety functions supported by SB I&C systems,
- The implementation of a cybersecurity feature directly in a pre-developed SB I&C system should be justified and otherwise avoided because of adding complexity and introducing new potential failure modes,
- Implementation of cybersecurity within or between safety systems shall be justified from both perspectives, the safety and security side,
- If cybersecurity features are implemented in safety system displays and controls, they shall not adversely impact the operator’s ability to maintain the safety of the plant,
- Cybersecurity features and controls included in safety systems should be developed and qualified to the same level of qualification as the systems,
- Cybersecurity features should not significantly increase diagnostic and reparation time of safety functions.

A distinct cybersecurity issue is to develop and maintain a common SB I&C procurement strategy for the system vender and the component suppliers. This strategy should cover software and hardware development taking into account software or logic patterns embedded in pre-developed components such as complex programmed logic devices, field programmed gate arrays, or application specific integrated circuits. Suppliers should meet the same security requirements as the vendor responsible for final product.

On national level, according to the new added § 44b in the Atomic Energy Act (2016) licensees shall report impairments of their information technology systems, components or processes which may lead to or already have led to a threat or disturbance of the nuclear safety of the relevant installation or practice, without delay to BSI.

The report must contain information about the disturbance and about the general technical conditions, especially of the supposed or actual cause, and about the information technology affected. BSI shall transfer these reports to the Federal licensing and supervisory authorities that are responsible for nuclear safety and security without delay which requires the support by the Incident Registration Centre of the Federal Office for the Safety of Nuclear Waste Management.

One event of malicious software occur in a German nuclear power plant (see BSI 2016): over the course of preparations for inspection work, malicious programs were discovered on a computer used for presenting and highlighting operating steps on the fuel rod loading machine (visualisation computer). The malicious programs that were detected are widely distributed and have been easily identified by virus scanners for a long time.

The visualisation computer itself was no longer running with the current version of the operating system and did not have a virus scanner. This is not unusual in the Supervisory Control and Data Acquisition system environment due to the authorisation procedures and compatibility requirements in this area. This combination enabled an attack by the Concker. In addition to this, the malicious program Ramnit was found on the visualisation computer. Besides computer networks, both Concker and Ramnit use USB storage devices in order to infect other systems. The infection could therefore have been originally transferred onto one of these USB storage devices using a PC connected to the Internet which had been infected with the malicious software online. The USB storage device was then used at a later point in time on the visualisation computer and was thus able to infect the unprotected computer even though it was not connected to any network.

No damage occurred to the nuclear power plant itself, the associated infrastructure or the information technology. However, the operator incurred costs in terms of the working time involved in reconstructing the course of events, the ongoing analysis and the subsequent cleaning of the computers and data storage devices affected.

As a conclusion from this event, BSI recommended that both Concker and Ramnit should be regarded as common and now even obsolete malicious programs which by today's standards do not use any special mechanisms. The distribution method via USB data storage is also not unusual.

4. CONCLUDING REMARKS AND OUTLOOK

There has been remarkable consistency in the identification of the key governance improvements that are needed. The regime needs to be more cohesive and its current components universalized and maximally utilized. There needs to be greater cross-border communication of non-sensitive information for the purpose of building international confidence in the system.

The system requires the institution of a peer review process similar to that employed in the nuclear safety regime. Moreover, best practices need to be disseminated, but allowed to be implemented in a flexible and culturally sensitive manner.

Although safety and security programs have different requirements, they overlap in key areas and could support and enhance one another. However, the cybersecurity reaches very high importance as the BSI identified a new quality to the nature of this threat for every type of critical infrastructure.

The main gateways for cyber-attacks are unchanged and remain critical:

- Vulnerabilities exist in software, in some cases also hardware products, which are used most often and which enable attackers to remove information or gain control over systems,
- Attackers have botnets available which have been developed and are executed in an organised manner for distributing malicious software or spam emails on a mass scale. These botnets can also be used successfully for attacks on the availability of services,
- Users also often either fail to apply conventional and straightforward security measures, or do so inadequately,
- Opportunities are arising for cyber criminals in the marketing of attack tools, but also for extortion due to anonymous payment methods such as Bitcoin.

According to GAO (2015) the number of major cyber events continues to increase sharply every year, taking advantage of weaknesses in processes and people as well as technologies. There has been widespread recognition that some of these cybersecurity (cyber) events cannot be stopped and solely focusing on preventing cyber events from occurring is a flawed approach. Organizations should improve their prevention capabilities with modern technology and tools while augmenting their cyber event detection and response capabilities.

Organizations used to focus their information security efforts on cyber event protection, but adversaries have modified their attack techniques to make protection much more difficult, including taking advantage of weaknesses in processes and people as well as technologies. The number of cyber events continues to increase sharply every year leading to a widespread recognition that some cyber events cannot be stopped (GAO 2015). As a result of this risk recognition, organizations have started to improve their prevention capabilities with modern technology and tools while augmenting their cyber event detection and response capabilities.

However, although recovery is an important part of the enterprise risk management process lifecycle (see Figure 2); for example, NIST (2014) defines five functions: identify, protect, detect, respond, and recover. These functions are all critical for a complete defense. The recovery area is described in more detail in Bartock et al (2016).

Cybersecurity has become an essential element of the overall security framework of nuclear facilities and it is establishing itself as a priority for facility operators and national regulators.

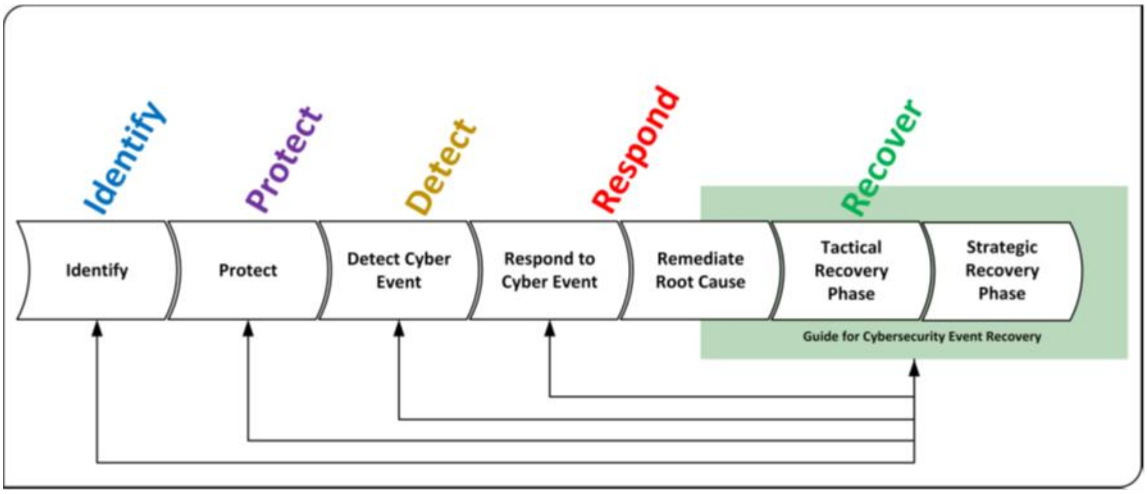


Figure 2: Risk management process lifecycle according to Bartock et al (2016.

In that context, a research project by the Institute for Security and Safety (2015) has been performed on cybersecurity at nuclear facilities. This study focuses on characterizing what several countries are doing at the national level and introduces a potential model for developing a national approach to cybersecurity at nuclear facilities.

Thematically, this study focuses on the underlying frameworks comparing laws, regulations, regulatory frameworks, licensing and other associated regulatory activities and analysing differences and similarities across the countries surveyed. The range of activities considered in the study provides a model of a national legal and regulatory framework necessary to ensure cybersecurity at nuclear facilities.

After several years in which cybersecurity at nuclear facilities has evolved from ad hoc measures and pilot projects to a fairly established and important element of overall nuclear security, it is important and timely to try and capture a comparative snapshot of where its implementation stands in several countries.

The threat from cyber-attacks is increasingly perceived as a problem of national and international security as cyber-attacks grow in number and sophistication and as actors behind them are no longer only private hackers or organized criminals but also nation states. Likewise, attacks once confined to networks and computer systems have now been extended to instrumentation and control systems with all the implications and potential consequences such attacks may carry.

Nuclear facilities – in operation or being built – have progressively become heavily reliant on digital I&C systems or computer based information systems. This is a consequence of the disappearance from the market of analog products as the digitalization of operational functions and working processes increases in quality and efficiency. This development gives rise to new threats confirmed by the publications of security vulnerabilities in the area of process control and automation systems.

Further efforts need also to be made in ensuring that cybersecurity is acknowledged and fully referenced in the other domains protecting the operation of nuclear facilities (safety, physical security, nuclear material accountancy and control). In particular in some fields like instrumentation & control, the interaction between the cyber and physical sides is so strong and inextricable that they are coming into fields of studies and analysis of their own, see Institute for Security and Safety (2015). It is therefore crucial that these interdependences are rapidly recognized and documented at the appropriate level in guidance instruments. Where relevant, most safety and security functions may have to be reassessed with a clear understanding of possible interactions with cyber threats in mind.

The impetus for the focus on cyber security is that it is one of the most significant new key elements that have entered the nuclear security arena in the last decades, quickly gaining prominence and significance due to growing reliance on digital equipment and to game-changing events like the Stuxnet attack. After several years in which cyber security at nuclear facilities has evolved from ad hoc measures and pilot projects to a fairly established and important element of overall nuclear security, it is important and timely to try and capture a comparative snapshot of where its implementation stands in several countries.

In general, cybersecurity concerns should extend to cover the full lifecycle of nuclear facilities and their components. Therefore, cyber security should become a fully incorporated factor in such activities associated with the operation of nuclear facilities like the management of the nuclear supply chain, instrumentation certification procedures, personnel security issues, core training curricula or threat assessment.

An important aspect is to provide an appropriate security testing methodology because an asset is safe and secure if it free from unwanted damage. Traditional software testing doesn’t distinguish. The difference between software safety and software security is the presence of an intelligent adversary bent on breaking the system which makes security testing more difficult.

Therefore, a security methodology is not a simple thing. It is the back-end of a process or solution which defines what or who is tested as well as when and where. It must take a complex process and reduce it into elemental processes and sufficiently explain the components of those processes. Then the methodology must explain the tests for verifying what those elemental processes are doing while they are doing, moving, and changing. Finally, the methodology must contain metrics both to assure the methodology has been carried out correctly and to comprehend or grade the result of applying the methodology. One approach for security testing is described in Institute for Security and Open Methodologies (2010) differentiating six different types of tests:

- Blind: tester knows nothing about assets and defenses; target knows test details,

- Double Blind: tester knows nothing about assets and defenses; target is unaware of test,
- Gray Box: tester has incomplete knowledge of assets and defenses, target knows test details,
- Double Gray Box: tester has incomplete knowledge of assets and defenses; target expects test, but doesn't know details,
- Tandem: both tester and target know details of the assets, defense and test,
- Reversal: tester knows details of assets and defenses, but target is unaware of test.

Crafting a strategy that protects facilities from dynamic, evolving cyber threats requires a fresh, unconstrained examination of the overarching framework that guides cybersecurity. The report of van Dine et al. (2016) identified four overarching priorities, as well as specific actions, that if implemented would dramatically reduce the risk of damaging cyber-attacks on nuclear facilities: institutionalize cybersecurity, mount an active defense, reduce complexity and pursue transformation.

A recent report of the Energy Expert Cyber Security Platform (2017) proposed a strategic framework for the energy sector including nuclear with the target to address the challenges found in the energy sector including nuclear energy.

This strategic framework consists of four strategic priorities which address key areas of threat and risk management: the cyber response in case of a cyber-attack, the continuously improvement of cyber resilience, the build-up of required capacities and competences for the energy sector. In order to meet current and future cyber security needs, the strategic priorities target organisational preparedness and maturity of organisations rather than demanding specific cyber security functionalities. This should help to address the dynamics in the energy sector and to anticipate and adapt to existing and emerging threats by the analysis and implementation of capabilities and appropriate in-time mitigation measures.

Current questions about cybersecurity arising from the increasing use of digital control systems in nuclear power plants are being addressed by the research project SMARTEST where a test method for the detection of weak points of software-based control systems should be developed. The project will be completed in June 2018. Some information on modeling of techniques attacks are shown in Fischer et al. (2016).

References

Act on the Peaceful Utilisation of Atomic Energy and the Protection against its Hazards (Atomic Energy Act) of 23 December 1959, as amended and promulgated on 15 July 1985, last Amendment of 26 July 2016, corrected on 15 December 2016.

Bartock Michael et al. (2016) *Guide for Cybersecurity Event Recovery National Institute of Standards and Technology*. NIST Special Publication 800-184, December 2016.

Berg, H.P. and Seidel, F. (2014) Interface between Nuclear Safety and Security, *Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars*, vol 5, number 1, pp. 9-20.

Energy Expert Cyber Security Platform (2017) *Cyber Security in the Energy Sector, Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector*, EECSP Report, February 2017.

Federal Ministry for the Environment, Nature Conservation and Nuclear Safety - BMU (2013) *Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorien I und II gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie IT)*. Announcement of July 8th, 2013. GMBl. 2013, Nr. 36, p. 711 (without text).

Federal Office for Information Security - BSI (2014) *The State of IT Security in Germany*.

Federal Office for Information Security - BSI (2016) *The State of IT Security in Germany*.

Fischer, R., Clausing, R., Dittmann, J., Kiltz, S. and Ding, Y. (2016) Modeling Attacks on Critical Infrastructure: A first Summary of existing Approaches, *47th Annual Meeting on Nuclear Technology*, Hamburg, Germany

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) (2015). Bundesgesetzblatt Jahrgang 2015 Teil I Nr. 31.

Government Accountability Office – GAO (2015) *Federal Information Security: Agencies Need to Correct Weaknesses and Fully Implement Security Programs*, GAO 15-714, September 2015.

Institute for Security and Open Methodologies (2010) *Open Source Security Testing Methodology Manual*, www.isecom.org/mirror/OSSTMM.3.pdf.

Institute for Security and Safety (2015) *Cyber Security at Nuclear Facilities: National Approaches*, an Institute for Security and Safety (ISS) research project in cooperation with the Nuclear Threat Initiative, June 2015.

International Atomic Energy Agency - IAEA (2009) *IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection.* Vienna, Austria.

International Atomic Energy Agency - IAEA (2016) *Conducting Computer Security Assessments at Nuclear Facilities*, IAEA-TDL-006, IAEA, June 2016.

International Electrotechnical Commission - IEC (2015) *Nuclear power plants – Instrumentation and control systems important to safety – Classification of instrumentation and control functions*. IEC 61226:2015-08, draft.

International Electrotechnical Commission - IEC (2016) *Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coordinating safety and cybersecurity*, IEC 62859, Ed.1.0, October 2016.

National Institute of Standards and Technology - NIST (2014) *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February 2014.

Schoitsch, E. & Bleier, T. (2013). *Safety vs. Security*, available under:www.fh-campuswien.ac.at/index.php?download.

Van Dine, A., Assante, M. and Stoutland, P. (2016) *Outpacing Cyber Threats. Priorities for Cybersecurity at Nuclear Facilities*, Nuclear Threat Initiative, February 2016

Risk assessment for interconnected Critical Infrastructures: The case of ship- port interface

George Leventakis, Nikitas Nikitakos
Department of Shipping Trade and Transport, University of Aegean, Greece

Athanasios Sfetsos
Environmental Research Laboratory, Institute for Nuclear and Radiological Sciences, Energy, Technology and Safety, NCSR "Demokritos", Greece

George Leventakis
Center for Security Studies, P. Kanellopoulou 4, 101 77, Athens, Greece

Abstract

This paper introduces a holistic concept for the protection of heterogeneous critical infrastructure networks that is applicable on a strategic level. The basis of the proposed model is the concept that security incidents may be propagated between assets of interconnected networks. The proposed methodology emphasizes the strategic level protection both from the perspective of the network operator and the emergency responder, linking all phases of the disaster cycle into a unique concept of operations. As a case study for ship to port interface a LNG terminal is presented.

Keywords. Risk assessment, Interconnection analysis, Holistic impact analysis, European critical infrastructures, Climate Change.

1. Introduction

Critical infrastructures (CI) provide the essential services that underpin society and serve as the backbone of every nation's economy, security, and health. Historically, the design and operation of CI accounts for natural and accidental failures, but place little or no emphasis on protection against security incidents. Networks of assets are increasingly physically integrated with each other, with other installations, and with other economic activities and support the uninterrupted progress of mass events, forming synergistic "network of networks". An attack on a specific asset is likely to impact the entire "network of networks" within which it resides, since it can have swelling-effects and cascading failures.

Despite the fact that security issues are very similar across all counties, there is a remarkable gap in the derivation of a commonly agreed protection framework and a common concept of operations. Following the EC Critical Infrastructure Protection Program (Directive 114/2008/EC), a proposed strategic protection framework mainly could be considered a small yet decisive step towards the development of a common and harmonized security risk assessment process for critical infrastructures.

The unification of the crisis phases, Figure 1, will ensure effective and faster response: Early awareness from multiple fused data sources, increased readiness, education and training, reduced risk to emergency responders by providing accurate and timely coherent information relating to hazards and risks. The proposed work however is focused on the development of a consolidated risk assessment and risk management plan for interconnected CI systems linked to coherent contingency planning.

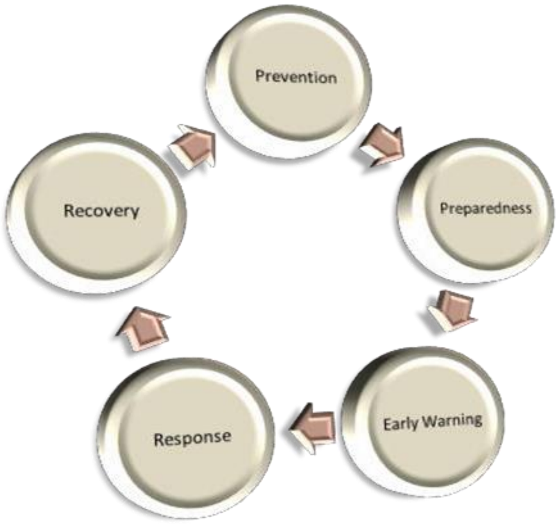


Figure 1. Phases of the Crisis Cycle (Leventakis et. all, 2014)

Risk Analysis is a continuously adaptive process where threats are evolving and more sophisticated technological solutions are used to exploit system vulnerabilities. In recent years, many researchers have tried to accommodate the complex interconnections of modern critical infrastructures and cascading events into a holistic risk analysis process.

(Earl *et al.*, 2007) and (Rosato *et al.*, 2008) applied complex network theories, whereas the introduction of not only abstract interdependencies but also selected properties of infrastructure types such as buffering of resources were proposed. (Sandmann, 2009) proposed stochastic models of networks covering a broad field of models and tools that might be applicable to (inter-) dependency modelling. (Eusgeld *et al.*, 2009) emphasized the importance of potential failure propagation among infrastructures leading to cascades affecting all supply networks, presenting a systems-of-systems (SoS) approach. A Complex Network theory based topology-driven method was presented to comprehensively analyze the vulnerability between interdependent infrastructures.

(Haimes *et al.*, 2007) proposed the inoperability input-output model for the analysis of the manner in which perturbations (*e.g.*, intentional attacks, accidental events, or natural disasters) to a set of initially affected sectors impose adverse impacts on other sectors, due to their inherent interdependencies.

The Hierarchical Coordinated Bayesian Model (Z. Yan et al, 2006) was developed as an analysis tool of sparse data which can be used to infer extreme event likelihoods and consequences using hierarchical coordination. (Pant and al, 2011) described the interdependent adverse effects of disruptive events on inter-regional commodity flows resulting from disruptions at an inland port terminal, using a risk-based Multi-Regional Inoperability Input-Output Model. (Zhang and Peeta, 2011) proposed a generalized modeling framework that combines a multilayer network concept with a market-based economic approach to capture the interdependencies among various infrastructure systems with disparate physical and operational characteristics. (Casalicchio *et al.*, 2010) proposed an agent-based modelling and simulation solution for critical interdependence modelling. The approach, named Federated-ABMS, relies on discrete agent-based modelling and simulation and federated simulation. It provides a formalism to model compound complex systems, composed of interacting systems, as federation of interacting agents and sector specific simulation models. (Balducelli, 2005) developed interacting agents for modelling the discrete event simulation as a tool to approach interdependencies analysis and evaluation for critical infrastructures.

The DECRIS model drew upon the experience obtained from the application of risk analyses within different critical infrastructures, to develop an all-hazard generic methodology suitable for cross-sector infrastructure analysis. A similar approach was derived in the COUNTERACT EU funded project. A generic security guide was developed which was focused exclusively on terrorist threats, using a human intent specific method to assess risks, based on harm (effect) and availability (vulnerability/threat). The approach lacked a mechanism to transfer the results of multiple risk assessments into a higher (hierarchical) level, in addition to the interconnected aspect of different infrastructures. Additionally, EURAM built a basic common methodology for the analysis of interdependencies between Critical Infrastructures (CI) of the same sectors and between CI of different sectors and different countries. The above approaches are very useful within their particular scope and frame of application. However, a gap that becomes visible is the lack of a generic and widely applicable risk assessment framework that can incorporate the concept of asset interconnection (and consequently the concept of network interoperability) into a holistic and integrated semi-empirical approach capable of being bringing together a broad range of networks (transport, energy, cyber, etc.), infrastructures (including critical ones) and response policies.

The specific objective of the present work is to develop a comprehensive Strategic Risk Assessment Framework for interconnected systems taking into consideration that (a) interdependent and heterogeneous networks are interconnected and (b) that risk is propagated between them. It is designed to estimate risk mainly in interconnected networks and finally the estimation of a holistic risk in the network of networks

2. **Strategic Risk Analysis Framework**

The process to derive the strategic risk analysis framework (RAF) is presented schematically in Figure 2. Its general principles follow a well-established path that has been followed in related literature, *e.g.*, [12, 17, 18, 19], and in related funded studies (*e.g.*, COUNTERACT , EURAM).

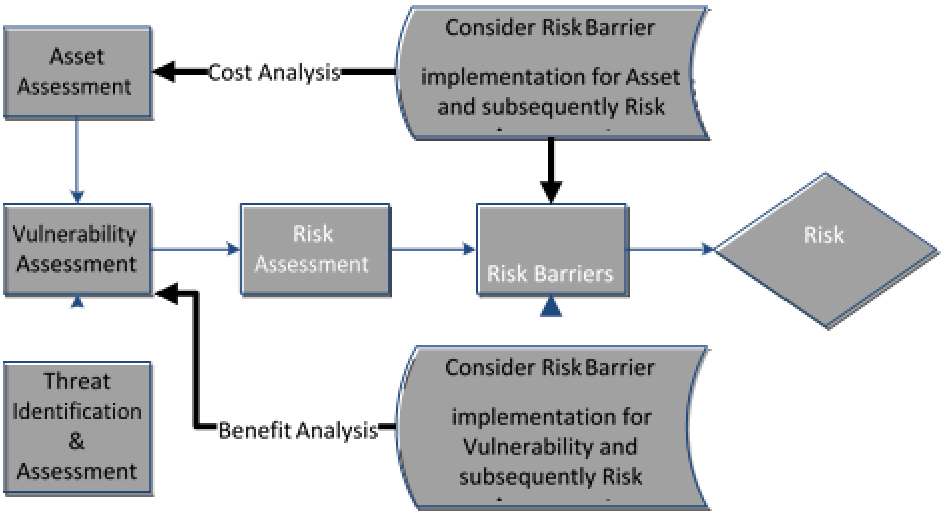

Asset Assessment
Cost Analysis
Consider Risk Barrier implementation for Asset and subsequently Risk
Vulnerability Assessment
Risk Assessment
Risk Barriers
Risk
Threat Identification & Assessment
Benefit Analysis
Consider Risk Barrier implementation for Vulnerability and subsequently Risk

Figure 2. Generic Strategic Risk Assessment Framework (Leventakis et. all, 2014)

The proposed framework is comprised of four main phases:

Phase 1: Assessment of present situation, which includes the detailed specification and description of the interconnected network (or network of networks) that is at risk.

Phase 2: Risk Assessment, which will be determined by an estimation of the likelihood and consequences of an event.

Phase 3: Response procedures, which includes specifying emergency response and business continuity operations.
Phase 4: Risk mitigation, which includes a determination is to identify countermeasure / security upgrades that will lower the various levels of risk.

The main benefit of the proposed framework in comparison to existing approaches is the combination of the below elements:

- A risk analysis and assessment methodology for CI at a strategic level.
- Response measures and procedures integration.
- Transition from a single infrastructure modelling to a holistic "network-of-networks" model.
- Compatibility with the EU Directive 114/2008 regarding the European Critical Infrastructure Protection Programme.
- Extendibility to various types of critical infrastructures.
- Ability to incorporate framework to a risk assessment IT tool.

3. Network Assets

The identification of the network assets is the first introductory step as it builds the foundations upon which relevant methodologies will be applied. Under the scope of the proposed RAF, an asset is considered as the basic unit of any critical infrastructure network, and in general the following basic principle is assumed: Each network will be decomposed into assets, *i.e.*, objects with specific and easily recognized roles.

In response to this approach, a conceptual framework for categorizing assets within any CI network is proposed comprising of:

- Direct assets
  - Humans, goods, services related with CI operation
  - Movable assets
  - Infrastructure
- Indirect assets
  - Utilities, *e.g.*, electricity, water
  - Information, *e.g.*, signals
- Auxiliary assets

The major source of complexity in heterogeneous systems is defined by the way each asset affects the others as well as the intensity of that effect. An important step in understanding and consequently modelling that relationship is to first identify all possible expressions and variations of the so-called "interdependencies" which link together assets. All interdependencies can be categorized in he proposed RAF, based on the medium which each connection utilizes in order to manifest itself. These categories according to are:

- ✓ **Physical Interdependency**: Two networks / assets are physically interdependent if the state of one is dependent on the material output(s) of the other. This sort of interdependency is realized when a physical linkage between the assets exists.
- ✓ **Systems Interdependency**: Two networks / assets have a systems interdependency, if its state depends on the properties of a system transmitted through another asset.
- ✓ **Geographic Interdependency**: Networks / assets are geographically interdependent if an incident in an asset may impact the state of assets in a defined spatial proximity.
- ✓ **Logical Interdependency**: Two networks / assets are logically interdependent if the state of each depends on the state of the other via a mechanism that does not fall into any of the above.

4. **Risk Assessment Framework Methodology**

A threat is any factual or probable condition (incident, fact or occurrence) that can inflict harm or death to passengers, personnel, damage or loss of equipment, property or/and facility as well as undermining the positive image or prestige of the operator.

In order for the attack or incident to inflict a measured impact on CI, certain vulnerabilities of the assets (*e.g.*, security flaws, operational, functional, by design) must be exploited.

These, on a second stage, should be exhaustively analysed by the security officers and risk managers of the CI network, and be used to define appropriate countermeasures and security policies that would considerably reduce the risk impacts.

Within the proposed RAF, a threat-risk matrix composed of the vast majority possible risks for a certain type of threat that could adversely affect the network operation, has been identified. For each identified risk a series of security incidents may be derived that would be the initiating mechanism of the proposed RAF, but are not introduced here due to space limitations.

Risk is evaluated from an iterative process assessing the probability of occurrence of the threat (Likelihood) and the Consequences in the event of a realization occurs. Figure 3 presents an analytical description of the proposed RAF, taking into consideration the main categories of Likelihood and Consequences The RAF has been designed to process diverse sources of information on an ordinal scale of 5 categories or/and numerical scale.

The advantage of the proposed approach is that for the estimation of risk, any type of information may be employed combining related scales in order to accurately estimate risk.

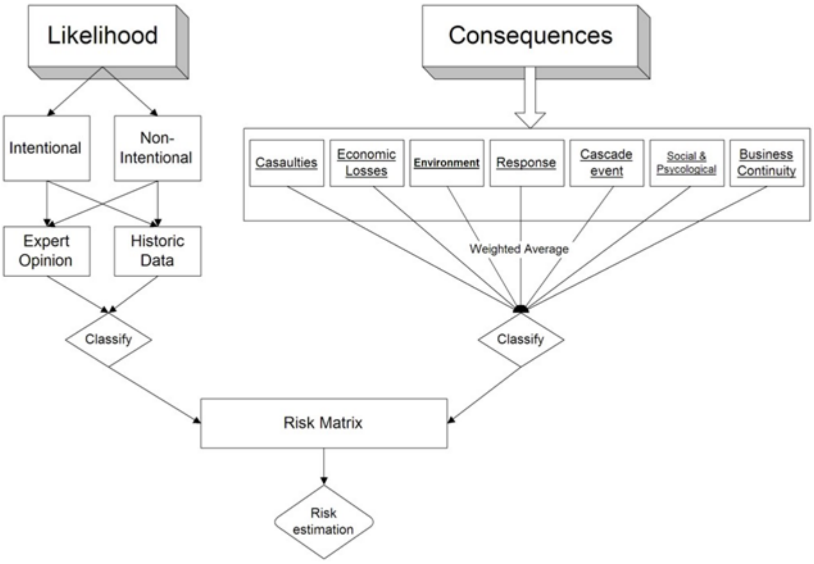


Figure 3. General Risk (Single Asset) Assessment Framework Methodology

Likelihood is the frequency of occurrence of a particular threat. In a more generic approach it is expressed by the generic formula: Likelihood = Intention to harm X Capability, which is directly related to the carrier of the threat as well as the vulnerability of the target.

Consequences are the result of the realization of a threat and defined as the harmful or damaging effects and can comprise physical harm, injury, death, loss, damage to property or revenue as well as loss in reputation and credibility of the company and of the critical infrastructure in general. The proposed approach estimates the consequences building upon a two level hierarchy. Level 1 is a generic category of consequences, quantified in a 5 class system (Negligible, Small, Medium, High, Severe), whereas Level 2 may have numerical / logic / categorical / binary / etc. values. A detailed analysis of the consequences is presented in the work of (Leventakis *et al.*,.2014)

Business continuity planning is the process of identifying critical systems, identifying reasonable threats, and creating a long-term strategy for reducing the impact of interruptions to the business and stabilizing critical business functions. It consists of several tasks that together constitute a set of integrated procedures to minimize the impacts of a security incident, ensuring operations remain viable. For the business continuity approach is multi-dimensional meaning that consequences have been accounted for damage to the asset, loss of service, impact on personnel, capability to use asset at risk and impact on the network flow.

The proposed risk analysis framework has the inherent ability to propagate risk in interconnected assets, employing the proposed Impact Propagation Matrix (IPM) which will be extensively analysed in the following section. However, there is the additional capability to account for the impact (i) in the network operation containing the asset at risk and (ii) in the entire “network of networks” of a region.

The Risk Assessment Matrix is a classic tool to conduct semi-quantitative risk assessment, widely applied in many different frameworks. Some basic principles that were adopted within the present RAF that the output risk index is determined only by the mapping of the consequences and the likelihood to a single risk level, all of which can be divided into different levels, respectively, with qualitative descriptions and scales

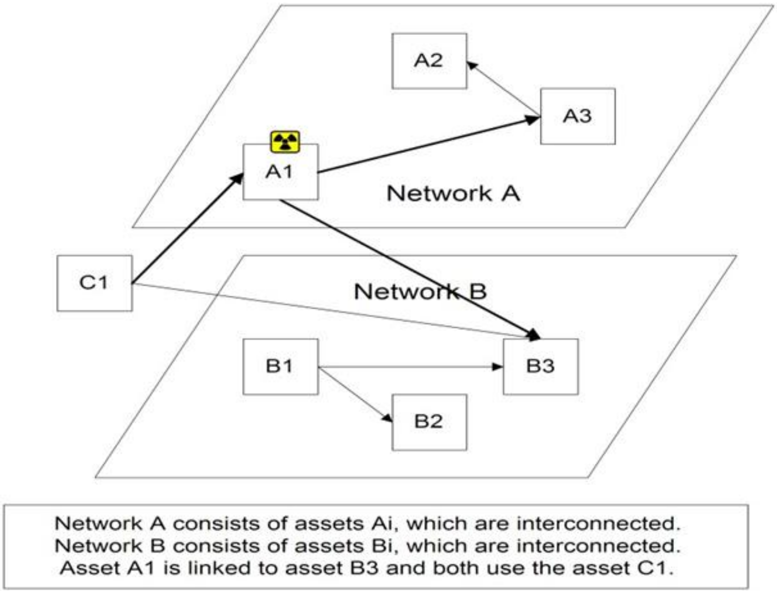
Aggregating the risk between different levels is a crucial task that significantly tests the validity of the proposed approach. Although a variety of different options can be applied, the one selected here as returning the most reliable estimates is the Weighted Mean. A subjective assignment of weights (wi, summing to 100%) can be assigned to the different classes based on their presumed significance, whilst some maybe be ignored. By assigning individual impact rating to ordered numbers (xi) the final value may be estimated as:

$$R_i = \frac{\sum_i w_i x_i}{\sum_i w_i}$$

5. **Risk Propagation**

The core idea of the approach developed for modeling risk propagation in the framework is that a user defined security scenario which originates in an asset of any network can cause diverse impacts and affect other interconnected assets or networks. It builds upon the fundamentals of Markovian chain process, so that the state of an asset will be dependent upon its previous state and/or the states of its interconnected assets. The state of an interconnected asset (Xn) is thus a result of the nature of the incident affecting the originating asset, the characteristics of the asset under consideration (risk countermeasures, means of immediate response, *etc.*,) and the type of interconnection between the assets.

Figure 4, presents an example of the interconnected network assets (which in generalization A and B may be heterogeneous networks), to aid in understanding of the defined process.



Network A consists of assets Ai, which are interconnected.
Network B consists of assets Bi, which are interconnected.
Asset A1 is linked to asset B3 and both use the asset C1.

Figure 4. Example of Assets within Interconnected Networks

Step 1: <u>Scenario outline definition and description of the initial incident(s) that occur(s).</u>

Step 2: Estimate Risk of incident in the Asset A1.

Step 3: Apply the response procedures to the asset at risk.
These will be enforced in order to account for the optimal response to the asset-at-risk, ensuring that disruptions to the network services are minimized. They can be classified into **Emergency response and Business Continuity**. Both procedures described will result in several assets of the network being considered as non-operational and a geographical interconnection established to the asset at risk.

Step 4: Determine the Assets that are interconnected to A1.
The next step involves the process of identifying those Assets that will be affected by the impacts of the incident in asset A1. The new set of assets-at-risk, i.e. those linked to A1 by any type of linkage, will be determined by (i) the type and nature of the initial incident, (ii) the type and characteristics of the interconnection between the assets. To that end a separate Incident Propagation Matrix will be designed for each type of interconnection (Physical/System/Geographical/Logical). Additionally, due to the highly interconnected properties and functionality of the operation of the network asset, it is anticipated that the security incident in any asset, may trigger a different security incident in the same asset, thus establishing a self-interconnection.

Step 5: Estimate the probability of incident initiation at interconnected assets
This will be modeled through the definition of an Incident Propagation Matrix (IPM) which will evolve through a Markov chain process into the risk assessment procedure.

Conceptually, the Incident Propagation Matrix (IPM) is a probabilistic input / output matrix where inputs are the security incidents and output(s) are also security incidents, on the immediately interconnected asset, with the exception of geographically linked assets. It shows in a consolidated form the probability of incidents triggering in linked assets resulting from the initial security incidents.

As triggered incidents are occurring at interconnected assets the likelihood of subsequent incidents is calculated based on the probability of the previous incident multiplied by the probability of the current incident occurring, given that the previous incident has already occurred. This is based on the definition of the conditional probability formalized as such: $p(B \cap A) = p(B/A)p(A)$.

Where A is the generating incident and B is the current incident considered to happen, P(B∩A) is the probability of both A and B occurring and P(B|A) is the conditional probability of B occurring after A. In order for this principle to be applicable in cases where 5-level scale likelihoods are used we introduce the “Likelihood Matrix” which is the tool used to map the probabilities of the initial incident and the conditional probability found in the IPM to the probability of both incidents occurring.

Step 6: Estimate Risk in interconnected asset
The Risk in the interconnected / linked asset(s) is estimated using the main approach (Steps 1 and 2). However, it has to be noted that: The likelihood of the cascading incident equals to the defined probability value of the Markovian process estimated in step 4.

Step 7: Incident termination
Subsequent incidents related to non-zero probabilities can never be brought down to zero since they are multiplied by also non-zero probabilities. This can cause an endless loop which practically serves no purpose other than overloading the system with insignificant incident occurrences. In order to alleviate this we set a probability threshold under which the calculated probabilities are considered to be practically zero and thus the incident propagation from that incident is effectively terminated.

6. **Risk Barriers**

The effective risk assessment should consider a range of control measures (mitigation strategies) and additionally provide a basis for the selection of control measures. Risk control measures are relevant in all security phases, before, during and after a potential threat may be executed, *i.e.*,

a. **Preparedness** before a potential threat may be executed including preventive/detection measures;
b. Capacity for **response**, relief and mitigation, during an incident;
c. Capacity for **recovery** after an incident has occurred.

The introduction of a suitable methodology may lead to a combined approach for (i) optimise the use of resources, (ii) determining the effectiveness and costs of different control options, (iii) improving the overall decision-making process and (iv) providing a basis for allocating resources in the most effective manner. The risk assessment process should provide the following in relation to control measures:

a) identification or clarification of existing and potential control measure options;
b) evaluation of effects of control measures on risk levels (likelihood / impact / interconnection);
c) basis for selection or rejection of control measures and the associated justification of adequacy; and
d) basis for defining performance indicators for selected control measures.

The most common control measures that should be evaluated in terms of:

a) **Viability** that relates to the practicability of implementing the control measure within the facility; and
b) **Effectiveness** which is related to the effect of the control measure on the level of risk. For example, the reliability and availability of control measures influence the likelihood of an incident occurring, while the functionality and survivability of the control measures during the incident influence the consequences.

The evaluation of options for control measures within the proposed risk assessment framework should allow the determination of additional benefit gained from introducing additional or alternative control measures. The proposed approach is build on the capability to search for gaps in the existing control regime, where the introduction of further control measures may seems appropriate.

In order to incorporate the notion of Risk Control Measures (RCM) in the overall risk assessment process a Risk Mitigation Matrix (RMM) was introduced into the framework. This is a two-way matrix used to adjust the initial likelihood and/or consequence estimation of a threat on an asset based on the available pro-active measures in place that can lower the likelihood of a threat, its consequences or both. The columns of the matrix represent the different levels of effectiveness of the overall risk control measures and range from “Ineffective” to “Very Effective”. The initial level estimated for the likelihood or consequence (rows) may be decreased by a varying number of levels based on the effectiveness of the risk control measures. The output of the matrix (cells) represents the revised likelihood or consequence level estimation for the specific threat on the asset in question taking into account all relevant risk control measures.

First and foremost, it is important to define the risk mitigation in terms of its properties, (effectiveness, costs) as proposed in the risk analysis framework. Once these are defined then the likelihood mitigation matrix will be estimated.

7. Case Study

The following section introduces the application of the developed framework on a case study concerning an onshore liquefied natural gas (LNG) terminal. It is assumed that risk analysis, includes receiving terminals and land transport of LNG. as in Figure of a planned import terminal with three storage tanks and with the capability of docking two LNG carriers at once.

Figure5. Receiving terminal artist’s rendering of docks, transfer lines, and storage tanks (www.cheniere.com)

The safety systems aboard an LNG carrier are required by the following:• International Convention for the Safety of Life at Sea (SOLAS) 1974; IMO International Gas Codes (IGC); Flag State Regulations; Classification Society Rules.

In addition to the required safety systems on board LNG carriers, additional safety systems have been installed as a result of recommendations from the Oil Companies International Marine Forum (OCIMF) and the Society of International Gas Carriers and Terminal Operators (SIGGTO). Typical operating conditions for an LNG receiving terminal it could be found in ref (J. L. Woodward,2010)

An LNG receiving terminal consists of four areas:

1. the dock and storage tank area, connected by the LNG transfer line loop;
2. the LNG process area for regasification;
3. the utilities area; and
4. the supporting area.

A transfer line loop delivers liquid from the docked LNG carrier to the storage tank and returns displaced vapor to the carrier tanks to avoid drawing a vacuum in the carrier or building pressure in the terminal tank. The transfer line loop recirculates at other times. A boil-off compressor recovers vapors

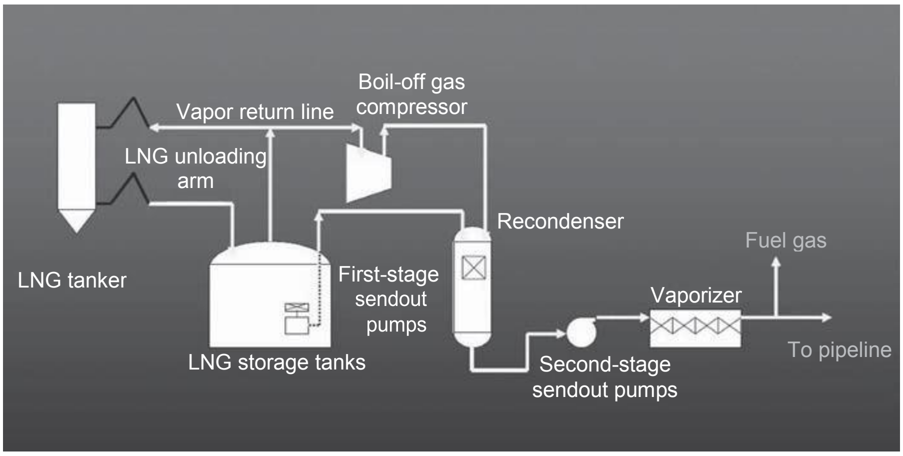


Figure6. Flow diagram of an LNG regasification terminal (www.final-yearproject.com)
evaporated during the transfer. Liquid is pumped to the pipeline pressure and is then vaporized.

The LNG process area primarily vaporizes LNG to natural gas with a heat source. The LNG process area may have a distillation column to separate and recover heavier components called natural gas liquids (NGLs). NGL includes propane and butane and may have a higher price than the LNG and can be sold separately. It may also be necessary to adjust the heat of combustion of LNG to deliver a consistent product to pipeline customers. If the heat of combustion or more specifically the "Wobbe Index" is too high, this requires either diluting the natural gas with nitrogen or air or extracting ethane and heavier components (C2+ extraction), so end users do not have to adjust their equipment.

The utilities area provides services required by the plant including instru- ment air, nitrogen, fuel gas, power generation, emergency power, flare and blowdown system, drain systems, waste water and effluent treatment, demin- eralized water, fire water, and backup diesel-driven fire water pumps.

The supporting area includes maintenance shops, parts storage, offices, and the like.
In order to apply our proposed methodology the following procedure is recommended:

1. Describe the initiating event. (i.e. terrorist attack)
2. Identify interdependencies. Perform qualitative analysis.
3. Perform a semi-quantitative assessment of the risk of the scenario.
4. Perform a detailed quantitative analysis of interdependencies
5. Evaluate risk and measures to reduce interdependencies. Define risk barriers
6. Cost/benefit analysis.

Conclusions

The paper introduced a strategic risk analysis methodological approach that is applicable on Critical infrastructures. The innovation aspect of the introduced approach in comparison to standard risk assessment methodologies lies with its inherent ability to estimate risk in interconnected and heterogeneous networks based on a repetitive process of risk evaluation and assessment of severity, taking into account the Likelihood of occurrence and the Consequences on each interconnected asset. These additions complement traditional risk assessment techniques and improve modelling capacity by incorporating various realistic concepts (risk barriers, risk propagation, asset interconnections, etc.,) that add up to a multi-faceted and holistic framework. In order to verify the applicability of the approach proposed an initial conceptual application to an LNG terminal is presented

References

George Leventakis, Athanasios Sfetsos, Nikolaos Moustakidis, Nikitas Nikitakos 'Strategic Concept for the Protection of Regionally Interconnected Surface Transportation Networks' International Journal of Transportation Vol.2, No.3 (2014), pp.95-116

E. L. Earl II, J. E. Mitchell and W. A. Wallace, "Restoration of services in interdependent infrastructure systems: a network flows approach", IEEE Tr. on Systems, Man, and Cybernetics—Part C: Application and Reviews, vol. 37, (2007), pp. 1303-1317**.**

V. Rosato, L. Issacharoff, F. Tiriticco and S. Meloni, “Modelling interdependent infrastructures using interacting dynamical models”, Int. J. of Critical Infrastructure, vol. 4, (2008), pp. 63–79**.**

W. Sandmann, “Rare Event Simulation Methodologies and Applications”, Simulation, vol. 83, (2007), pp. 809-810.

I. Eusgeld and C. Nan, “Creating a simulation environment for critical infrastructure interdependencies study”, IEEE Int. Conf. on Industrial Engineering and Engineering Management, (2009), pp. 2104-2108.

M. Ouyang, L. Hong, Z. J. Mao, M. H. Yu and F. Qi, “A methodological approach to analyze vulnerability of interdependent infrastructures”, Simulation Modelling Practice and Theory, vol. 17, (2009), pp. 817–828.

Y. Y. Haimes, J. Santos, K. Crowther, M. Henry, C. Lian and Z. Yan, “Risk analysis in interdependent infrastructures”, E. Goetz and S. Shenoi (eds) Critical Infrastructure Protection. Springer, Boston, (2007), pp. 297-310.

Z. Yan, Y. Y. Haimes and M. Waller, “Hierarchical coordinated Bayesian model for risk analysis with sparse data”, Society of Risk Analysis, Annual Meeting, (2006).

P. Zhang and S. Peeta, “A generalized modeling framework to analyze interdependencies among infrastructure systems”, Transportation Research Part B: Methodological, vol. 45, (2011), pp. 553-579.

E. Casalicchio, E. Galli and S. Tucci, “Agent-based modelling of interdependent critical infrastructures”, International Journal of System of Systems Engineering, vol. 2, (2010), pp. 60-75.

C. Balducelli, S. Bologna, A. Di Pietro and G. Vicoli, “Analysing interdependencies of critical infrastructures using agent discrete event simulation”, International Journal of Emergency Management, vol. 2, (2005), pp. 306-318.

I. B. Utne J. Vatn and P. Hokstad, “A structured approach to modeling interdependencies in risk analysis of critical infrastructures”, Reliability, Risk, and Safety Theory and Applications, eds (C. Guedes Soares , Radim Briš , and Sebastián Martorell), CRC Press, (2010).

I. B. Utne, P. Hokstad and J. Vatn, “A method for risk modeling of interdependencies in critical infrastructures”, Reliability Engineering and System Safety, vol. 96, (2011), pp. 671-678.

Couneract, Cluster Of User Networks in Transport and Energy Relating to Anti-terrorist ACTivities, EC Contract Number SSP4/2005/TREN/05/FP6/S07.48891.

EURAM, Generating a European risk assessment methodology for critical infrastructures, Funding through EC Directorate General for Justice, Freedom and Security, (2006).

S. M. Rinaldi, J. P. Peerenboom and T. K. Kelly, “Identifying, understanding and analyzing Critical Infrastructure Interdependencies”, IEEE Control Systems Mag., vol. 21, (2001), pp. 11-25.

IFC Environmental, Health, and Safety Guidelines LNG LIQUEFIED NATURAL GAS FACILITIES, April 2007

J. L. Woodward & R. M. Pitblado ‘LNG Risk Based Safety: Modelling and Consequence Analysis, 2010.

SIGTTO web site http://www.SIGTTO.org/

Cheniere web site (2008). www.cheniere.com

Some Specifics on Using Probabilistic versus Deterministic Approaches in Emergency Zoning Evaluations

Dan Serbanescu
Division of Logic and Models – CRIFST Romanian Academy
Dr Taberei 35A bl803 ap 33
061358, Bucharest, Romania

Abstract

The paper provides an overview of some specific aspects related to the use of probabilistic Safety Assessments (PSA) in tasks related to Emergency Zoning (EZ). The PSA specifics in performing EZ tasks are presented considering also in general the options to solve the EZ tasks by using deterministic approaches for the same tasks

Keywords: Deterministic, probabilistic, analyses, emergency zoning.

1. Background

1.1 Status of the issue

The paper provides an overview of some specific aspects related to the use of probabilistic Safety Assessments (PSA) in tasks related to Emergency Zoning (EZ). The PSA specifics in performing EZ tasks are presented considering also in general the options to solve the EZ tasks by using deterministic approaches for the same tasks. A more detailed evaluation of the issues related to EZ and the specifics of the use of PSA was performed in [1].

The evaluation was also in line with some new trends in using PSA applications for EZ tasks, as part of the Risk Informed Decision Making (RIDM) process, as well as of the harmonization process for EZ requirements. In the process of the evaluation of the issues, that have to be solved in using PSA for the EZ tasks the following aspects were considered:

- EZ is an area of interest for the harmonization process within EU. In this context, the Emergency Zoning Planning (EPZ) is a very important part and it needs definition of the applicable tools. The EPZ are usually defined as in Figure 1.
  Where the notations are:
  - **On-Site**: Internal zone, under control of NPP operator
  - **PAZ**: Precautionary Action Zone
  - **UPZ**: Urgent Protective action planning Zone
  - **LPZ**: Long-term Protective Zone (Food Restriction Planning Zone-
  - **FRPZ**)

- The use of PSA could prove of significant use in EZ tasks because it is the best-suited tool to be used in order to comply with targets as applying RIDM in EZ tasks.
- The complementary use of probabilistic and deterministic tools for EZ tasks is mostly desired and details on PSA tasks for EZ are needed in this case.

The paper [1] presents the status of some important aspects on the Emergency Planning Zones and Radius Sizes.

There are some suggested EZ and Radius sizes for Nuclear Power Plants (NPP) considered in this moment in EPZ. For instance for the threat category I, i. e. for NPPs, IAEA document [2] in its Appendix 5 provides suggestions for the approximate radius of the EP zones and food restriction planning radius as given in the following Table 1.

The radii selected are based on calculations performed using deterministic tools [3]. However, the process of defining the radius involves also expert judgment and subjective opinions.

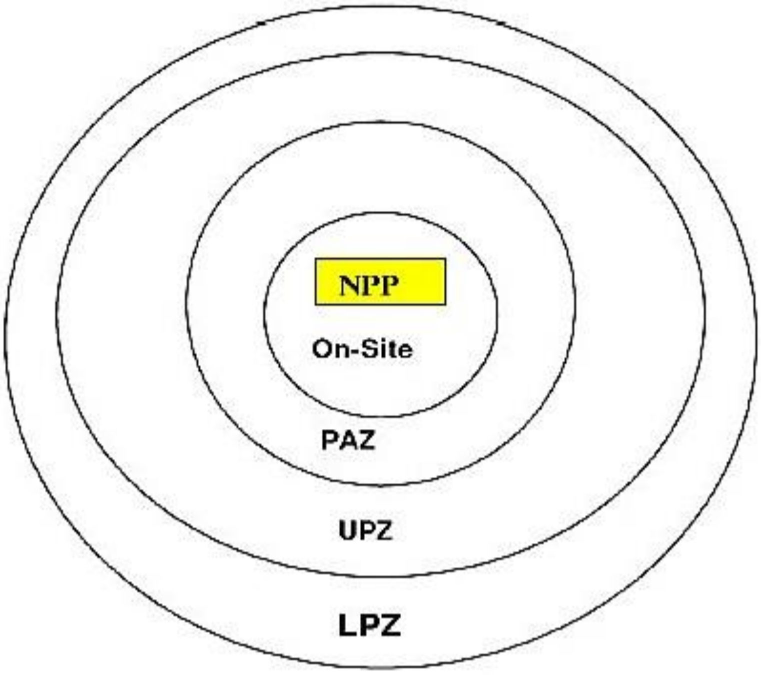


Figure 1. Radii defined for EZ [1]

Table 1. Sample case radii [1].

Combination cases (where D and F are weather categories)	50 mSv D75% 1Day	50 mSv F100% 1Day	50 mSv D75% 7Day	50 mSv F100% 7Day	500 mSv D75% 1Day	500 mSv F100% 1Day	500 mSv D75% 7Day	500 mSv F100% 7Day
Abbreviations (see Figure 6)	UPZL _ D0D1	UPZU _50F1	UPZBE _50D7	UPZEX U_50F7	PAZEXL_500D1	PAZBE _500F1	PAZL _500D7	PAZU _500F7

The current approach to EP is, in general, traditionally deterministic, when usually a reference accident is defined to be used as a basis for drawing up corresponding emergency plans essentials on EP.

Nevertheless, the use of PSA could be helpful as a complementary tool for some aspects as mentioned before.

However, the use of PSA is limited. In this context, it is important that questions related to areas of applicability for probabilistic and deterministic analyses, as shown in Figure 2 [1] are determined prior to any decision of areas of PSA applicability to EZ tasks.

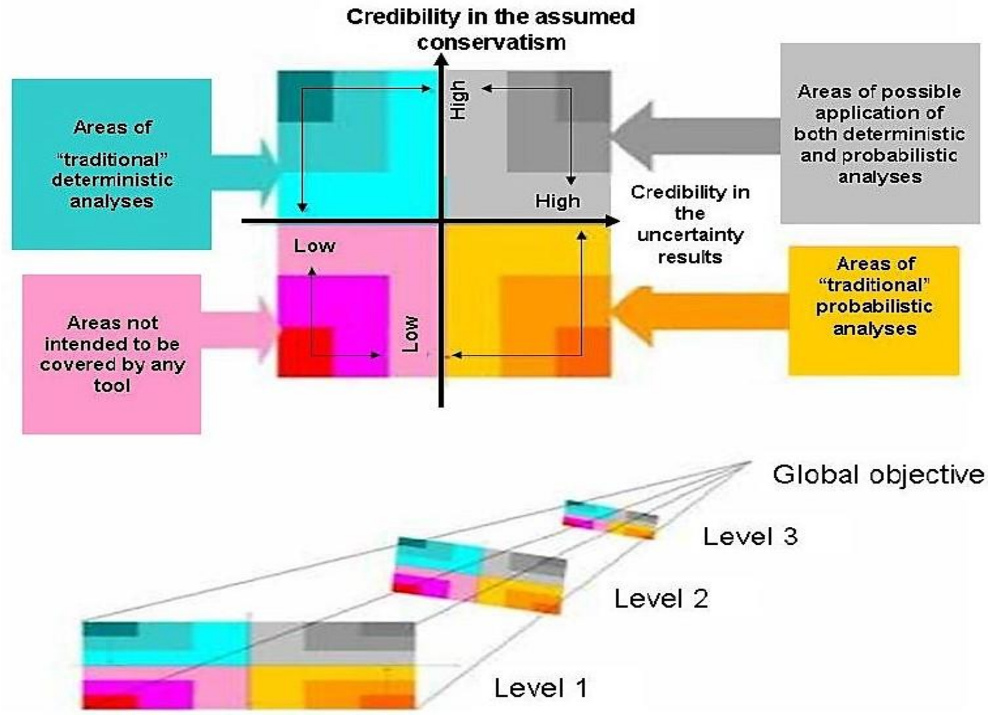

Credibility in the assumed conservatism
Areas of "traditional" deterministic analyses
High
High
Areas of possible application of both deterministic and probabilistic analyses
Credibility in the uncertainty results
Low
Low
Areas not intended to be covered by any tool
Areas of "traditional" probabilistic analyses
Global objective
Level 3
Level 2
Level 1

Figure 2. Applicability areas for deterministic and probabilistic methods [22]

Figure 2 shows that the expectation for PSA to have a higher impact in EZ is for the tasks in which the optimization of adopted (unnecessary) conservatism in safety margins is needed coincidently with a higher and/or measurable and reviewable degree of certainty on results.

This is actually the case for some EZ tasks as for instance the definition of EZ radius and the trend of harmonization in EZ on those issues.

1.2 Status of the existing generic results and approaches on EPZ for NPP

Other important aspects on EZ, except the definition of the EZ radius presented in the previous paragraph, which are considered of relevance for the investigation of the combined use of deterministic and probabilistic approaches are related to the:

- Postulated events and accidents for the NPP
- Definition of source terms

1.3 Specific features of PSA of importance in its use in EZ tasks

The PSA objectives and context are of high impact for its use on any application, including for EZ. In [16; 18] a set of results for various risk metrics in PSA studies is presented for all the period since early 1980's.

These surveys and the information on PSA referred in previous chapters present the PSA studies status. PSA studies are performed for various objectives and goals and with various limitations. Their intended use for various applications is also very diverse. Therefore, for all those situations there are some limitations well known for PSA, which have a direct high impact if they are to be used for EZ applications.

1.4 PSA metrics

PSA risk metrics are expected to have an important impact on the EZ application. The existing situation of PSA studies is summarized in [18] for the whole period since PSA started to be developed. As it is shown in Figure 3, there was a continuous change of requirements to risk analysis and thus a certain evolution of risk metrics can be noticed.

By risk metrics it is understood further mainly CDF (as the main result from Level 1 PSA -L1 PSA), LERF (as the main result from level 2 PSA - L2 PSA) and risk (as the main result from Level 3 PSA - L3 PSA).

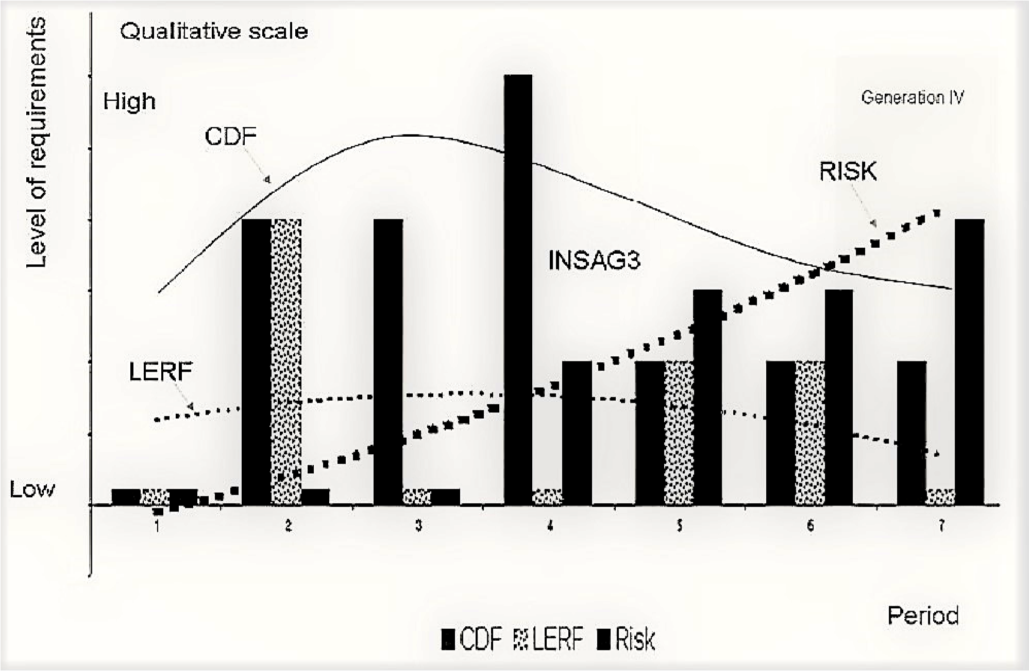


Figure 3. Risk metrics [22]

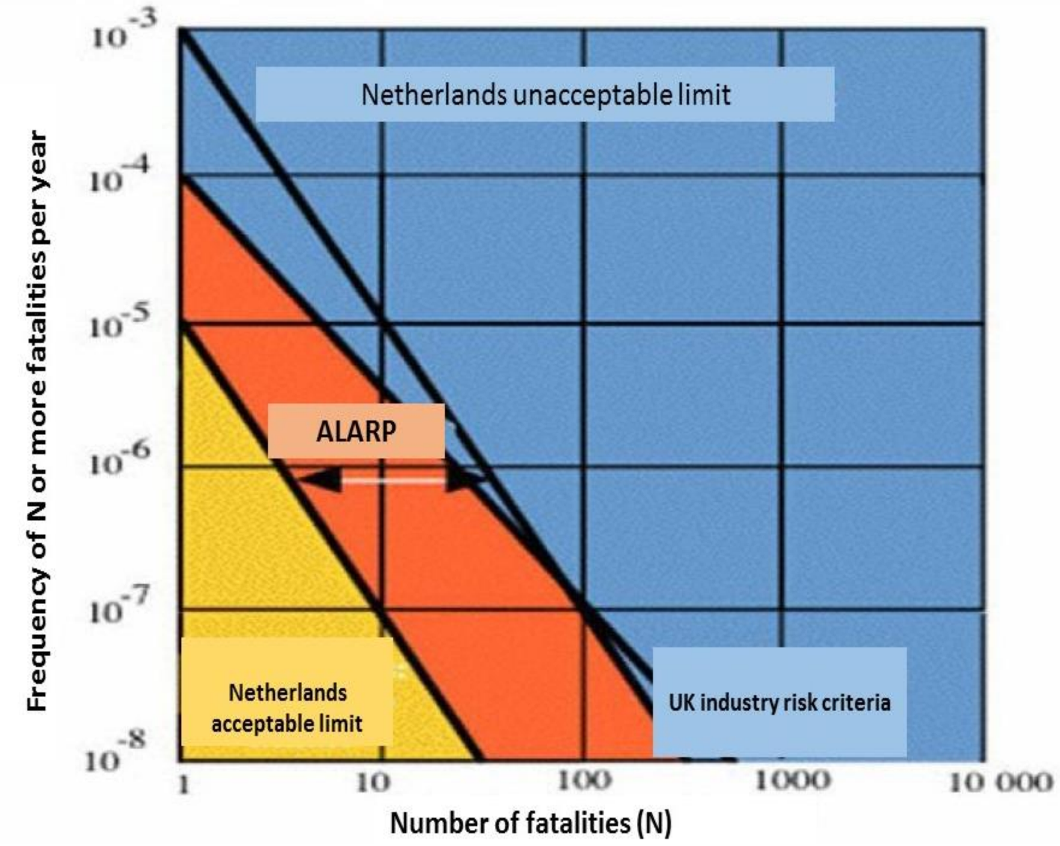


Figure 4. Risk acceptability criteria [23]

2. Description of methodology

2.1 The main PSA tasks changes for its use to EZ applications

Assuming that the generic aspects of PSA procedures are considered as discussed above and illustrated in previous chapters, then the next step in the use of PSA for EZ application is to define how specific tasks of L1, L2, L3 PSA are applicable and which are the differences (if any).

It is considered that, in principle, the tasks of PSA are applied as defined by standards for each level of PSA without modifications in order to use them in EZ application. However, some of the tasks need either special attention or some modifications for such a case. The next part presents those specific aspects for the tasks, which are considered to be of higher impact for EZ applications and some details on how some of the tasks in PSA have to be performed.

The tasks will be coded as ***Task PSA_EX_X***. The coding is used in order to underline the tasks which are important and to which more attention should be devoted. There are also some references not only to NPP of generation II+ and III, but also to generation IV. PSA starts by considering diverse and all sources of radiation and all scenarios challenging them, and therefore, it is highly suitable for EZ application. The results and insights from L2 PSA, in the format of LERF calculations based on various scenarios combined between L1 and L2 PSA in a process called “binning”, which is presented at PSA_EZ_1 below, lead to a conservative envelope of the EZ parameters.

This process is possible by application of the PSA procedure, which combines inputs from source term evaluation with containment impact - in event trees for containment, CETs, and by including results on phenomenological evolution of various scenarios calculated in the severe accidents codes, as it was described in previous chapters.

In fulfilling all below tasks for EZ application, no major change from standard procedures is expected. On the contrary, it is expected that the PSA approach of addressing all scenarios and challenges might be highly beneficial, providing more conservatism in comparison with the deterministic evaluations.

The logic of combining initiating scenarios and end states of containment and the final proposal of source terms might be the most important specific set of tasks from L2 PSA, making the difference between the deterministic and probabilistic approaches in EZ application.

Task PSA_EZ_1: Source Terms Evaluation
The identification of radioactive sources, of the timing of the release, of the quantity and chemical form of radioactivity released and the modeling of dispersion inside containment is a very important part requiring special calculations. In case of this EZ task a special attention is allocated to the choice of the source of radiation and the scenarios postulated. The PSA approach could bring, as a new part in this task, the

possibility to evaluate more comprehensively all the range of initiating events (as postulated in PSA) and to perform a series of severe accident calculations to define and refine the source term parts.

Task PSA_EZ_2: Sensitivity and uncertainty (S&U) analyses in L2 PSA methodology

The S&U analyses might be the next significant specific set of tasks from L2 PSA of high importance for the EZ application. This is due to how the following items are performed:

- Definition of PDSs;
- Number of nodes and endpoints defined in the containment event trees;
- Number of source terms and release categories defined;
- The assumptions resulted from the phenomenological codes runs;
- The independent alternative approaches are used in severe accident analyses;
- The independent alternatives perform a correlation between the probabilistic and deterministic descriptions;
- The S&U are actually performed.

Task PSA_EZ_3: Definition of the plant damage states

Definition of fault sequences that lead to core damage, which are identified in L1 PSA are taken forward into the L2 PSA. The groups obtained, called plant damage states (PDS), are defined in terms of the attributes that would influence the way that the accident progresses to challenge the containment integrity and to release of radioactive material to the environment.

The PDS attributes are specific to the type of reactors (PWR, BWR, heavy water channel type, etc.) as well as also for gas reactors. For generation IV gas reactors, for which there is no sense to consider core damage, but only release categories (RC), binning process is of much higher importance than for LWR. Things are also more sensitive to systematic errors for channel reactors.

The binning rules and results of the binning for PDS are of high importance and need to be subject to careful and independent reviews in order to assure accurate L2 PSA results.

Task PSA_EZ_4: Accident progression analysis

This L2 PSA task model the progression of the accident from core damage to the challenges to the containment and the subsequent release of radioactive material for each of the PDSs by using an event tree approach in the format of CETs or APETs. These event trees need to model all the significant physical and chemical processes, which might be actually the source of potential important systematic modeling errors. Those event trees require also inputs from specialized codes calculations. For the generation IV gas reactors with confinements the release categories defined for the CET are of special importance. The latest developments in PSA technique also take the advantage of integrated PSA models (including internal and external events, all modes of operation PSA models in one unitary model). This is of special help for the performance of intensive sensitivity calculations, which are considered in order to evaluate the impact of the modeling aspects on the results.

Task PSA_EZ_5: Severe accident modeling

The tasks of L2 PSA related to severe accident modeling are considered also to be subject of intensive review and check. This is mainly because the physical and chemical processes that are expected to occur during severe accidents typically involve many simultaneous phenomenological interactions for which detailed experimental information may be sparse or not available and therefore they use mathematical and computer simulation. For the generation IV reactors this is of one of the highest priorities.

Task PSA_EZ_6: Containment performance analysis

L2 PSA quality and accuracy of results potentially to be used in EZ applications depends on the containment performance analysis. For the water reactors of generation II+ and III, a series of containment integrity issues were identified during the experience accumulated so far and they could be found in [16;18]. Mechanisms challenging the containment function and the containment failure modes were extensively illustrated in [1]. Typical gas reactor confinement has, however, other problems and the whole mechanism is different. An illustration of such a confinement is shown in [20]. The energies of the released gas, the radioactivity carried away, and the timing, which have very high impact on severe accident concepts and the definition of EZ, give the difference. Nevertheless, the process required by this task is the same as the similar L2 PSA task, performed not for EZ application.

Task PSA_EZ_7: Quantification of L2 PSA model

The tasks of quantification in all PSA levels, including L2 PSA are important and related to the accuracy of the models, which are built using various software codes. The PSA models include also assumptions and interface with results from deterministic analyses. The quantification of the frequency of the various sequences from the containment event trees uses the data on frequencies of the PDS's, derived from the L1 PSA, and the conditional probabilities of the event trees. These probabilities include failure of safety systems such as the containment spray system (quantified also using fault trees) structural failures of the containment (quantified using a model of the performance of the structure), and the occurrence of physical phenomena where the split fractions relate to the analyst's evaluation.

For the split fractions, the numerical values are derived from judgment supported by available sources of information. After obtaining frequencies for PDS, fatalities are calculated for each release category (in case of generation IV gas reactors), or for PDS (for the water reactors) as shown in Figure 5. The results of L2 PSA are then post processed and used for PSA applications as licensing or EZ in the form of fatalities. It is important to mention that in Figure 5 the summary table for all the release categories and the total fatalities for all distances are already summed and normalized for the risk metric of L3 PSA, because the example is actually illustrating such a case.

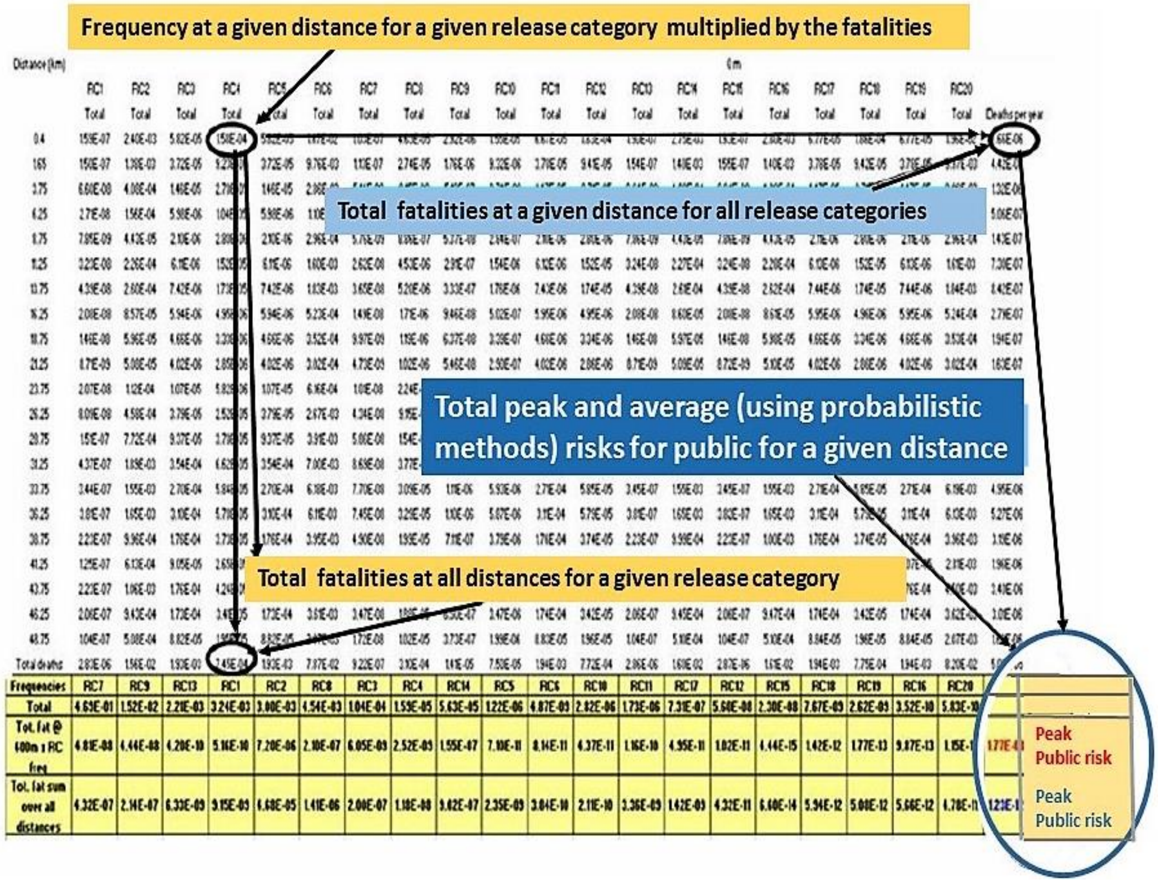

Frequency at a given distance for a given release category multiplied by the fatalities
Total fatalities at a given distance for all release categories
Total peak and average (using probabilistic methods) risks for public for a given distance
Total fatalities at all distances for a given release category
Peak Public risk
Peak Public risk
Distance (km)
Deaths per year
Total deaths
Frequencies
Total
Tot. fat @ 400m x RC freq
Tot. fat sum over all distances

Figure 5. Main steps for the calculation of risk criterion (PSA level 3) [1]

Task PSA_EZ_8: Use of computer codes and various models

A significant set of problems has to be solved for new applications in PSA for the computer codes used. The situation is increasingly complicated from L1 to L3 PSA because more advanced and higher-level codes are used and coupled, that results in dependency of their interface on connecting assumptions.

A special category represents the separate phenomena codes for L2 PSA, which are of two groups as it was mentioned in [1].

For each of those codes extensive verification and validation (V&V) was performed for water reactors. Some examples of the V&V actions for MAAP codes are presented in [47, 49]

Though for those codes their V&V process is very important, the most important aspect for PSA calculations is to be able to define and perform V&V for all the PSA flow path of the calculations using diverse codes.

As it was shown in [20], in case of performing such calculations for a generation IV gas NPP, there are some very important aspects to mention

- The error evaluation and uncertainty calculations should consider the fact that a set of codes are used for the full L3 PSA calculation;
- It was established that some diffusion codes have an error variation with the distance from the source (i. e NPP in EZ application);
- Many phenomenological codes are providing results with their own uncertainties and
- limitations, which have to be considered while being prepared as inputs to other codes;
- There is a need to define a procedure for uncertainty calculation of the whole calculation flow path for the risk metrics adopted in the EZ application.

Task PSA_EZ_9: L3 PSA process
In the L3 PSA, a large number of CET end-points are grouped to provide the interface between the L2 PSA and L3 PSA consequence analyses. This grouping and classification for L2 PSA and L3 PSA interfaces is called also “binning”, like the similar action between L1 PSA and L2 PSA. This subtask is of utmost importance for the PSA results and subject to extensive sensitivity analyses.

The flow path of L3 PSA as shown in [20] in a format of a series of code calculations and other assumptions, and this aspect is not usually mentioned. However, the definition of the calculation sequences and the codes to be used is one of the most important in order to obtain the risk metrics. The results are presented usually in risk metrics (risk for instance) and its uncertainty band.

Task PSA_EZ_10: Use of results and various risk metrics
PSA results are mainly in a form of risk metrics. As it was shown previously in Figure 5, there was a certain development of risk metrics requirements during the years. One reason for that is that not all the PSA like risk metrics are suitable for decision making process of many PSA applications. This statement is fully applicable for EZ, for which the use of CDF is the less desirable and adequate and the use of risk is the best option. This is also illustrated by the latest developments as shown for a case of using L3 PSA in applications similar to EZ [19]. In this case the risk metrics are represented in early fatalities/year, early injuries/ year, latent fatalities/year, thyroid cancer/year, whole-body person* rem / year, based on a series of sensitivity calculations to derive the envelope of the EZ parameters.

PSA calculations are done so that they lead to a reasonable envelope of the risk metrics of various scenarios and this is the main difference from deterministic calculations valid for EZ applications of PSA. The risk metrics are then represented with the range of their variation for all scenarios [20] for any type of NPP, including generation IV ones, as illustrated in Figure 6.

If the dependence of the risk metrics of a large set of parameters is considered, then one can actually obtain a set of acceptable risk surfaces as shown in Figure 8. To conclude on the use of various risk metrics, Figure 6 shows that the applicability of L3 PSA risk metrics to NPP EZ is much better than L2 PSA, while L1 PSA risk metrics is not expected to be of some help for the definition of EZ.

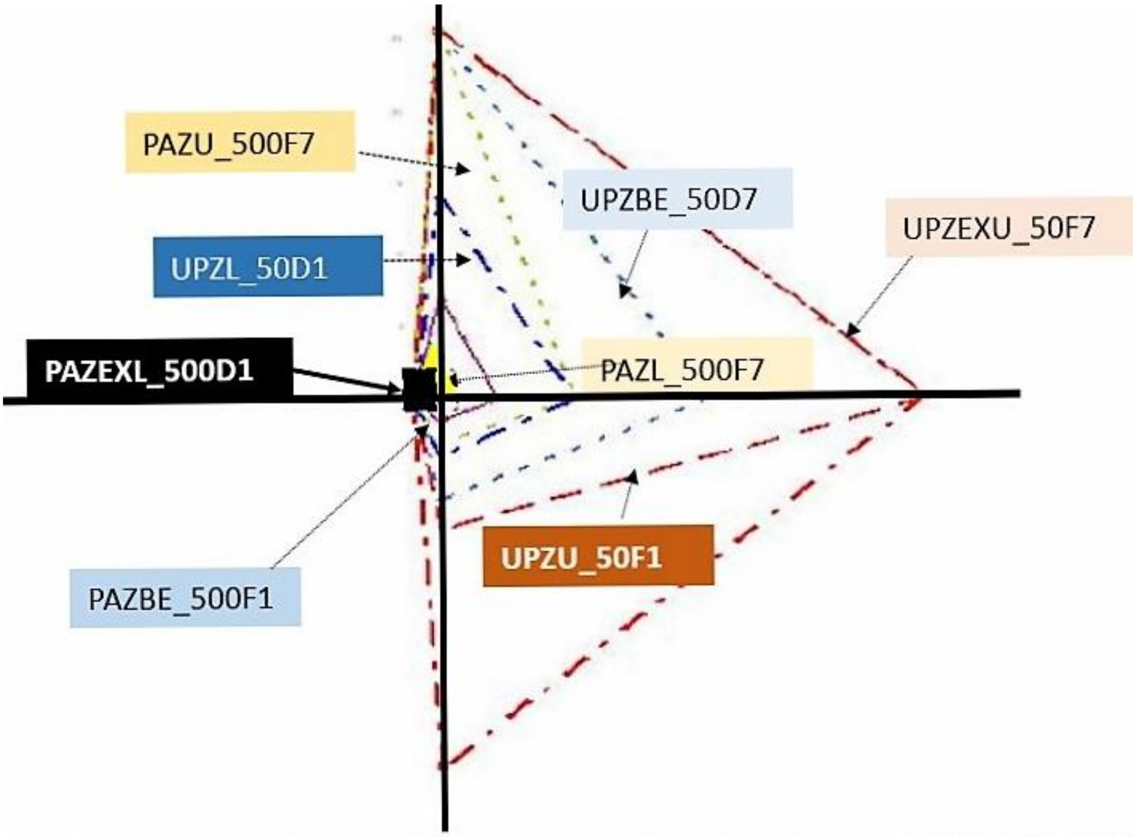


Figure 6. Sample case results for EZ radii as defined in Table 1[1]

Results of the case study use of PSA for EZ

PSA results for risk metrics as decided by the analysts (but considering the limitations mentioned above) can be used in order to evaluate parameters important to EZ like for instance PAZ and UPZ. Since PAZ and UPZ should be roughly circular areas around the facility, the results should be represented in a corresponding format. The PSA calculations are practically able to evaluate suggested PAZ and UPZ radii.

Task PSA_EZ_11: Use of PSA results for defining NPP EZ

PSA application for EZ includes the modeled barriers and scenarios aspects, common in nuclear safety for any kind of analyses (deterministic or probabilistic) as for instance DBA, BDBA, SA, fission product characteristics, meteorological considerations, exposure pathways, adverse health effects, and avoiding adverse health effects.

PSA performs evaluation of risk metrics considering all those aspects but using the strengths of the PSA method able to derive an envelope of all the challenges to the installation (initiating events) in one single unitary and systematic approach. However, there are limitations due to PSA performance and methodology, specific to each country and group of users, which could produce supplementary difficulties in the interpretation of PSA results for applications like EZ. For example, grouping of

NPP events including accidents by frequency of their occurrence differs in different countries.

Nevertheless as shown in Figures 7, 10, and 11, the expected PAZ and UPZ are distributed within a range of values. In order to decide on the final values, more information is needed to be available for the decision makers. It can be also mentioned, as shown in [20] that practically there is no expected fundamental difference for the calculations of EZ parameters of radii in case of a gas NPP of generation IV in comparison with a water reactor NPP. This is true even if decision on whether to have or not PAZ/UPZ and which are to be their magnitudes is still a debated issue.

For the sake of underlying the computational aspects of the radii in a deterministic like approach versus a probabilistic like approach, a set of simplified formulas can be derived as per (1) to (3):

$$\mathrm{Rad_d} = \mathrm{S_d} * R_\mathrm{d} * \mathrm{C_d} * \mathrm{Diff_d} * \mathrm{D_d} + \Delta \mathrm{U_d} \qquad (1)$$

$$\mathbf{Rad_p} = \mathbf{S_p} * \boldsymbol{R}_\mathbf{p} * \mathbf{C_p} * \mathbf{Diff_p} * \mathbf{D_p} + \Delta\mathbf{U_p} \cong$$

$$\cong \mathrm{S_p} * R_\mathrm{p} * \mathrm{C_p} * \mathrm{Diff_p} * \mathrm{D_p} * \int f1(Sp) * f2(Rp) * f3(Cp) * f4(Diff\,(p) * f5(Dp)dx \pm \Delta U \qquad (2)$$

$$\mathrm{Rad_p} = \mathrm{Rad_d} * f1(Sp) * f2(Rp) * \mathrm{f3(Cp)} * f4(Diffp) * f5(Dp) + \Delta\mathrm{U_p} \qquad (3)$$

Where,

S_d - Source term in deterministic approach
R_d – Reactor failure criterion in deterministic approach
C_d – Containment failure criterion in deterministic approach
$Diff_d$ - Diffusion criterion in deterministic approach
Dd - Fatalities criterion in deterministic approach
S_p - Source term in probabilistic approach
R_p – Reactor failure criterion in probabilistic approach
C_p – Containment failure criterion in probabilistic approach
$Diff_p$ - Diffusion criterion in probabilistic approach
D_p - Fatalities criterion in probabilistic approach
$\Delta U_{d,p}$ -Uncertainties in deterministic, respectively probabilistic calculations
ΔU - Final total uncertainties
f_1(Sp), f_2(Rp), f_3(Cp), f_4(Diffp), f_5 (Dp) - Distribution functions for the probabilistic criteria
f_{total} - Convolution of functions f_1 to f_5

For the cases represented in Table 4, a representation of PAZ and UPZ is shown in Figure 7.

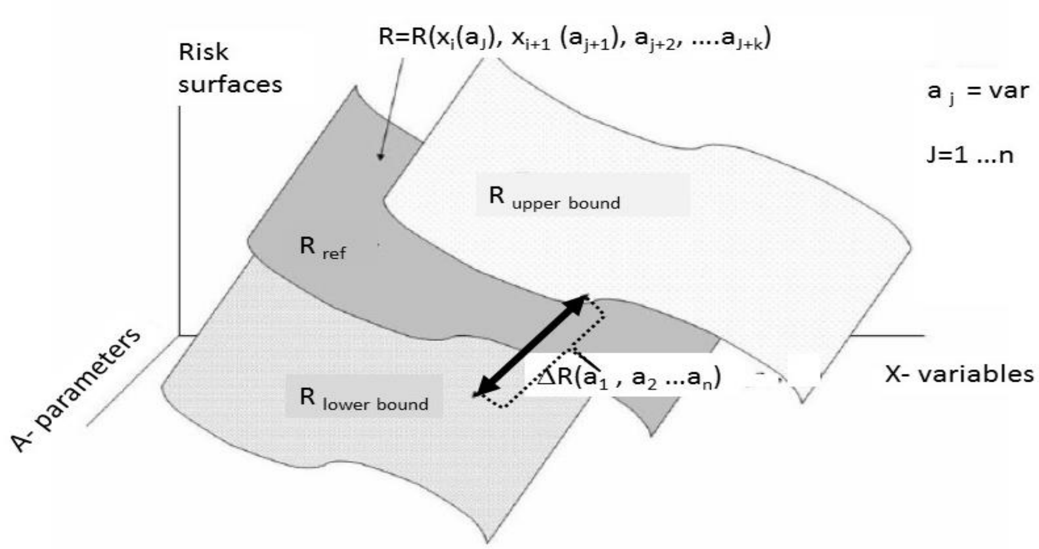

Risk surfaces
$R=R(x_i(a_j), x_{i+1}(a_{j+1}), a_{j+2}, \ldots a_{J+k})$
a_j = var
J=1 ...n
R upper bound
R ref
$\Delta R(a_1, a_2 \ldots a_n)$
R lower bound
A- parameters
X- variables

Figure 7. Risk surfaces for a PSA set of results [22]

The calculations from probabilistic point of view require combination of all the probabilistic criteria distributions, which is done by calculating convolution integral as shown in Figure 8. If the calculations have been performed for generation IV reactors, then there are not expected any changes in the type of results.

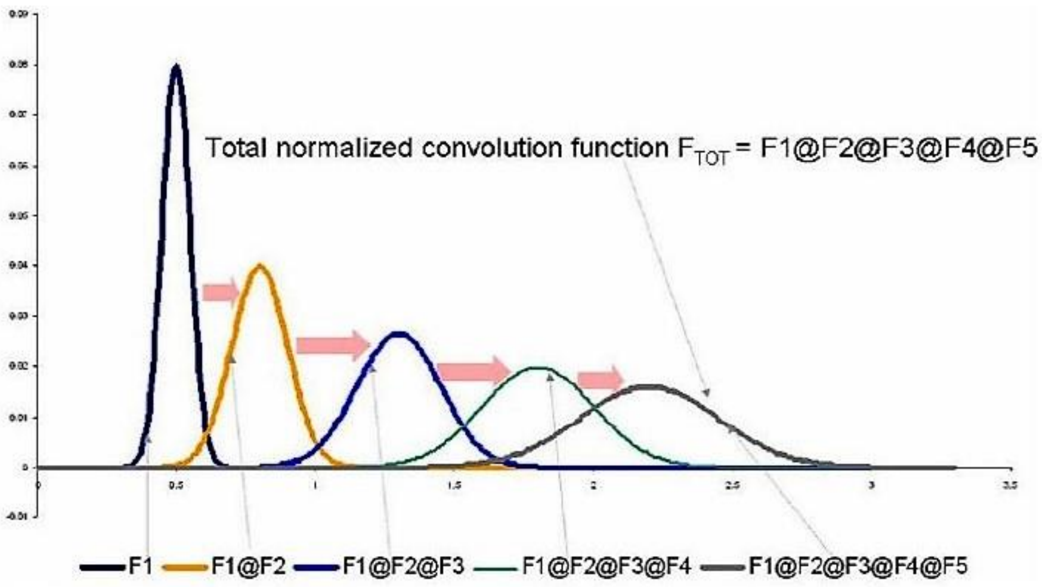


Figure 8. Convolution integral for total impact of factors in formulas (1)-(3)

Final results of L1, L2, or L3 PSA are actually represented by a set of surfaces within a certain error band, as a function of the probabilities of events and parameters governing the model.
After performing those calculations, the results are obtained in the form from (4) with some uncertainty band and a certain connection with the expected deterministic like result:

$$Rad_p = Rad_d * \mathit{ftotal} + \Delta U_p \qquad (4)$$

The calculation of the convolution integral is embedded in the PSA codes calculation and the flow of calculation was already shown in [20]. The formulas shown above are illustrating the fact that there is a traceable connection between the deterministic type of results and the probabilistic/risk metrics ones.

2.2 Results and some concluding remarks on the main aspects of the PSA use for EZ tasks

In the previous paragraphs there were illustrated some specific aspects and details of implementing PSA for EZ application, including some samples of PSA practical results.

However, it is of the highest importance to mention that obtaining risk metrics based EZ parameters does not constitute the end of the EZ application in PSA approach.

On the contrary, if the PSA based results are not using a specific approach in reasoning, which is called “risk informed decision making” (RIDM), then the conclusions could be fundamentally wrong. In order to apply RIDM one has to use carefully the logical connectors between deterministic, probabilistic and correlation statements.

The important aspects to be noted in relation to the use of PSA like results in the decision making process based on the use of decision tables is (as shown in [20]) that it is highly recommended to use a risk informed type of approach in formulating the final decision.

This is due to the fact that risk results require probabilistic type of inferences in the judgments to build decision tables. This involves also a very clear description of the limits and strengths of deterministic and probabilistic results for EZ parameters.

Based on the results of combination of various approaches (optimistic, pessimistic, etc.) using insights from all methods, i.e. deterministic and probabilistic, a decision on the EZ parameters can be taken.

To summarize, it is highly recommended to consider deterministic and probabilistic approaches being complementary. An example of formulation of results interpretation of the EZ parameters by using different approaches, i.e. deterministic and probabilistic, and for various events and for various risk zones could be as follows [22]:

- If the decision is aimed at evaluating high foreseen risk situations above the acceptable limits, then the deterministic pessimistic statements may lead to the most conservative decision, even if that happens under less credibility than for the probabilistic ones. On the other hand, due to other reasons than technical ones, the deterministic based decisions could be expected.
- If the decision is aimed at evaluating high or moderate foreseen risk situations below the acceptable limits, then there is no difference between the very pessimistic way of thinking and optimistic one, or a probabilistic one. However, there is an exception based on the fact, that the probabilistic evaluation has more credibility, which could make it the best option to choose for the decision.
- If the decision is aimed at evaluating low and very low foreseen risk situations below the acceptable limits, then it may be based on the probabilistic approach, giving the fact that it generates the most conservative results with highest credibility. Evaluation of risk impact using extensive sensitivity cases is one of the key issues to support the probabilistic type of thinking and its more extensive use in decision making process.

This is integrated in the verification and validation process, of which independent review and benchmarking play a very important role in confirming the truth-value of probabilistic statements. In a geometric representation that means, that the EZ radii could be illustrated as a set of spectrum available values from low bound to upper bound with a certain best estimate set of values, as shown in Figures 9 and 10.

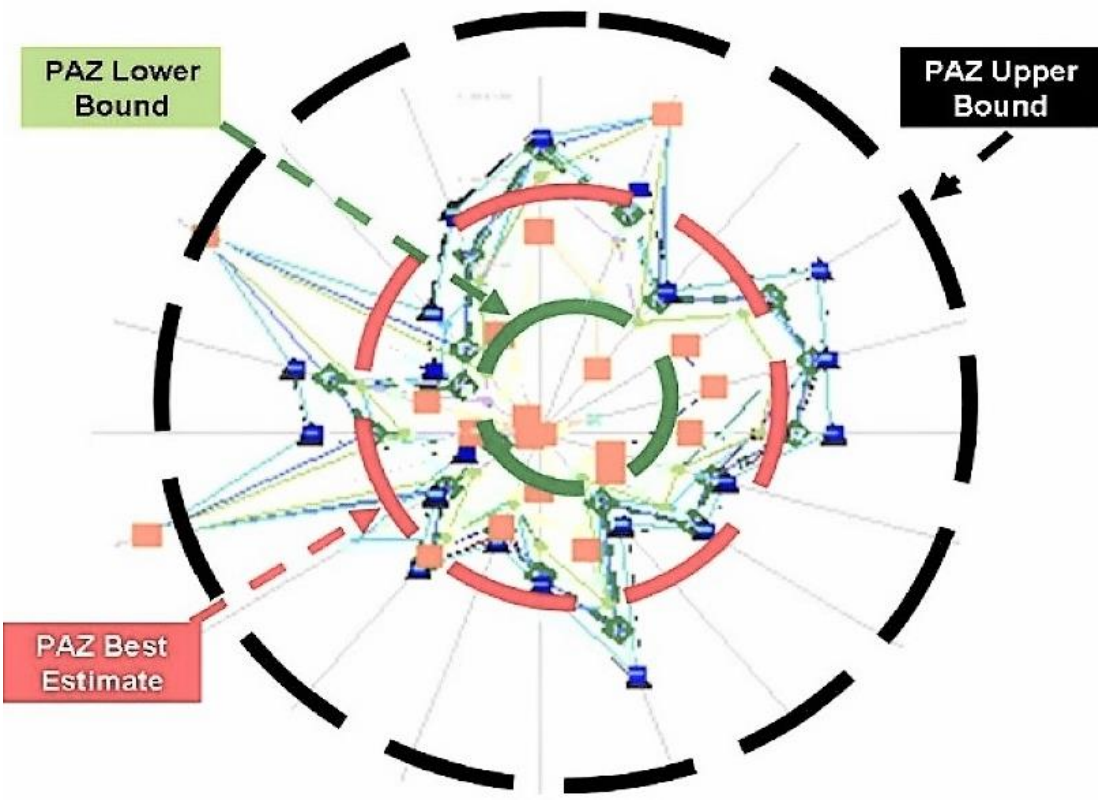


Figure 9. Representation of results for the case in Table 1 and Figure 6 underlying the relationship between various versions of calculations (optimistic vs pessimistic)

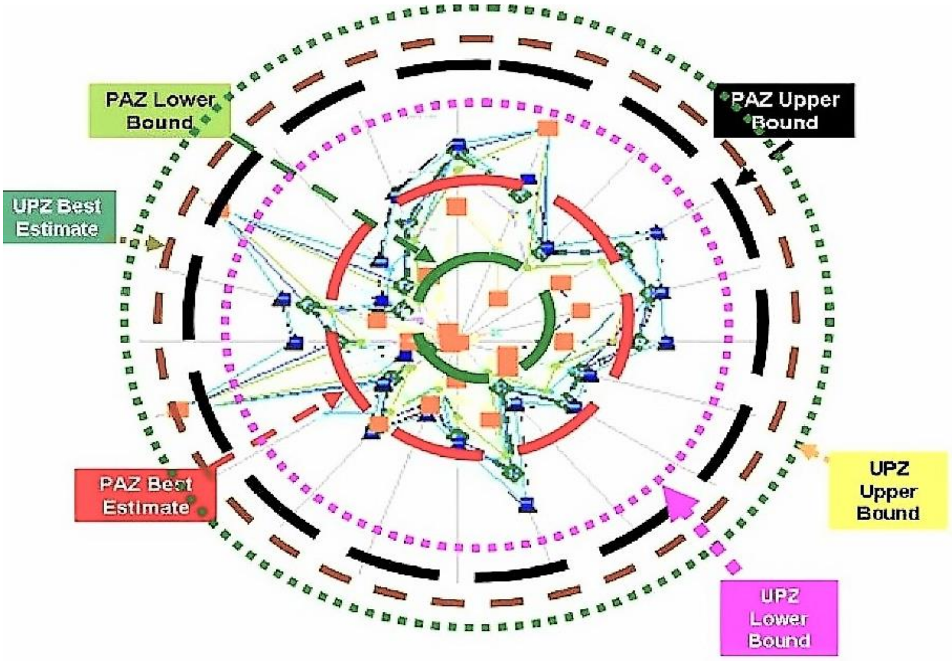


Figure 10. Representation of results for the case in Table 1 and Figure 6 underlying the relationship between various versions of calculations (optimistic vs pessimistic)

The last very important point of the performed evaluations is related to EZ parameters of multiple NPP units from various generations on the same site, as shown in Figure 11.

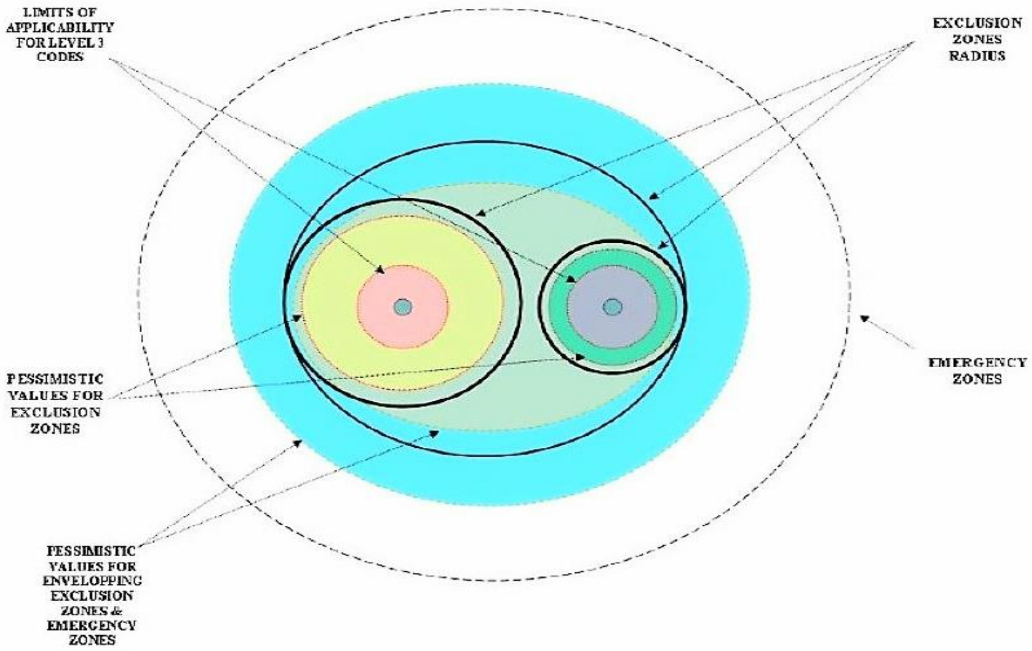

LIMITS OF APPLICABILITY FOR LEVEL 3 CODES
EXCLUSION ZONES RADIUS
PESSIMISTIC VALUES FOR EXCLUSION ZONES
EMERGENCY ZONES
PESSIMISTIC VALUES FOR ENVELOPPING EXCLUSION ZONES & EMERGENCY ZONES

Figure 11. Representation of results for the case in Table 1 and Figure 6 underlying the relationship between various versions of calculations (optimistic vs pessimistic) for a multiunit case

3. Conclusion

The specifics of using PSA for EZ tasks are mainly depending on the possibility to solve the problems of RIDM application for EZ and the evaluation of the uncertainty and degree of conservatism in EZ decision-making process.

One of the key challenges in dependable RIDM is the reconciliation of PSA results and insights with traditional deterministic safety analysis. This is particularly true when it comes to defense in depth and safety margins. PSA results may and often conflict with deterministic insights. If a method of reconciling these conflicts is not defined, then RIDM can become deterministic assessment, along with PSA.

These results in PSA are an additional layer of requirements rather than a tool for optimized decision-making [11].

In [1] the issues raised by the use of PSA as a complementary tool for a balanced approach in RIDM on EZ issues has been done and illustrated on some specific examples, resulting in the realistic, feasible outcome from NPP emergency zoning practice.

There is a general agreement that RIDM has the potential to contribute towards maintaining and improving nuclear safety. It can complement the deterministic approach to nuclear safety and maintain the concepts of defense in depth and adequate safety margins. However, RIDM is broader concept than just the use of PSA in NPP applications. RIDM uses the results of PSA as one input to the decision making process, but allows for consideration of other factors, in particular aspects of safety management and safety culture. At present, these aspects are included in PSA only to the extent that they are reflected in the plant-specific data used, but they are not explicitly modeled in PSA [12].

RIDM in NPP EZ is a process, which can be used by the utility and the regulator, and provides the framework for risk informed regulation in this area. The objective should be to enhance regulatory effectiveness, using risk information to optimize nuclear safety regulation.

Whether risk informed regulation is of benefit to utilities depends to a large extent on the common understanding developed with the regulatory authorities.

Since the preparation of a PSA imposes a considerable burden in terms of the human and financial resources that need to be expended, it is of utmost importance to define clearly what is expected from the utility and how the results will be used. This common understanding can be developed in a dialogue that includes all stakeholders. RIDM would strengthen the perception that the operator is assuming the primary responsibility for safe operation. RIDM in areas that affect licensee requirements necessitates review (and, ultimately, approval) of PSA and supporting information by the regulatory body. A suitable regulatory framework and regulatory staff with considerable technical capabilities in the areas of PSA and risk informed decision making are prerequisites for such review and approval. This constitutes a considerable burden for countries with small nuclear programs and limited numbers of regulatory staff [12].

It is necessary to ensure the availability of high quality PSA to support RIDM. The meaning of “high quality” in this context can vary and is defined as being commensurate with the intended use. Several IAEA as well as EU Member States have developed national PSA guidelines, and the IAEA has prepared guidance on PSA quality for applications in NPP at the international level [13].

The American Society of Mechanical Engineers (ASME) has developed a standard on PSA. Additional efforts to promote the production of high quality PSA include peer reviews, establishment of user groups for similar type of plants, pooling of data and preparation of reference PSA [12].

RIDM in NPP emergency zoning can be successful - like in other areas - only if all stakeholders understand the process and the results obtained.

In addition to the main nuclear regulatory body, a licensee has to deal with several other regulatory organizations, e.g. those responsible for environmental protection. If the concept of RIDM in NPP emergency zoning is not shared by these other authorities, this might complicate the decision making process. Thus, consistency between the approaches followed by different authorities would be beneficial. Owing to the state-of-the-art understanding and increased characterization of NPP severe accidents as well as advanced understanding of PSA technology, which can be currently considered mature enough, overall management of NPP severe accidents could be – and also should be - analyzed as an integrated complex process.

The interrelationship of NPP emergency operating procedures, safety and risk assessments, severe accident management guidelines, and emergency off-site actions should be planned and organized to minimize the consequences of such accidents. This approach might be a contribution to ensure the continued safety of NPPs and to improve effectiveness of regulatory practices in EU Member States.

As the transition to risk informed regulation is taking place gradually more or less worldwide, activities conducted within this project represent comprehensive application of PSA technology to contribute to NPP emergency zoning issues. This report indicates clearly that the current, state-of-the-art PSA technology is significantly able to contribute – as a complementary tool - to the traditional engineering, deterministic approach to addressing various issues of NPP emergency planning practices, especially emergency zoning and might be highly topical at present in terms of regulatory effectiveness in EU Member States.

And finally, there is one more facet of the subject matter: some safety consequences resulting from economic pressure on NPP operators as a result of deregulation of electricity markets.

Although deregulation is not the only reason why nuclear operators have intensified their efforts to reduce costs and become more efficient, it is clear that the industry is changing and that regulators must prepare for this new situation. This report would not like to outright advice regarding any prioritizing.

This must follow from the assessment of the national situation in each EU Member State.

However it was the intention of the authors of this paper to hope that the paper insights will be of help in this assessment and in thorough consideration to the subject.

References

[1] Jozef Kubanyi, Ricardo Bolado Lavin, Dan Serbanescu, Bela Toth, Heinz Wilkening, Risk Informed Support of Decision Making in Nuclear Power Plant Emergency Zoning Generic Framework towards Harmonising NPP Emergency Planning Practices European Commission, *DG JRC Institute for Energy* January 2008 EUR 23280 EN

[2] IAEA, *Method for the Developing Arrangements for Response to a Nuclear or Radiological Emergency*, EPR-METHOD (2003), ISBN 92-0-111503-2, IAEA, Vienna,2003,at http://www-pub.iaea.org/MTCD/publications/PDF/Method2003_web.pdf

[3] RASCAL 3.0, Description of Model and Methods, *NUREG-1741, US NRC*, Washington DC, 2001.

[4] Severe Accident Risk: An Assessment for five US Nuclear Power Plants, NUREG -1150, US NRC, Washington DC, 1990, at http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1150/

[5] Generic Environmental Impact Statement for License Renewal of Nuclear Plants. *NUREG-1437, Vol. 1, US NRC*, Washington DC, May 2001, at http://www.nrc.gov/readingrm/doccollections/nuregs/staff/sr1437/v1/part05.html#_1_129

[6] IAEA International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources, Safety Series No. 115, *IAEA*, Vienna, 1996, at http://www-pub.iaea.org/MTCD/publications/PDF/SS-115-Web/Start.pdf

[7] Libmann, J.: Elements of nuclear safety. IPSN, *Les Editions de Physique*, 1996 (ISBN: 2-86883-286-5).

[8] Apostolakis, G. E.: How Useful Is Quantitative Risk Assessment? *Risk Analysis*, Vol.24, No. 3, 2004, p. 515-520.

[9] Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications, *ASME RA-S-2002. An American National Standard, The American Society of Mechanical Engineers*, New York, NY 10016, USA, 2002.

[10] OECD NEA, Recent Developments in Level 2 PSA and Severe Accident Management. *A Supplement to Report NEA/CSNI/R91997)11, OECD NEA*, (Draft).

[11] Niehaus, F., Szikszai, T., Risk-informed Decision Making, Topical Issues Paper No.1, *Proceedings of International Conference on Topical Issues in Nuclear Safety,* IAEA, 3-6 September 2001, Vienna, Austria.

[12] Risk-informed Decision Making, Topical Issues Summary. *Proceedings of International Conference on Topical Issues in Nuclear Safety, IAEA,* 3-6 September 2001, Vienna, Austria.

[13] IAEA, Determining the quality of probabilistic safety assessment (PSA) for applications in nuclear power plants. *IAEA-TECDOC-1511, IAEA* Vienna, 2006.

[14] An American National Standard ASME RA-Sa-2003, Addenda to ASME RAS-2002 Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications. *The American Society of Mechanical Engineers, New York*, NY 10016, USA, 2002.

[15] Jay Wu; Yung-Muh Yang; Ing-Jane Chen; Huan-Tong Chen; Keh-Shih Chuang: Reevaluation of the emergency planning zone for nuclear power plants in Taiwan using MAACCS2 code. *Applied Radiation and Isotopes 64 (*2006), pp. 448-454, ELSEVIER 2006, at www.elsevier.com/locate/apradiso

[16] OECD, Level 2 PSA Methodology and Severe Accident Management. Prepared by the *CNRA Working Group on Inspection Practices (WGIP),* CDE/GD(97)198 , Paris, 1997.

[17] Durham, F.A., Camp, A. L., Apostolakis, G., and Golay, M.: A Framework for Regulatory Requirements and Industry & Standards for New Nuclear Power.SAND2000-1598C, *International Conference PSAM 5*, 27 November-01 December 2000, Osaka, Japan.

[18] NEA OECD, Level-2 PSA for Nuclear Power Plants. *CSNI Technical Opinion Papers No. 9, OECD 2007,* NEA No. 5322, ISBN 978-92-64-99008-1.

[19] Levinson, S., H., Doug, P.: Beyond level 1 & 2 PSA's: B&WOG's development of level 3 models. *International Conference PSAM 6, 23-28 June 2002, Puerto Rico, USA*. 0-0804-4120-3, Elsevier Science, 2002.

[20] Serbanescu, D.: Sensitivity and Uncertainty Issues in the Integrated PSA Studies, EC DG JRC-IE/OECD NEA *International Seminar on Emergency & Risk Zoning around Nuclear Power Plants, 26-27 April 2005*, Petten, Netherlands.

[21] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Functional safety of electrical/electronic/programmable electronic safety-related systems. International Standard IEC 61508, Geneva, 1998-2000.

[22] Serbanescu, D.: Some specifics of the use of probabilistic risk analyses as a support to the evaluation of safety margins and the interface with the deterministic based decisions. *IAEA Technical Meeting on Effective Integration of Deterministic and Probabilistic Safety Analysis in Plant Safety Management, Barcelona,* Spain, 4 – 8 September 2006.

[23] Charpin, F., Raimond, E.: Chaumont, B.: Technical basis for off-site emergency planning in France. *Proceedings of the EC DG JRC-IE/OECD NEA International Seminar on Emergency & Risk Zoning around Nuclear Power Plants*, 26-27 April 2005, Petten, Netherlands.

Risk informed inspection and decisions making

Robertas Alzbutas
Lietuvos energetikos institutas, Kauno technologijos universitetas
Breslaujos str. 3, LT-44403 Kaunas, Lithuania

Abstract

During recent years, both the nuclear and non-nuclear industry and regulatory bodies have recognized that probabilistic safety assessment (PSA) has evolved to the point that it can be used increasingly as a tool in decision making and particularly in risk informed inspection. In this paper the Risk Based Inspection (RBI) or Risk Informed In-Service Inspection (RI-ISI) and Integrated Risk Informed Decision Making (IRIDM) approaches are considered. PSA are complementary to the deterministic and defence-in-depth philosophy and is advocated to be used in safety-related decision making, e.g. for optimizing activities related to in service inspection, testing, and maintenance.

The following topics are discussed in this paper:
- The integration of deterministic and probabilistic approaches in order to define integrated risk measures and approaches for risk-informed decisions when deterministic and probabilistic methods integration are used;
- Decision making and risk management in order to minimize risk, using proper inspection and maintenance procedures, as well as seek other benefits additional to safety improvements and risk reduction.

The methods application includes results, obtained through the author's participation in a number of related research and students projects.

Keywords: Risk-informed Approach, Probabilistic Modelling, Risk Management, Decision Making, In-service Inspection.

1. Introduction

In general, the risk measures minimization and application to inspection is risk informed action and is related to the process of decision making. The general concept of risk informed decision making (RIDM) was described in TECDOC-1436 [1] and further discussion of the integrated risk informed decision making (IRIDM) process was given in INSAG-25 [2], which presented a framework for the decision making process. One of the aims of these publications was to provide a common understanding in the international nuclear community (designers, suppliers, constructors, licensees, operators, technical support organizations, and regulatory bodies) of how to implement a risk informed decision making process. However, both publications did not provide guidance on how the IRIDM process should be established and carried out in practical manner or even specifically for risk measures minimization and application to inspection.

The risk-informed approach with appropriate risk measures/estimates aims to integrate systematically quantitative and qualitative, deterministic and probabilistic safety considerations. There is explicit consideration of both the probability of events, i.e. failures, and their potential consequences, supported by consideration of sound engineering practice and managerial arrangements. Estimates of risk, likelihood and consequence, are based on knowledge or data from experience, or derived from a formal, structured analysis such as a Probabilistic Safety Assessment (PSA).

1.1 Key Elements of the IRIDM Process

The key elements of the IRIDM process are shown in Fig. 1 below, which is based on the descriptions of a framework and the process given in INSAG-25 [2]. The IRIDM process shown in Fig. 1 below includes several Key Elements (KE), each of which has implicit risk aspects. Each KE comprises several Constituent Factors (CF) (not shown on Fig. 1 below), which further define the safety requirements and other conditions, and are used to evaluate the options being considered. In any particular application, not all the KE, nor all their CF, will be relevant to the issue under consideration. The aim of defining this framework is to better focus licensee and regulatory attention on design, operational and security issues commensurate with their importance to public health and safety.

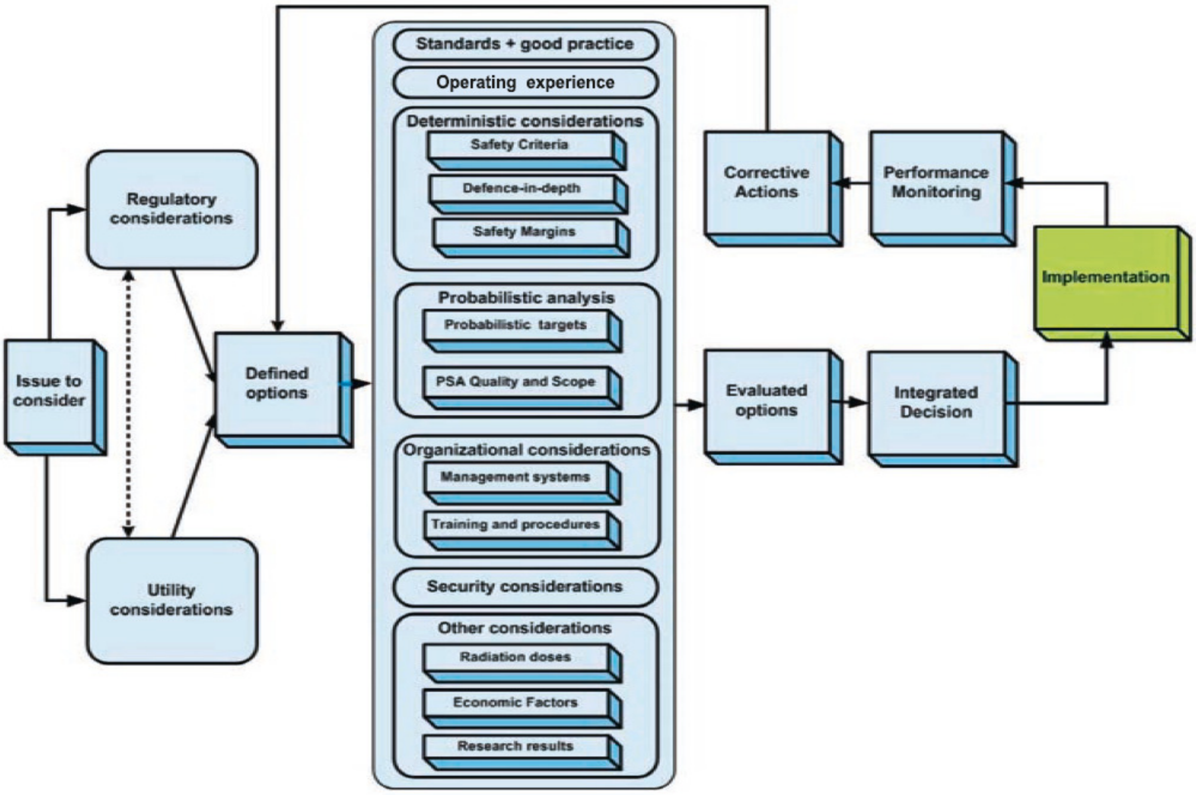


Figure 1. Key elements of the IRIDM process (based on IAEA INSAG-25 [2]).

1.2 Stages in Performing General IRIDM Process

The general process for the RI Decision Making includes the following main stages:

- Stage I Characterization of the issue and team formation;
- Stage II Preparation for the evaluation of the options;
- Stage III Assessment, integration and documentation;
- Stage IV Selection of the option to implement;
- Stage V Implementation of the selected option;
- Stage VI Performance monitoring.

The stages listed above reflect the logical order of tasks to be performed. Some of the associated activities may be performed in parallel. Hence the order of stages does not represent a sequence in time. Iterations between the different stages may also be necessary. After completion of stage V, the results of implementation of the selected option are monitored.

The IRIDM process as carried out in the organization should also be periodically reviewed and improved if deemed necessary. The IRIDM process can be adjusted specifically to risk measures minimization and application to inspection.

2. Issues of Integrated Risk-Informed Decision Making

As considered in various papers and projects, like in the ongoing project ASAMPSA_E (see [3] and acknowledgements), there is no common understanding on the correct (or even appropriate) approach to decision making regarding risk in the scientific community as well as with actual end-users. Depending on the subject matter to decide and the role and the interest of the decision maker or stakeholder, different approaches to decision making are advocated or rejected [1], [5], [6], [7], [8], [9]. Moreover, the acceptability of these approaches to the stakeholders or the society obviously depends on the culture of the society in question and the specific values and believes on risk acceptance on a personal and societal level [10]. For the purpose of risk minimization, work on the ethical or legal or theoretical foundations of decision making [11], [12], [13] is clearly out of scope, as it is more a discussion on cultural influences.

It is important to note that the aforementioned issues have partial implications for the further discussions contained in this paper. Decision makers are influenced by factors that transcendent natural science and cannot be resolved in a strictly objective manner in this sense. Consequently, implicit and explicit utility considerations on decision alternatives will necessarily have a strong subjective component. Furthermore, the relevance of information, e.g. from PSA, the acceptability of certain kinds of risks, and finally the adequacy of risk measures to support decisions will depend on the decision maker. In the end, the decision maker has to decide which aspects of risk and thus which risk measures are relevant for each alternative. Therefore, the discussions in this paper have to be understood as options for decision makers. The presented approaches have been identified as suitable for a wide range of typical situations and they might help to select the best decision alternative. The approaches should not be interpreted as a fixed set of rules which can be applied to every situation. Similarly, they might lead to results which decision makers do not agree with. Thus, even if decision makers and PSA analysts follow the approaches in the paper, they should be free to select alternative approaches. It is therefore essential that PSA analysts and decision makers agree on the scope of approaches application at an early stage.

2.1 Integration of Deterministic and Probabilistic Approaches

Various recent researches and analyses of complex systems safety methods show that integration of various methods can present more accurate and practical results, which cannot be obtained by single methods used up to now. Two approaches basically different in its nature are based on deterministic analysis and probabilistic analysis. They also can be practically applied for decision making even without any consideration of risk.

Actually, the risk measure is defined in different ways for specific purposes. There is no such one way of defining risk, which is always more adequate than another, since this will depend on the purpose of defining risk. The developed Integrated and Risk-informed (IRI) approach uses risk measures based on qualitative or quantitative information. IRI approach is not a probabilistic approach, which is alternative to the deterministic one, but it is a combination of both. In the integrated risk-informed approach fundamental deterministic safety principles, mainly defence-in-depth and sufficient safety margins, have to be maintained, even if probabilistic evaluation would indicate the safety level, which is already high enough.

The risk measures used in risk-informed approach is related to decision models. It is important to stress that risk information (e.g. from PSA) in IRI approach is not used in order to find the best solution in terms of safety but to select the most efficient solution among a number of alternatives, while achieving the required safety level.
The main elements of integrated risk-informed approach:

- Safety analysis, using deterministic approach and defence-in-depth philosophy;
- Probabilistic evaluation of risk (insights from PSA);
- Knowledge from operating experience.

One basis of integrated approach, the doctrine of determinism, assumes that any failure has a cause and can be explained and in reality, there are no random failures. It is a matter of knowledge in order to identify, model and explain the cause of any event or effect. Another fundamental concept of deterministic doctrine is that everything could be understood by analysis.

The quantitative analysis in deterministic approach considers the performance of components and compares it with required performance capability under design basis conditions. The analysis process involves the identification of functional failure modes or states of components. In addition, the performance margins between component specific performance capability and the defined design basis performance capability is analysed for each identified functional failure mode or state.

The pure deterministic approach is very effective to achieve a very high safety level. The used or assumed simplicity and predictability also somehow helps in decision making. However, its main disadvantage is that it is not efficient regarding the use of resources (human, financial, others) according to the impact on risk. The decisions produced by deterministic design principles usually have a very high range of conservatism. This is natural, because the same criteria are applicable for high-risk systems and low risk systems. In addition, it is possible to recognise that some practical situations are too complex to clearly identify what is conservative and what is not. An action that is good from one side may be bad from another side (e.g. possible safety-security conflict for decision making). In spite that probabilistic approach can be conservative as well, the more advanced ranking of problems and resources, used for decision-making, is based on measure, received using integrated risk-informed approach. Also, the more advanced ranking process can be based on probabilistic sampling and probabilistic sensitivity analysis.

2.2 Definition of Integrated Risk Measure

The definition of risk measure depends on the approach to risk. The choice of a qualitative or quantitative approach is based on the level of available detailed information and the level of rigor and confidence required (e.g. for regulatory acceptance). In determining the integrated risk-informed measure, associated with operation and inspection of a given plant structures, systems and components, in general, four aspects are considered, namely:

1. The failure mode or state;
2. The likelihood of detectable failure;
3. The likelihood of reliable detection of failure;
4. The consequences of failure.

The integration of deterministic and probabilistic approaches is proposed to be made using different methods. The nature of simpler qualitative approach is that it can only act as an indicator of risk, which can be used for simple screening, and does not constitute a risk assessment. Without strict definition, the risk is proposed to be expressed as the combination of the qualitatively assessed actual frequency of failure and the consequences of failure. In developed scheme, the actual frequency of failure is quantitatively expressed as the combination of likelihood of detectable failure (i.e. empirical frequency) and likelihood of unreliable detection of failure (i.e. probability of non-detection).

If qualitative ranking, such as high, medium, and low are used, the rank of this risk kind is limited because there are only nine possible combinations. In this case, a simple bar matrix is proposed to be illustrated in a manageable fashion as schema for risk estimation and results visualization (see the following figure). The values of this matrix are the combination of probabilistic importance evaluation (high, medium, and low) in the actual failure frequency axis and deterministic importance evaluation (high, medium, and low) in the consequence axis.

In general, the risk level increases if there is the increase in the actual and empirical frequency of failure and in the probability of non-detection of failure events as they affect the increase of empirical frequency of failure. In quantitative expression case, the normalized parameters' values (e.g. 1, 0.1, 0.01, and etc.) can be used for risk evaluation.

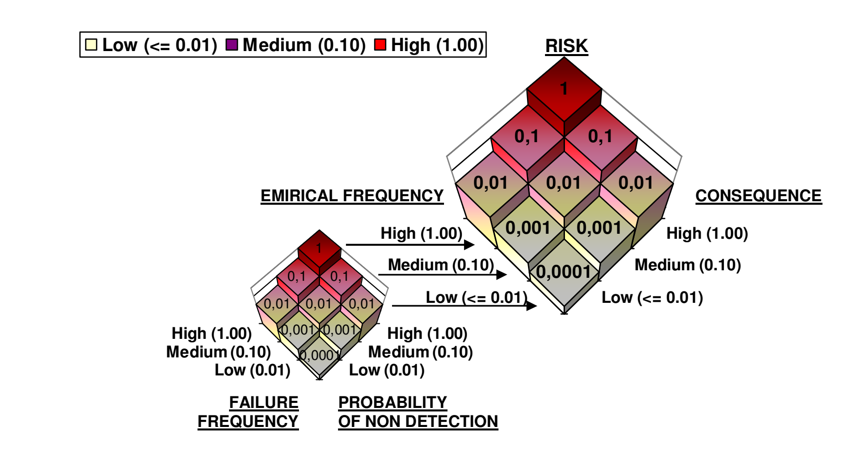


Figure 2. Simplified schema for qualitative risk estimation and results visualization.

In order to reflect the impact of inspection and probability of non-detection, the more precise and formal mathematical quantitative definition of risk for one component can be expressed as follows:

$$R_c = \sum_i \sum_d \sum_s [f_i \cdot p_i \cdot P(d \mid i)] \cdot P(s \mid d) \cdot C(c \mid s) \cdot \qquad (1)$$

Here, R_c is the risk of consequence expressed by measure c, f_i is the frequency of the detectable initiating event i (i.e. failure frequency), p_i is the probability of non-detection of initiating event i, $P(d|i)$ is the conditional probability that the initiating event i will lead to plant damage state d; $P(s|d)$ is the conditional probability that plant damage state d will lead to the source term (radioactive release) s, and $C(c|s)$ is the conditional consequence measure, c, given the occurrence of source term s. The proposed risk measure is more complex than the typical one as the failure frequency is evaluated, using the separation of information, related to the probability of empirical failure and the probability of detection of failure.

The results of typical probabilistic risk assessment study in nuclear industry can also be treated as risk measures. The selection of appropriate quantities, resulting from PSA as risk measures, and target quantities for optimisation is a very important step (see [4] to get a view on existing risk measures). The results of optimisation depend on this selection. For instance, risk measures in nuclear industry can be defined for each component in terms of annual core damage frequency (CDF) and, if available, in terms of annual frequency of large early release (LERF). However, in order these measures to be consistent with R_C measure, the reliability of detection and the conditional estimates of initial events probability should be investigated additionally.

Operational Experience Application

Plant specific operating experience should be used in determining both the initiating event frequencies and initiating event consequences. A continuous plant specific data collection and processing system should be set up and maintained as it is considered important for the achievement of reliable data. For that purpose, there is a demand to have the operating experience feedback programmes which yield plant specific data for the use in the PSA. Generic data is used only when plant specific data does not exist or it is so scarce that reasonable and reliable estimates cannot be provided. The estimation of reliability parameters (e.g. failure frequency) are supported by a Bayesian updating of generic data if necessary.

Ideally, the considered parameters of risk model should be based on detail operational data of considered system. However, due to small quantity or unavailability of system-specific data the risk assessment often has to rely on various sources and types of information:

- The general engineering (expert) knowledge;
- The failure data in other similar but not identical systems;
- The failure experience with the specific-system being studied.

In such cases, expert judgment, generic information, or surrogate data are used directly or in combination with (limited) system-specific data. In general, various information types can be proposed to be considered and integrated.

If PSA results are to be used for risk-informed applications, the data requirements should be far stricter than in a typical use of PSA results. The measure, based on IRI approach, includes the data reliability measure, which is related to degradation level detection efficiency (i.e. failure inspection reliability) and represents the generic data reliability insights and insights regarding uncertainty of failure events occurrences and classification. Typically, the data and detection reliability (probability of non-detection) insights are not included in the PSA scope and appropriate deterministic analysis of consequence.

2.3. Risk-Informed Assessment and Results Visualization

The risk associated with different systems, components and structures has become subject to re-evaluation when the results of additional information became available. Detailed, systematic, plant specific analyses with an operational experience are thought to give realistic and relevant estimates of used risk measures. Such risk estimates could be considered as useful also for the risk-informed applications, e.g. modification of the inspection and testing strategy. In this section, the general model of risk-informed assessment as well as formulas for risk measure calculation and visualization is presented.

The first task for risk informed (RI) approach application is the determination of the high-risk components or locations. The procedure for risk ranking and decision-making is proposed to be based on division of overall system risk into so called components risks measures. For practical applications, these measures can be calculated as the product of degradation frequency estimate P and estimate C of consequence probability to degrade the overall safety. If there are some degradation states k (e.g. crack with small leak, crack with large leak) up to maximum degradation state D - failure (e.g. pipe rupture) then the total conditional risk due to the component i degradation influence on the main system is proposed to be expressed as such sum:

$$R_i = \sum_{k=1}^{D} n_i \cdot P_{i,k} \cdot C_{i,k}. \tag{2}$$

Each summand reflects the conditional risks due to the component *i* degradation state *k* influence on the main system and they are assumed to be mutually exclusive. In fact, the risk R_i reflects the risk of the single ($n_i=1$) component *i* or the risk of similar components group *i* with n_i components influence to overall risk to degrade the safety of system. As an example, in Nuclear Industry the influence to overall risk can be expressed as Conditional Core Damage Frequency (CCDF), where the overall system risk reflects the total Core Damage Frequency (CDF). The conditional risk due to some subsystem *S* specific degradation states influence on overall system safety is proposed to be expressed as follows:

$$R_S = \sum_{i=1}^{N} R_i = \sum_{i=1}^{N} \sum_{k=1}^{D} n_i \cdot P_{i,k} \cdot C_{i,k}. \tag{3}$$

In practice, the conditional probability to degrade the safety of system (consequence $C_{i,k}$) can be assessed as safety barrier used for CCDF calculation in PSA. As an example, the CCDF for different postulated Loss of Coolant Accident (LOCA) events can be used as such safety barrier. These safety barriers in most cases can be taken from PSA model. The calculation of frequencies (probabilities estimates expressed per time unit), related to the degradation states occurrence, usually needs a separate model which includes the information and assumptions concerning failure detection procedure and its reliability.

Visualization of Risk-informed Measures

The risk-informed measures can be estimated for each state of degradation in similar component (or location) of considered subsystem. In order to simplify the risk interpretation, according to the dominating risk part, like in approaches of other authors [14], [15] only two generalized values C_{Plot} and P_{Plot} (as one point coordinates) for each component are defined (as example, see figure 2).
In case of two degradation states (e.g. leak and rupture):

$$\mathrm{R_i = n_i \cdot P_{i,1} \cdot C_{i,1} + n_i \cdot P_{i,2} \cdot C_{i,2} = P_{i,Plot} \cdot C_{i,Plot}}; \tag{4}$$

$$\mathrm{C_{i,Plot}} = \begin{cases} \mathrm{C_{i,1}\ if\ P_{i,1} \cdot C_{i,1} > P_{i,2} \cdot C_{i,2}} \\ \mathrm{C_{i,2}\ if\ P_{i,1} \cdot C_{i,1} \le P_{i,2} \cdot C_{i,2}} \end{cases}; \ \mathrm{P_{i,Plot}} = \frac{\mathrm{R_i}}{\mathrm{C_{i,Plot}}}. \tag{5}$$

In case of D degradation states:

$$\mathrm{C_{i,Plot}} = \underset{\mathrm{C_{i,k}}}{\arg} \max_{\mathrm{k \in (1,D)}} \mathrm{(P_{i,k} \cdot C_{i,k})};\ \mathrm{P_{i,Plot}} = \frac{\mathrm{R_i}}{\mathrm{C_{i,Plot}}}. \tag{6}$$

The total risk R* coordinates C* and P* are proposed to be expressed as follows:

$$\mathrm{C}^* = \underset{\mathrm{C_{i,Plot}}}{\arg} \max_{\mathrm{i \in (1,N)}} \mathrm{C_{i,Plot}} \text{ and } \mathrm{P}^* = \frac{\mathrm{R}^*}{\mathrm{C}^*}. \tag{7}$$

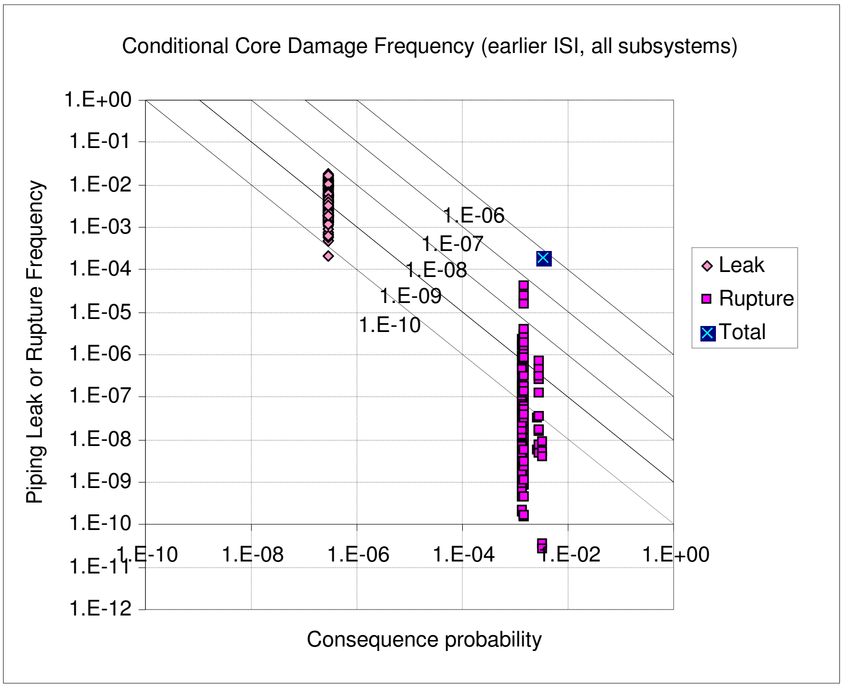


Figure 2. Conditional core damage frequency per weld for various piping.

The presented general model for risk-informed assessment and result visualization is proposed to be used in order to model failure detection (e.g. inspection) and risk reduction process. The presented modelling method is very useful for risk ranking and decision making purpose [17]. In future, it would be interesting to discuss how the results of practical decisions based on such decompositions differ (if at all) from decisions based on various sensitivity and importance measures.

3. Decision Making and Risk Management to Minimize Risk

The content of this section is mainly directed towards the investigations of decision-making framework and how general decision-making and inspection process can be applied for risk reduction. In this section, some aspects, that may be considered when discussing a strategy for risk informed in-service inspection and testing, are presented as well.

General Procedure of Decision-Making. The main steps of proposed decision-making procedure (see the following figure) are:

- The analysis of issue and the available data sources;
- The quantitative modelling of considered details;
- The simulation and ranking of alternatives;
- The quantitative selection from alternatives;
- The analysis of decision and final case.

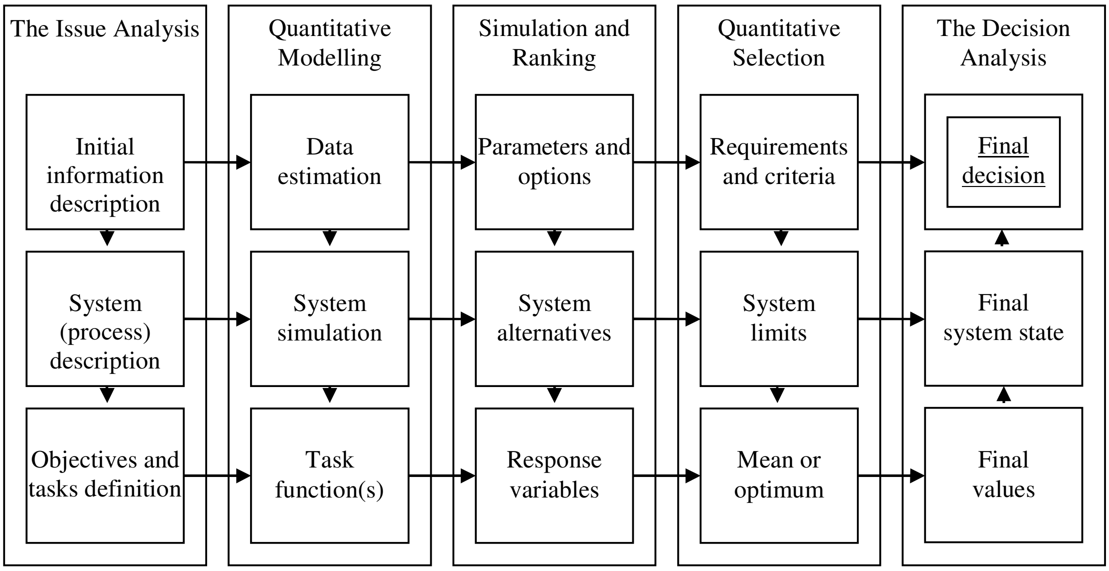


Figure 3. Decision making procedure.

Considering risk reduction procedure, it can also be treated as general inspection and testing procedure with specific parameters and objective to minimize total risk. The following separate actions of general inspection (including testing) procedure are proposed: Objects selection, Targets specification, Tools qualification, Physical process, Results evaluation, and Experience feedback. Governed by scope, objectives and strategy of inspection and testing, the proposed general inspection procedure can be regarded as a closed loop (see the following figure).

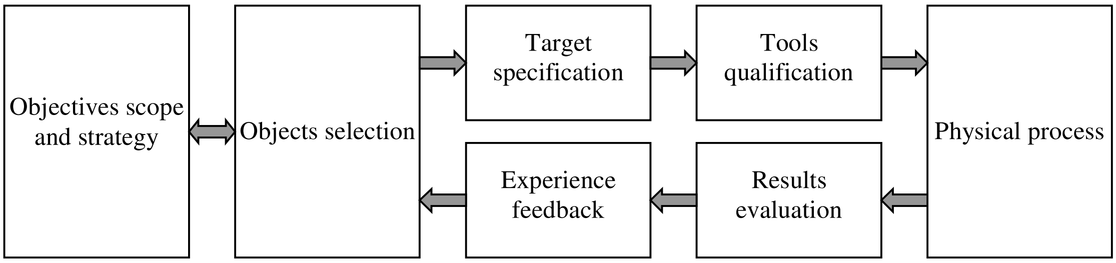


Figure 4. Elements of a general inspection procedure.

In order to perform a selection of objects (structures, systems and components) for the risk-informed ISI/IST programme and to optimise the testing and inspection frequencies, a more detailed procedure needs to be implemented for such applications. So, the scope of general inspection procedure was considered in order to investigate the possibilities of using the plant specific PSA analyses, minimise the risk and effectively allocate resources for in-service inspection and in-service testing. Therefore, according to the general decision-making and inspection procedure, the general inspection analysis and risk reduction procedure is proposed and presented in the following figure.

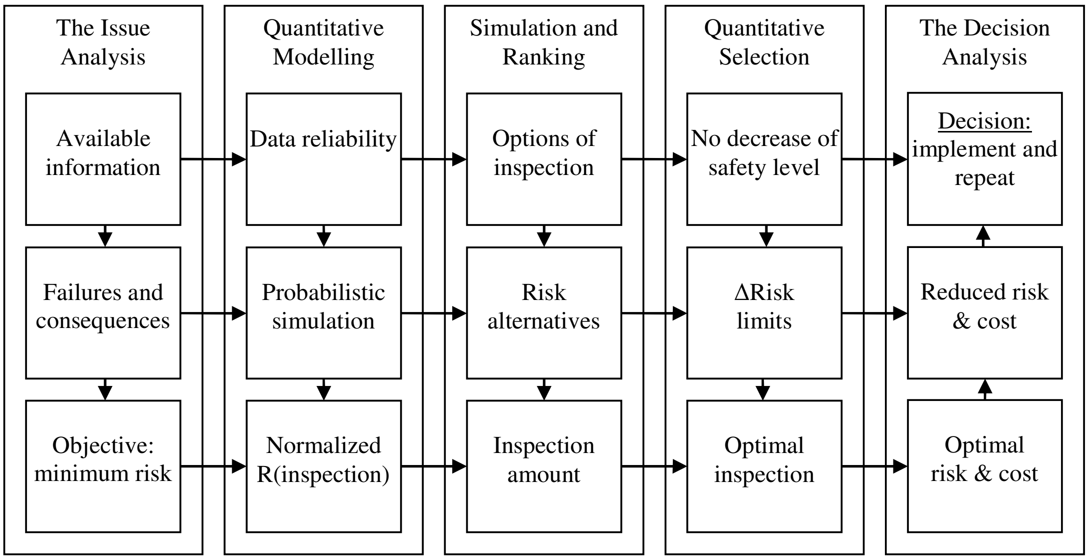


Figure 5. Inspection analysis and risk reduction procedure.

When making decisions under uncertainty it is reasonable to use all parameters and related available information, old and/or new, objective or subjective. This is especially true when the consequences of the decisions can have a significant impact, financial or otherwise. If directly applicable data for a specific parameter is sufficiently plentiful, it may be practical to derive an uncertainty distribution from the data using classical statistical approaches.

However, in many cases, a useful assessment of uncertainty cannot be obtained solely from existing performance data, which may be in doubt e.g. if obtained under different operating conditions. In these cases, it is necessary to do the best that one can, integrating such information into a state-of-knowledge probability distribution for the parameter in question. An important basis for information integration in such cases is Bayes' theorem.

In developing the approach of risk-informed decision-making, which takes into account the uncertainties, various decisions have to be made. Firstly, it has to be decided how the numerical results are to be compared with any acceptance guidelines. Furthermore, recognizing that not whole uncertainties are represented in the probability distribution, a decision has to be made on how to handle these issues. The proposed decision is to allow a variety of models and assumption, but require alternates to be considered, e.g. by performing sensitivity analyses to determine whether the decision will change if alternates are used. The decision would then be made by assessing the relative changes of those alternatives' impact on the task function(s).

There is a general agreement that there are substantial uncertainties in any risk measure. Therefore, for most applications, it is left as a general expectation that a decision maker will give less credit to risk values with a larger uncertainty.

4. Risk-informed in-service inspection

Traditionally, the inspection and maintenance strategy is deterministically based on the intuitive or quasi-quantitative assessment of safety. The PSA is proposed to be used to support new inspection program and reduce the risk, taking into account the relative risk significance of the components or locations. Once the new ISI program has been defined, the PSA can help to demonstrate that the effect on the overall risk due to program changes can be acceptable.

The main objectives of ISI program, based on the IRI approach, is related to the estimation of the likelihood of severe damage (e.g. core damage) and consequences (e.g. large release of radio nuclides) and application of this information in order to select most risky components and locations for ISI and maintenance. In addition, in such program the following problems presented in the following figure should be solved.

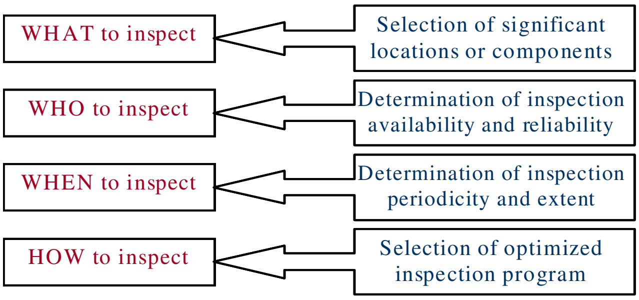

WHAT to inspect
Selection of significant locations or components
WHO to inspect
Determination of inspection availability and reliability
WHEN to inspect
Determination of inspection periodicity and extent
HOW to inspect
Selection of optimized inspection program

Fig. 6. ISI problems and solutions supported by IRI approach.

Using the integrated risk-informed approach, it is possible to estimate and compare the existing ISI program with set of new possible programs and according to the safety and acceptability requirements and optimization criteria, to suggest the ISI program improvements.

The steps for risk-informed inspection program development were summarised in the following list of tasks:

- Analyse the system and components degradation and failure mechanism;
- Estimate data reliability and the probabilities of degradation and failure P;
- Assess the conditional probabilities of the worst consequence C;
- Using probabilities P and C formulate risk measure R;
- Perform the calculated risk ranking for each part of system;
- Considering the parts with highest risks define a new inspection program;
- Estimate the total risk changes (e.g. risk in new case - risk in previous case);
- Estimate costs and positive effects due to the new inspection program;
- According to the results, make recommendations concerning further inspection.

Moreover, the ISI, based on RI approach, should be considered as a living program. Therefore, as part of its implementation process, performance monitoring, periodic update and corrective action program need to be established. Data reliability, probabilistic analysis of degradation and failure occurrence as well as risk measures formulation and estimation.

In general, ISI programs are intended to address all dynamic systems that are subjected to degradation. The incorporation of risk insights in the programs can help inspections to focus on the more important locations. The ISI, based on IRI approach, broadly consists of ranking the elements for inspection according to their risk significance and developing the inspections strategy (frequency, method, size limits, etc.) corresponding to their risk significance. It provides a framework for allocating inspection resources in cost effective manner and helps to focus the inspection activities where they are most needed.

Summary and conclusions

During recent years, both the nuclear and non-nuclear industry and regulatory bodies have recognized that PSA as Probabilistic Safety Assessment has evolved to the point that it can be used increasingly as a tool in decision making and particularly in risk informed inspection. From the IRIDM as Integrated Risk Informed Decision Making and PSA point of view, it is possible to mention that PSA methods are flexible enough to provide the decision maker with almost all technical values which he might ask for risk minimization.

This covers information about the plant (e.g. frequency of various plant damage states), environmental data (e.g. frequency of different source terms) and health effects (e.g. frequency of radiation exposure to the public). It is nevertheless prudent that decision makers are aware of the strengths and weaknesses of PSA and seek support of PSA experts, especially to discuss whether the PSA status is consistent with its application to support decision-making.

Typical ISI can be routinely carried out by the utilities in order to detect and characterise possible material degradation in a timely way. It is clear that by performing ISI, utilities are acting effectively in order to reduce the likelihood of failure of these components. Furthermore, it is clear that the selection of systems and components with consideration for their consequences of failure has a direct bearing on the effectiveness of ISI, in terms of their contribution to overall plant safety.

The application of ISI is entirely consistent mainly with the deterministically based philosophy of defence in depth. However, ISI programmes carried out to current requirements essentially reflect qualitative engineering judgements. This means that without the benefit of quantitatively based risk-informed insights, a disproportionate effort may be expended on the inspection of certain items that do not contribute significantly to the overall plant risk. Equally, there is a possibility that certain risk significant items may not be covered in the inspection programme.

The benefit of the risk-informed approach to ISI is that it increases existing engineering judgement and experience in a way that helps to refocus ISI according to the assessed contribution.

The use of risk assessment in the optimization of the ISI helps to focus limited resources. In addition, one of the outcomes of the optimization may be a reduction in operational and maintenance costs while maintaining a high level of safety.

References

[1] IAEA TECDOC-1436, Risk informed regulation of nuclear facilities: Overview of the current status, IAEA (2005).

[2] IAEA INSAG-25, A Framework for an Integrated Risk Informed Decision Making Process, IAEA (2011).

[3] ASAMPSA_E, Recommendations on Extended PSA and its Use in Decision Making, Technical report ASAMPSA_E/WP30/D30.6/2016-28 IRSN PSN/RES/SAG/2016-0234 (www.asampsa.eu, submitted to a peer review).

[4] ASAMPSA_E, Risk Metrics and Measures for an Extended PSA, Technical report ASAMPSA_E / WP30 / D30.5 / 2016-17, IRSN PSN/RES/SAG/2016-00171 (www.asampsa.eu, submitted to a peer review).

[5] T. AVEN and B.S. KROHN, "A New Perspective on How to Understand, Asses and Manage Risk and the Unforeseen", *Reliability Engineering and System Safety*, Vol. 121 (2014), p. 1-10.

[6] L. A COX, "Does Concern-Driven Risk Management Provide a Viable Alternative to QRA?", *Risk Analysis*, Vol. 27, Issue 1 (2007), p. 27-43.

[7] B. GRECHUK and M. ZABARANKIN, "Risk Averse Decision Making under Catastrophic Risk", *European Journal of Operational Research*, Vol. 239 (2014), p. 166-176.

[8] NASA, *Risk Management Handbook*, Version 1.0, NASAA/SP-2011-3422 (2011).

[9] U.S. NRC, White Paper on Risk-informed and Performance-based Regulation, SECY-98-144 (1999).

[10] S.M.E. WINT, "An Overview of Risk", *RSA Risk Commission*, ca. (2006).

[11] T. AVEN, "On the Ethical Justification for the Use of Risk Acceptance Criteria", *Risk Analysis*, Vol. 27, Issue 2 (2007), p. 303-312.

[12] D. N. D. HARTFORD, "Legal Framework Considerations in the Development of Risk Acceptance Criteria", *Structural Safety*, Vol. 31 (2009), p. 118-123.

[13] G. ERSDAL and T. AVEN, "Risk Informed Decision-making and its Ethical Basis", *Reliability Engineering and System Safety*, Vol. 93 (2008), p. 197-205.

[14] F.R. FARMER, "Reactor safety and siting: a proposed risk criterion", *Nuclear Safety*, 8, 539–548, 1967.

[15] U.S. NRC NUREG-1860, Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing, U.S. NRC (2007).

[16] U.S. NRC RG 1.178, An Approach for Plant-Specific Risk-Informed Decision-making for In-service Inspection of Piping, RG 1.178 Rev. 1, U.S. NRC (2003).

[17] A. KLIMAŠAUSKAS, R. ALZBUTAS, V. KOPUSTINSKAS, J. AUGUTIS, E. UŠPURAS, Updating of risk-informed ISI programme for Ignalina RBMK-1500 nuclear power plant in Lithuania: results and challenges, *Nuclear engineering and design*. ISSN 0029-5493. Vol. 236, Iss. 24 (2006) p. 2547-2555.

The Importance of Safety Assessment, Reliability and Maintenance for Critical Infrastructures

Luís Andrade Ferreira
University of Porto – Faculty of Engineering
DEMec, Rua Dr. Robero Frias
4200-465 Porto, Portugal

Abstract

Critical Infrastructures (CI's) are essential to maintain our way of life, based on secure, safe and dependable equipment, in essential areas as they are Energy Production and Distribution and Transportation. Today most of the attention and action on CI's is focused security, because of last terrorist events. But if we look to the past accidents with important repercussions they happened because of misuse or lack of maintenance.

In this paper we present a case where the lack of monitoring of a road bridge lead to an accident with 59people dead in March, 2001. The consequences of this accident were the imposition of a national policy of risk safety assessment of all bridges, especially in situations of changes in the use of bridges, with an increase of unexpected stresses arriving on to them.

Keywords: Critical Infrastructures, Railways Bridges, Risk Assessment.

1. Introduction

In today's developed societies we are more and more dependent on technological equipment on our daily lives and to deliver services or goods. But there are infrastructures that are vital for our quality of life. Those infrastructures are considered critical and they must be dependable, meaning that all of us expect that those services or goods are available and can be provided in a safe way and without any interruption, enabling economic and social sustainability.

In Europe, the 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, defines on its Article 2 that 'critical infrastructure' (CI) means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions [1].

In the same directive, on its Annex I, the sectors of European critical Infrastructures are listed and they are two: Energy (electricity, oil and gas) and Transport (road, rail, air, inland waterways ocean and short-sea shipping and ports).

In the USA the Department of Homeland Security considered that there are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof [Retrieved from: https://www.dhs.gov/critical-infrastructure-sectors].

The CI sectors that were considered in the US are : Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defence Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems and Water and Wastewater Systems [2].

Even if the definitions of the CI in the EU and in the USA are not exactly the same, they are very similar and they are mostly directed to the security concerns caused by malicious activities at the different levels of these systems, cyber or physical.

Also the resilience of these systems under a possible attack has been studied and as a result CI's are more resilient today than they were in the beginning of this century.
These concerns about terrorist attacks to CI's are understandable in face of the last events, and the results can be considered to be quite good till now, as the terrorist attacks have had little or no impact on the CI's availability.

But there are other concerns about CI's that must not be overlooked. A look into past and relatively recent disasters involving CI's shows that the different government agencies around the world have not considered as they were expected to do the effects of poor reliability in the design and most of all on the operation and on the poor maintenance of CI's.

Most of the Critical Infrastructures are by their nature complex systems or networks of systems with many interdependencies that are designed to operate in an optimal way, providing the functions for which they were designed in a reliable and safe manner.

These CI's are designed to function for long periods of time (most of the times for decades). So, they have to be maintained, adapted to new legislative demands for safety and the environment, to adapt to new capacity demands and to the introduction of new control technologies. Many times, due to the lack of financial resources their expected lives are extended well beyond the one foreseen in the original requirements for design.

Also, in many sectors different countries have promoted deep reorganizations of their public sectors, because of financial restrains. Some public institutions became completely or partially privatized, others were outsourced to private organizations and many new projects pf CI's are private or Public-Private Partnerships.

These contracts with private organizations are usually made for a certain number of years. Also, sometimes they imply the deregulation of the systems, what is relatively new in Europe in certain areas like energy or railways.

So, many concerns are arising about the vulnerability of these complex systems, because one must be sure they are able to support the new capacity demands that imply bigger stresses to the equipment or if they age in a reliable and safe way. And the fact that new and inexperienced managers entered in these new "markets" can involve increased risks due to the lack of experience in running such infrastructures. All these factors trying to promote more efficient and less costing services can cause greater vulnerabilities that are multifaceted in nature [3].

2. Bridges in Portugal as an example

From what we have come to realize over time, the countries of Europe and other developed countries have the skills and competences that are necessary to respond to the threats that are being put to Critical Infrastructures.

However, if we take a look to past and relatively recent accidents involving CI's one can conclude that the concerned authorities were very attentive towards preventing terrorist attacks, but paid little attention to misuse (usually overstress) and above all to poor maintenance. This may be the consequences of possible political gains through terrorism prevention that does not exist when the budgets on operation and maintenance are discussed.

In Portugal, in the 90s of the 20th century, a policy of deregulation of the basic sectors of the economy was implemented, with the partial privatization of these or with the introduction of "commercial" models for the management of public infrastructures.

In the case of bridges, with the exception of large bridges, its management and maintenance was decentralized at that time and it was delivered to regional entities. These entities had little preparation and lack experience in the maintenance of this type of equipment.

As a consequence of this, a decrease in the maintenance capacity was noticed immediately, especially in infrastructures that demanded a greater technological knowledge, as it is the case of the bridges. The most complicated situations occurred in old bridges and those whose pillars are flooded every year.

The worst consequence of this policy occurred on March 4, 2001, and which consisted of the collapse of the Hintze Ribeiro Bridge, inaugurated in 1887, and which made the connection between Castelo de Paiva and the town of Entre-os-Rios, over the Douro River in the north of Portugal.

From this accident resulted in the death of 59 people, including the passengers of a bus and three cars that tried to reach the other margin of the river Douro.

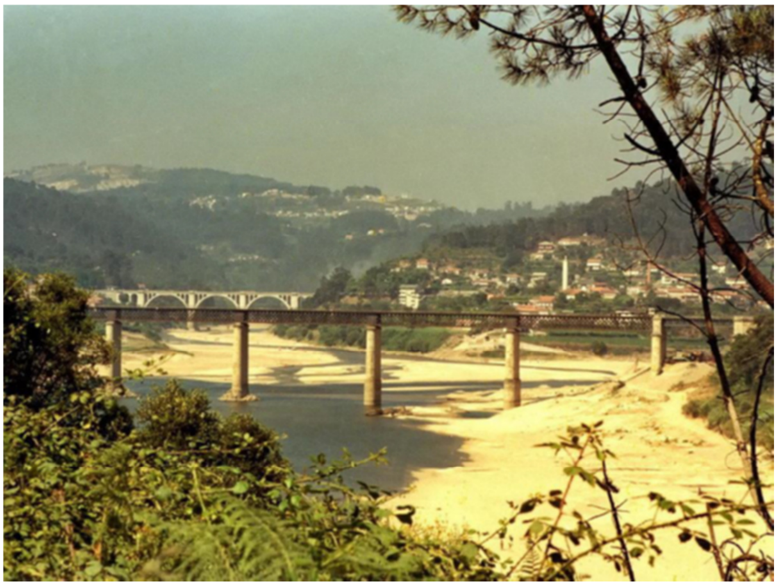


Figure 1. The bridge “Hintze Ribeiro” in Entre-os-Rios, Portugal (1997).

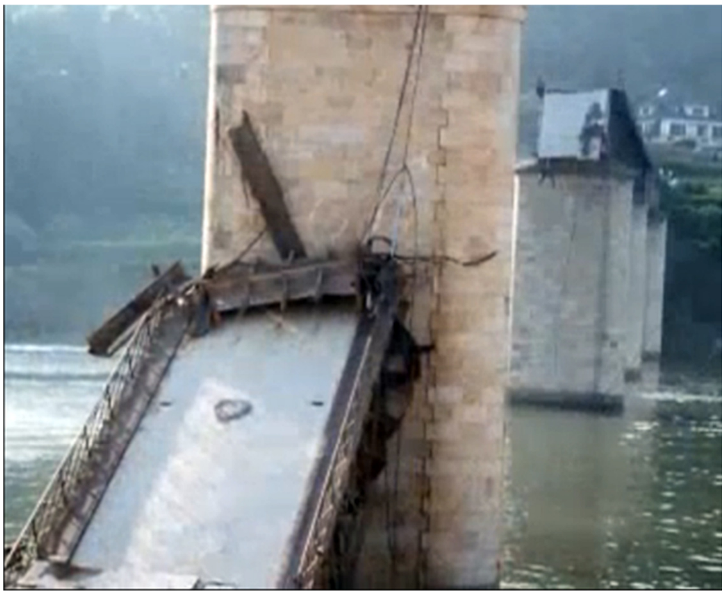


Figure 2. The bridge “Hintze Ribeiro” the day after it collapsed.

A parliamentary commission of inquiry concluded at that time that the cause of the fall of the bridge was "the descent of the river bed in the fourth pillar zone", related to the "inert extraction activities of the river bed".

This descent of the pillar caused the loss of support from the ground beneath the foundation coffin (by erosion and reduced load resistance) that caused the collapse of the pillar abutment. Also, it was noticed a “lack of proper monitoring of the infrastructure functional conditions”.

At that time and with the exception of large national bridges, such as the 25 de Abril Bridge in Lisbon and most of the railway crossings, inspected by the National Railway Network (Refer), there was no entity in Portugal that monitored and maintained the structures of the bridges. The service responsible for the inspection and maintenance of the bridges existed in fact, but was eventually dissolved two years before when the Government decided to extinguish it and transferred the responsibility to local entities.

From that accident, it was concluded that was indispensable to have a national inspection plan because there were reasons to believe that other bridges in the country could be in a situation similar to that of the bridge that collapsed. A bridge inspection initiative was created and two years later a report was produced mentioning that at least about 200 structures needed maintenance work.

3. Safety Assessment for Critical Infrastructures: a case example for railways bridges

At that moment, it was imposed a policy of safety culture for the operation, monitoring and maintenance of the Portuguese bridges. In particular, if there were expected new and higher stresses on the use of the bridges a safety assessment should be performed and a monitoring and maintenance plane should be approved by a new national safety board.

In particular, for railways bridges that were expected to support the stresses imposed by new heavier and faster trains (the “Pendolino”) the safety assessment should be made before the trains could travel at the high expected speeds.

The dynamic behaviour of railway bridges has become an issue of main concern between scientists and engineers over the last 20 years, due to the extensive construction of new high-speed lines and also the use of old lines for higher speeds. Fast trains can induce resonance situations in railway bridges, being the short-to-medium-span bridges where the main structural elements are simply supported (S-S), the most critical in this regard.

When the train travels at a resonant speed, high levels of the deck vertical acceleration are to be expected, which can result in adverse consequences such as ballast deconsolidation, passenger discomfort or higher risk of derailment.

The present case study is the Canelas Bridge, located in the Northern line of the Portuguese railway. The bridge has six simply supported spans of 12 m each, resulting in a total length of 72 m. The bridge deck is a composite structure consisting of two half concrete slab decks with nine embedded rolled steel profiles HEB 500. This kind of structural system is called filler beam and is a very common structural solution for small span bridges in the European high-speed railway lines. A general view of the bridge used as case study is shown in Fig. 4, as well as the typical cross section of the bridge deck.

The structural system of the bridge consists of simply supported beams. However, the rail is continuous and this continuity affects the dynamic response of the bridge. This is included in the numerical model that was applied to simulate the bridge behaviour by extending the rail 10.5 m in both directions over the length of the bridge.

Experimental campaigns on the bridge were performed in order to confirm the simulation model and that allowed knowing that all the spans have similar dynamic response and for this reason there was no need to include all the spans in the finite element model, which allowed for the consideration of a lighter numerical model. A schematic view of the bridge model used can be seen in Fig. 3.

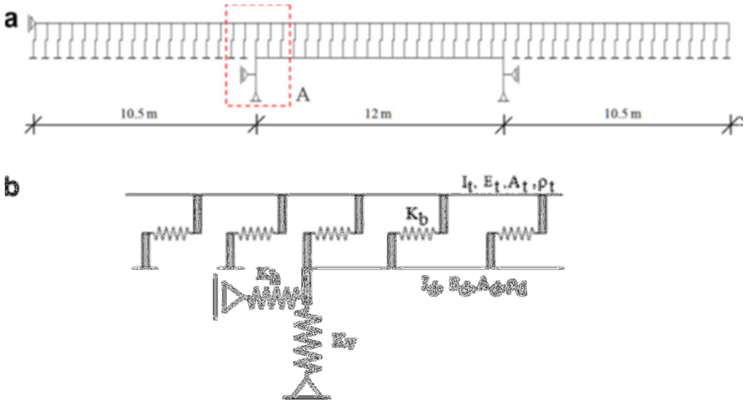


Figure 3. Bridge model

To perform the experimental work, it was designed and developed a set up that allowed to monitor the bridge during its normal operation.

There is a great amount of characteristics that the designer of the Structural Health Monitoring System must have into account when choosing the data acquisition system for a certain application. However it is possible to name a few factors that should always be matter of study:

- Resolution usually referred to the number of bit of the analogue-to-digital converter;
- Sampling frequency;
- Processing power;
- Embedded communication module, important to transmit data to a remote post;
- Power consumption;
- Cost.

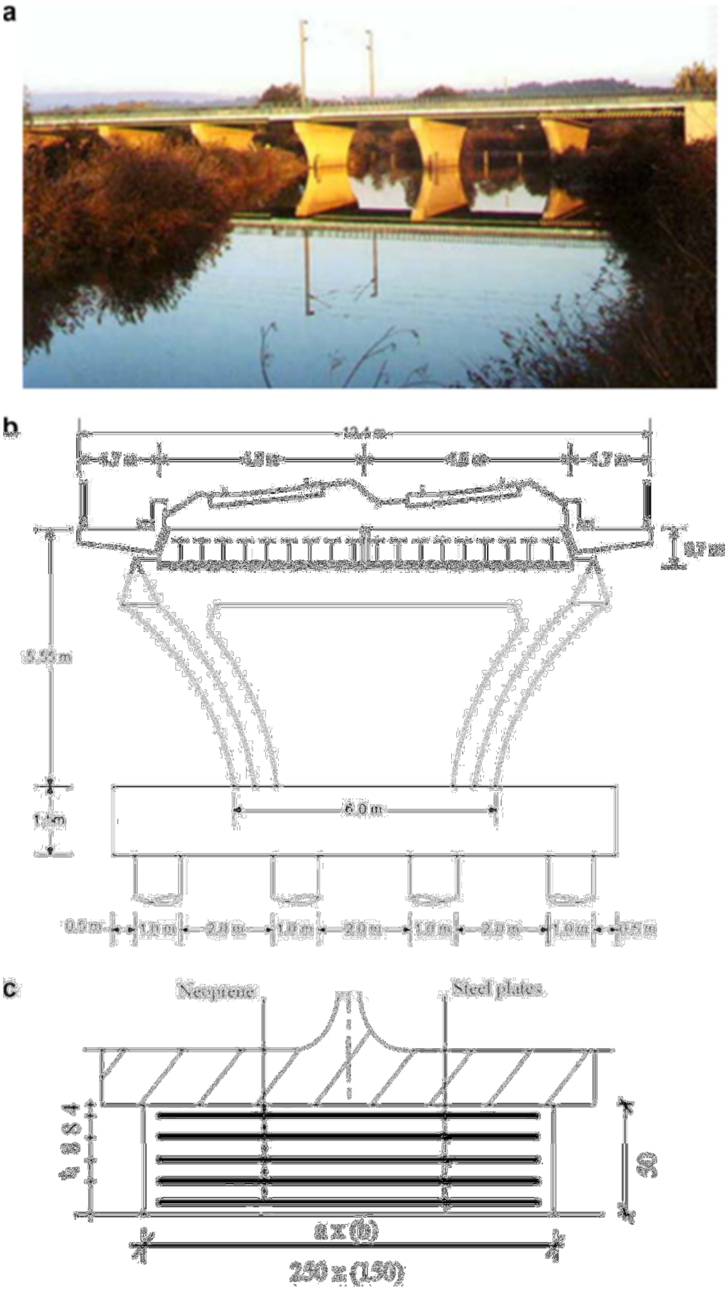


Figure 4. Canelas Bridge: (a) general view; (b) typical cross section of the bridge; (c) detail of the bearing.

Another big issue when deploying sensors in a structure is the place where they are located. Even high quality sensors cannot produce useful data if placed in the wrong places. There is a need to study the structure and realize its key points in order to find where it is worth to put these transducers.

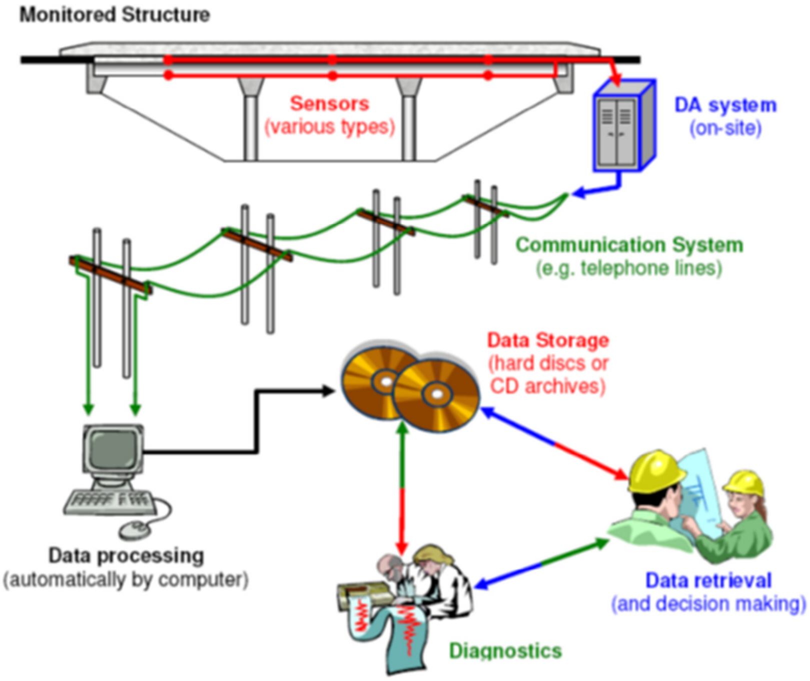


Figure 5. Composition of a Structural Health Monitoring System for a railway bridge

The measures that were performed on the vertical acceleration of the ballast and on the structure of the bridge made possible to validate the results obtained by simulation for higher speeds [3].

The applied methodology for the simulation and the selected variables, their simulation identification number as well as their corresponding distribution and variability were pre-defined and can be seen in [4]. Four distinct response parameters were analysed in the screening procedure: natural frequencies, displacements, accelerations and reactions.

In order to establish speed limits for high-speed trains that might pass on the bridge, a safety assessment of Canelas Bridge was performed based on the obtained results for the different simulation scenarios. This analysis was based on the acceleration values recorded at mid-span of the bridge, which proved to be the most restrictive aspect of the response. In this work the acceleration limit was considered to be 7 m/s2, which is the value that some laboratory tests confirmed to be the limit for the beginning of the ballast instability.

After analysing the results from the safety assessment some conclusions can be drawn. First of all, the estimated speed limit obtained was 295 km/h. This limit was obtained considering the typical values used in ultimate limit states, using probability values up to 10 4. It could also be observed that if a more conservative approach was used, and this probability was lowered to values up to 10 5, no significant difference would be obtained, decreasing the speed limit to 290 km/h.

So, it was defined that the speed limit for trains passing over the Canelas Bridge would be 290 km/h.

4. Conclusions

Nowadays it is expected that Infrastructures that are considered Critical to our way of life cannot fail and should always to be available to provide goods and services.

A lot of attention has been given to the security of these Critical Infrastructures. That can be explained easily by the last dramatic events in different parts of the globe.

But if we take a look to the most important accidents and incidents in Critical Infrastructures, most of them have happened not because they have been under terrorist attack, but because there was a lack of a safety assessment to new operational stresses under higher demands or because there was not in place an efficient monitoring system for the health condition and a proper maintenance.

In Portugal, after the collapse of the Hintze Ribeiro Bridge in March 2001, a safety assessment is obligatory for bridges, if they are submitted to higher stresses to understand their behaviour. For that purposed a methodology was developed that allowed to state the safe conditions for the bridge operation. A case study was presented.

References

[1] Official Journal of the European Union, L345/75

[2] Presidential Policy Directive/PPD-21 - Critical Infrastructure Security and Resilience, February 12, 2013

[3] IRGC. White paper on managing and reducing social vulnerabilities from coupled critical infrastructures, Geneva, 2006.

[4] Ferreira, J. M., “Civionics - An Interdisciplinary and Emerging Area”, Master Thesis, Electrical and Computers Engineering, FEUP, 2011

[5] Rocha, J.M., Henriques, A.A., Calçada, R., Safety assessment of a short span railway bridge for high speed traffic using simulation techniques, Engineering Structures 40 (2012) 141–154, doi:10.1016/j.engstruct.2012.02.024

Exploring public expectations for aid from critical infrastructure operators

Laura Petersen
Laure Fallou
European-Mediterranean Seismological Centre (EMSC)
c/o CEA, Bât. BARD, Centre DAM - Ile de France
91297, Arpajon, France

Paul Reilly
Elisa Serafinelli
University of Sheffield
211 Portobello Rd
S1 4DP, Sheffield, UK

Abstract

While the importance of transportation infrastructure in emergency management is recognized, the role of critical infrastructure (CI) operators has yet to be fully established, especially when it comes to providing aid to the public. This paper addresses this under-researched issue by drawing on key themes that emerged from a review of the literature on public expectations of transportation CI operators in disaster management and presenting the results of an online questionnaire-based study of disaster-vulnerable communities. Results indicate that members of the public expect CI operators to contribute to emergency response, to provide a means of evacuation, and to aid in long term recovery. The paper concludes with recommendations for how CI operators can meet these expectations.

Keywords: public expectations, emergency management, critical infrastructure operators, evacuation

1. Introduction

The coordination and active participation among the different actors involved in emergency management (EM) is often cited as a prerequisite for effective emergency management. While the importance of transportation infrastructure[1] in emergency management is recognized [2], less often examined is the role that critical

[1] Transportation networks provide mobility to the public through the use of private vehicles and public transport as well as provide the transportation of goods via roads, railways, waterways, airways, and transport lines [1].

infrastructure[2] (CI) operators[3] should play. While an "expectation gap" between what services the public expect CI operators to provide after a disaster and what CI operators are realistically able to deliver is a recurring theme in the literature [4], [5], few studies have empirically investigated what members of the public expect in relation to aid provided by CI operators during and after disasters. This paper sets out to add to the existing research in this area by examining public expectations for CI operators to provide aid during and after a disaster. This paper addresses these under-researched issues by drawing on key themes that emerged from a review of the literature on public expectations of transportation CI operators in disaster management and presenting the results of an online questionnaire-based study of disaster-vulnerable communities in France, Norway, Portugal and Sweden. It concludes by proposing recommendations for how CI operators can meet public expectations regarding aid.

2. Transportation in disaster management

Transportation infrastructure is a necessary component for emergency response activities such as transporting people to hospitals, evacuating people to safe zones, or bringing people essential goods such as food and water. The importance of restoring transportation networks in the aftermath of disasters was demonstrated during the 2011 Great East Japan Earthquake where the rapid reopening of the transportation network allowed authorities to reach and help the victims [2]. Transportation also plays a key role in the recovery of other critical infrastructures and damage to transportation infrastructure is often linked to cascading effects, whereby disruption spreads from one system to another. The repair of damage to transportation assets is considered a prerequisite for key agencies charged with rescuing stranded residents, restoring power, and beginning recovery [3]. For these reasons, during times of crisis society benefits greatly from resilient transportation networks. Indeed, expectations for transportation infrastructure during and after a disaster are high. There is an expectation that a minimum level of mobility can be achieved, even if that requires a change in means of getting around (using public transit instead of a private vehicle, bicycling instead of taking the subway, etc.), as was the case during the 2012 Hurricane Sandy when NYC subway users walked, biked or carpooled to maintain mobility [7]. Furthermore, after the 2011 Great East Japan Earthquake and the 2010-11 Queensland Floods residents who had lost access to their private vehicles expected there to be an offer of public transportation available [2], [8].

[2] The European Union defines CI as "an asset, system or part thereof that are essential for the health, safety, security, economic or social well-being of people, and its disruption or destruction would likely have a significant impact upon the ability of a Member State to maintain those functions [1]."

[3] CI operators are the actors who are in charge of the critical infrastructure. For example, the Oslo Port Authority for the Oslo Harbour or SANEF, a French motorway operator, for the A4 highway.

2.1 Evacuation

Evacuation is sometimes a necessary part of disaster response. Either the public decides for themselves to evacuate (either due to official warnings or not), or they are forced to evacuate by the authorities. In order for people to evacuate by themselves they need to be provided information (usually from multiple sources), understand the information (including that it is meant for them), confirm the information, be able to act on the information and then engage in the recommended actions [9]. Once the decision to evacuate has been taken, people expect to be able to evacuate safely and in a timely manner [9], [10]. People require transportation infrastructure to carry out evacuation actions. Most people expect to evacuate using their own private vehicles, as was the case during the 2011 Great East Japan Earthquake and Tsunami [11] and Hurricane Rita in Texas [12]. However, not all persons have access to a private vehicle and some people may simply prefer to use public transport instead. As such, there is an expectation to be able to evacuate even without the use of a private vehicle, especially since the resources required, such as buses, already exist in most cases [13].

3. Methodology

3.1 Research Questions

Three research questions emerged from the literature reviewed above:

1) Do citizens expect CI operators to provide aid during crisis situations?

2) Are there any noticeable similarities/differences between public expectations based on demographic factors?

3) How can CI operators meet these expectations?

In order to investigate these questions, the EU Horizon 2020 project IMPROVER[4] designed an online questionnaire-based study. Ethics approval was sought and obtained from the respective authorities prior to data being collected. The target population for the questionnaire was adults aged 18 years and over who were familiar with four project Living Labs, or clustered regions of different types of infrastructure which provide specific services to a city or region. These were: Barreiro Municipal Water Network, Oresund Region, Oslo Harbour, and French transportation networks (roadways). To maximise the response rate, the questionnaire was translated into six languages (English, French, Danish, Swedish, Norwegian, and Portuguese) prior to its distribution.

[4] IMPROVER: Improved risk evaluation and implementation of resilience concepts to critical infrastructure. The overall objective of IMPROVER is to improve European critical infrastructure resilience to crises and disasters through the implementation of resilience concepts to real life examples.

It was structured as follows: first, a brief description of the project was provided and participants were informed of their right to withdraw from the project at any time, as well as how all data would be handled during the project. For the purposes of this questionnaire, respondents were presented with the following definition of a disaster: "an event which has catastrophic consequences and significantly affects the quality, quantity, or availability of the service provided by the critical infrastructure." Respondents were also provided a definition of CI operators. Second, both multiple choice and Likert scales were used to measure participants' expectations. Participants were asked three questions regarding expectations of aid. The first asked, "After a damaging disaster, I expect aid from (check all that apply)" and listed the following actors: neighbours, volunteers, first responders, emergency management personnel, firemen, police, critical infrastructure operators, others, and I do not expect aid. The next two questions used a Likert scale: "During and immediately after a disaster, I expect critical infrastructure operators to provide means of evacuation for the local population e.g. providing free buses to safe areas" and, "Following a disaster, I expect critical infrastructure operators to aid in my long term recovery." The questionnaire also asked about the participants' demographics. Data from the questionnaire was collected between 28 March 2016 and 30 April 2016. The questionnaires were translated back into English at the data entry stage. The questionnaire was disseminated through the project's consortium partners' contacts as well as through the Living Labs.

3.2 Sample characteristics

The sample consisted of 403 respondents. Due to the dissemination method, this self-selected sample was not broadly representative (at least by age, sex, or education level) of the European population, nor those of the geographical locations from which participants were drawn. Sample characteristics showed that 57% of participants were male, 41% female, with 2% choosing not to answer that question. Most were highly educated, with 77% reporting that they have a university degree or higher qualification. Both young and old people appeared to be underrepresented in the study. Respondents aged 18-24 accounted for only 8% of the total sample, with 16% identifying themselves as aged 55 years and above. While 26 nationalities responded, 88 percent of the questionnaire sample consisted of French, Norwegian, Portuguese or Swedish respondents. As such, comparisons depending on nationality were carried out only for these four nationalities. Slightly over 40% of respondents have previously experienced a disaster. For those respondents who received aid in the past, none of them declared to have received help from CI operators.

4. Results

4.1 Actors from whom aid is expected

When asked from which actors respondents expect aid after a disaster, actors commonly associated with disaster response were the most chosen (See Figure 1). Over 90% of respondents selected firemen and first responders and over 80% selected police and emergency management personnel. CI operators are the next most chosen, with

73% of respondents expecting them to provide aid. There appears to be slightly lower expectations for volunteers (64%) and neighbours (57%). Only 1% of respondents stated that they do not expect any aid.

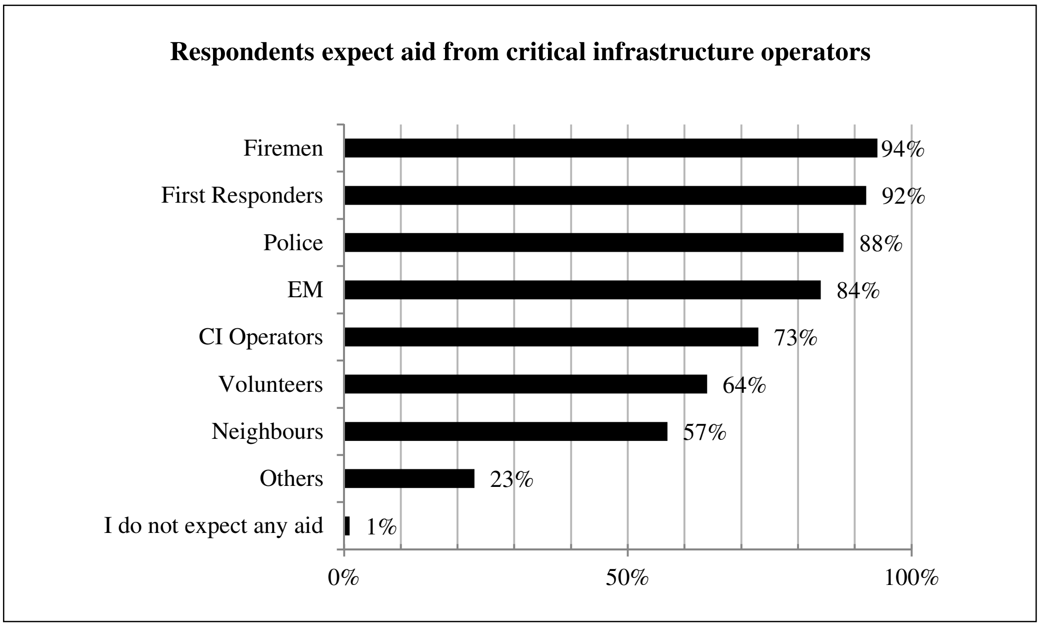


Figure 1: Respondents' expectations for aid after a disaster

4.1.1 Factors affecting expectations

Some demographic factors appear to influence expectations. When it comes to nationality, French respondents appear to be the least likely to expect aid from the police (See Figure 2).

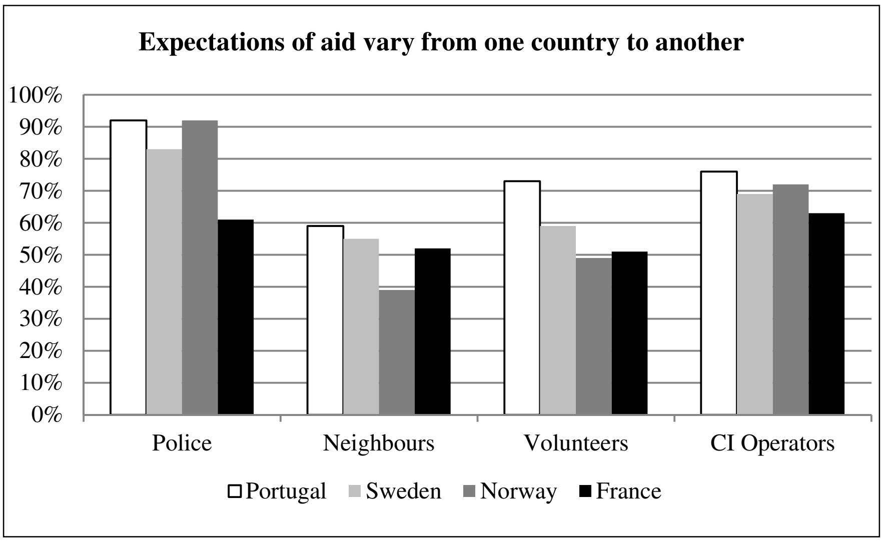


Figure 2: Expectations for aid based on respondents' nationality

Portuguese respondents have very high expectations for volunteers (73%) compared to the other nationalities studied (49% for Norwegian, 51% for French and 59% for Swedish respondents), and Norwegian respondents are the least likely to expect aid from neighbours (39% compared to over 50% for the other nationalities studied). Female respondents have slightly higher expectations of emergency management personnel, volunteers and neighbours than male respondents (with a 12 point, 9 point and 7 point difference, respectively). Lastly, respondents who have experienced a crisis expect more from their neighbours, but those who haven't have higher expectations of volunteers. No differences were found based on age or education level.

4.1.2 Aid from CI operators

While overall CI operators are often chosen for expectations of aid, some demographic factors appear to influence these expectations. A significant difference was found based on education level, with 74% of respondents with higher education choosing CI operators' aid compared to 57% for those respondents with a lower education level. When it comes to differences based on nationality, French respondents are the least likely to expect aid from CI operators (63%), compared to Swedish (69%), Norwegian (72%), and Portuguese (76%) respondents (see Figure 2). Respondents who have had disaster experience are less likely to expect aid from CI operators (68%) than those who have not (75%). No significant differences were found regarding the respondents' gender or age.

4.2 Expectations to aid in evacuation

Overall, the questionnaire found that 96% of respondents agree or strongly agree that CI operators should provide means of evacuation to the local population (see Figure 3).

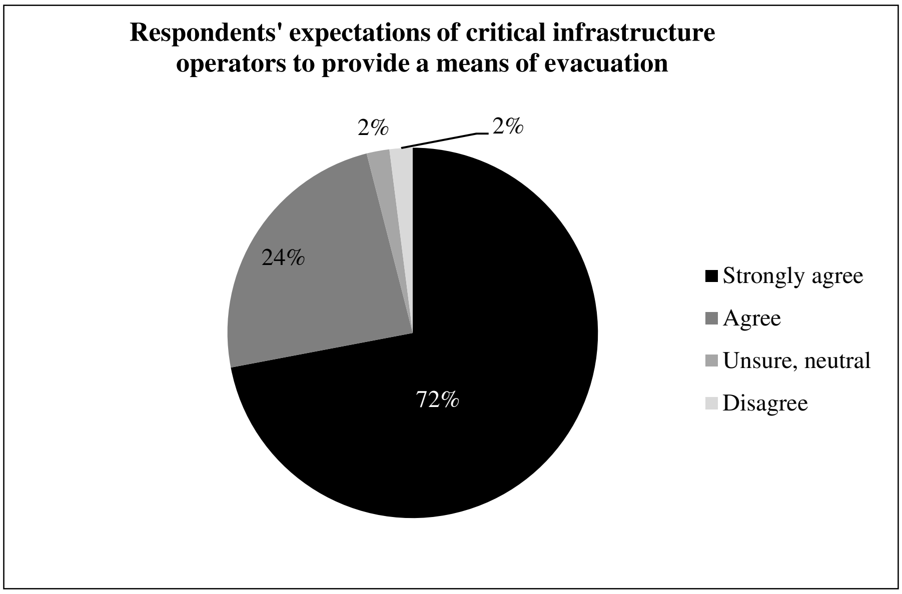


Figure 3: Evacuation expectations

No respondents strongly disagreed with this statement. No significant difference was found among respondents based on sex, age, education level, nationality or previous disaster experience.

4.3 Expectations of aid from CIOs in long term recovery

When asked if they expected CI operators to aid in their long term recovery, 75% agreed or strongly agreed (see Figure 4).

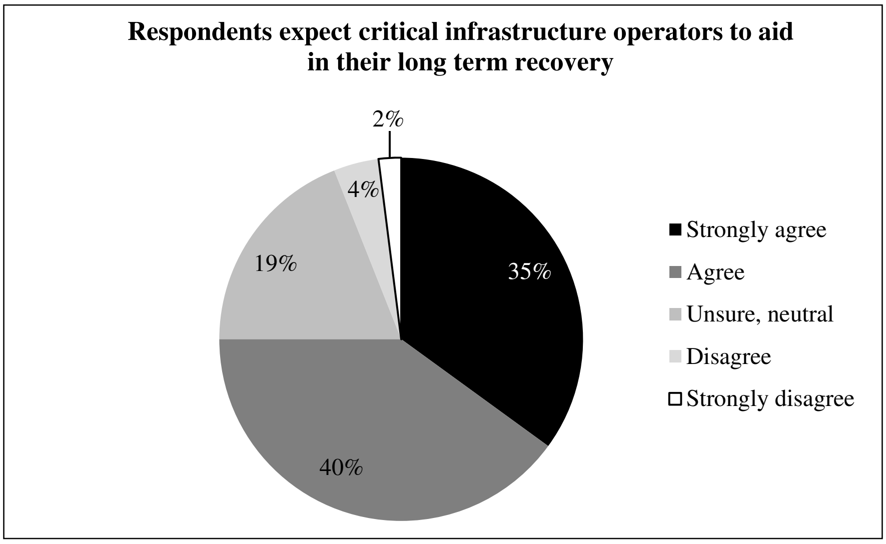


Figure 4: Long term recovery expectations

Portuguese respondents have a much higher expectation that CI operators aid in their long term recovery than the other nationalities studied, with 92% agreeing or strongly agreeing. Norwegian respondents are the least likely to expect CI operators to aid in their long term recovery with 51% agreeing or strongly agreeing and are most likely to disagree or strongly disagree (16% compared to 7% or less for the other nationalities studied). Respondents with previous disaster experience are less likely to expect CI operators to aid in their long term recovery (68%) than those who have no previous experience (78%).

5 Discussion

Overall, expectations for CI operators to partake in emergeny management appear high. While less often chosen than actors typically associated with emergency management such as firefighters or policemen, CI operators were more often selected than volunteers or neighbours. Low expectations of aid from neighbours and volunteers appears in contrast with the literature which acknowledges that neighbours are most often the true first responders in a disaster event and the high expectations for NGOs to provide aid during disasters [14], [15]. Despite the fact that no respondents who have received help in a past disaster received help from CI operators, still 68% expect aid in the future. This could imply that respondents think that CI operators should have helped them in the past, but further research is needed.

When it comes to evacuation, the findings seem to reflect what was found in the literature review, demonstrating that people expect to be able to use transportation assets provided by CI operators in order to evacuate.

Concerning the differences found based on gender and education level, literature is divided on how these factors affect expectations [16]. For gender, this is probably due to the fact that women's civil liberties and role within society may vary from one state to another. Women more than men have been found to use their specific social network in the response and recovery phases [17] and this could explain why female respondents were proportionally more numerous than male respondents to expect aid from neighbours and volunteers. As for education level, a better place to look may be income level, as people with higher education level tend to have higher incomes, and people with lower incomes have been found to have lower expctations of CI operators [18]. However, as socio-economic status was not examined in this study, further research is needed.

The cultural differences found may be due to differences in how crisis management is organised in the different countries and should be studied in more depth. French respondents' low expectations of police may be due to low trust levels. Whereas Nordic countries such as Sweden and Norway have nigh levels of trust in their police [19], French citizens have been found to lack trust in their police [20]. This may help explain the differences in expectation levels and should be researched further. The reason for differences in expectations to receive aid by volunteers is also unclear. Indeed, Portuguese respondents have the highest expectations of volunteers however levels of volunteering have been found to be relatively low in Portugal, compared to medium high in France or very high in Sweden [21]. High expectations of volunteers could then have more to do with trust in civil protection to provide aid during a disaster than tendency to volunteer, however more research is needed. Lastly, literature also confirms our finding that previous disaster experience affects expectations [22], [23].

5.1 Limitations

The limitations of the study should be acknowledged in the interpretation of the results presented above. As discussed earlier, this was a self-selecting sample that was not representative of the demographics in the four respective Living Labs nor the European population. The international aspect of the survey may also cause an inaccurate generalisation of the findings, as social and cultural backgrounds may create different meanings for the Likert scale [24]. Furthermore, people often respond to surveys by providing snap judgments based on available information and may be influenced by emotional or contextual factors [25]. Auestion wording may also influence stated expectations [26]. By asking if the respondent expects something, they may be more likely to say yes. This is furthered by the fact that research has also shown that disaster victims rarely passively wait around for someone else to take care of their needs [27] and having high expectations towards CI operators to act in a disaster may indicate a gap between expectations and the ability of citizens in responding to crisis situations.

6 Recommendations for participation in emergency response by transportation infrastructure operators

Meeting public expectations will help to provide a more thorough emergency response effort. Furthermore, meeting public expectations helps to maintain operators' image during and after crisis times. Here we present a brief look into some recommendations based on the outcomes of this study for how transportation infrastructure operators could help contribute to emergency response.

6.1 Participate in emergency planning

CI operators should be active participants in the elaboration of emergency plans. Risk and vulnerability assessment for each critical infrastructure, as well as coordination, cooperation, and communication between the critical infrastructures and emergency management are crucial to meet public expectations and avoid cascading effects [28]. Studies have shown that a lack of inclusion of CI operators in the disaster planning process has led to evacuation failures [29]. For example, one of the main reasons cited for why the Regional Transit Authority was unable to evacuate the people who need assistance during Hurricane Katrina was that they had not been part of the creation of the local emergency plan [13]. Lastly, disaster planning is often cited as a key component in both social and organisational resilience [16].

6.2 Provide evacuation

Transportation infrastructure operators should provide a means to evacuate free of charge to the public in times of crisis in order to meet public expectations. It is important to keep in mind the capacity of the infrastructure to support evacuation. The unavailability of transportation assets (employees, readiness of equipment) may also hinder evacuation [29]. During both Hurricane Katrina and Hurricane Rita, one of the reasons cited for the failure of buses to evacuate residents is that few of the transit drivers reported into work, with some already having evacuated themselves [29], [30]. Furthermore, it is important to keep in mind road traffic congestion during evacuations, which could vary depending on either the number of people who evacuate or the time of the disaster event. Indeed, during the 2005 Hurricane Rita in Texas and the 2011 Great East Japan Tsunami people evacuating experienced road congestion [13], [29].

6.3 Provide recovery transportation

Both the literature and results indicate that there is an expectation for transportation infrastructure operators to contribute to long term recovery by offering alternative means of transportation to victims. Literature shows that people expect to be able to maintain their mobility even after the loss of private vehicles due to a disaster. As such, it is recommended to have an offer of public transportation available to disaster victims to help them regain a sense of normalcy after the event.

7 Conclusion

After examining public expectations, it appears that CI operators should provide aid during disasters as well as aid in their long term recovery. Transportation infrastructure operators should also contribute to crisis management by providing the public with a means to evacuate. Indeed, even respondents who in the past received help during a disaster, none of whom received help from CI operators, expect CI operators to provide aid in the future. While expectations did vary based on age, gender, education level and nationality, expectations remained high in all cases. It is important to keep in mind that this was a self-selecting sample that was not representative of the demographics in the populations studied.

Based on these findings, recommendations for participation in emergency response by transportation infrastructure operators are to 1) participate in emergency planning 2) provide evacuation and 3) provide recovery transportation.

Acknowledgements

The IMPROVER project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 653390.

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. *Official Journal of the European Union*, 23 December 2008

[2] Nakanishi, h., Black, J. and Matsuo, K. (2014). Disaster resilience in transportation: Japan earthquake and tsunami 2011. *International Journal of Disaster Resilience in the Built Environment*. Vol 5 No. 4, 2014. Pp. 341-361. DOI 10.1108/IJDRBE-12-2012-0039

[3] Matherly, D. and Langdon Neeli. (2014). National Cooperative Highway Research Program (NCHRP) Report 777: A Guide to Regional Transportation Planning for Disasters, Emergencies, and Significant Events. *The National Cooperative Highway Research Program.*

[4] Buller, A. (2015). Closing the Gap: Expectations versus Capabilities. In PA Times.

[5] Iannucci, B. et al. (2013). A Survivable Social Network. In Technologies for Homeland Security (HST), 2013 IEEE International Conference on.

[6] Matherly, D. and Langdon Neeli. (2014). National Cooperative Highway Research Program (NCHRP) Report 777: A Guide to Regional Transportation Planning for Disasters, Emergencies, and Significant Events. *The National Cooperative Highway Research Program.*

[7] Kaufman, S. et al. (2012). Transportation During and After Hurricane Sandy. *Rudin Center for Transportation*.

[8] Regional Australia Institute. (2013). From Recovery to Renewal: Case Study Reports. April, 2013.

[9] Tierney. (2009). Disaster Response: Research Findings and Their Implications for Resilience Measures.

[10] Weathernews Inc. (2011). Great East Japan Disaster: Tsunami Study (Survey Results).

[11] Murakami, H. et al. (2014). Study on casualty and tsunami evacuation behaviour in Ishinomaki city – questionnaire survey for the 2011 Great East Japan Earthquake.

[12] Litman, T. (2006). Lessons From Katrina and Rita: What Major Disasters Can Teach Transportation Planners. *Journal of Transportation Engineering*, Vol. 132, January 2006, pp. 11-18.

[13] Schwartz, M. and Litman, T. (2008). Evacuation Station: The Use of Public Transportation in Emergency Management Planning. *ITE Journal on the web.* pp. 68 – 73. January 2008.

[14] Boris and Eugene Steuerle. (2006). After Katrina: Public Expectations and Charities' Response.

[15] Eikenberry, A., Arroyave, V, and Cooper, T. (2007). Administrative Failure and the International NGO Response to Hurricane Katrina. *Public Administration Review*. Special Issue pp160 – 170. December 2007

[16] Petersen, Laura et al. (2016). Social resilience criteria for critical infrastructures during crises. *IMPROVER project* D4.1.

[17] Fothergill A. (1996). "The neglect of gender in disaster work: An overview of the literature", *International journal of mass emergencies and disasters*, 14(1) 33-56.

[18] Leitch, J. (2012). The need for collaboration in planning efforts during natural disasters: an evaluation of the city of Richmond, Virginia. (Master's thesis, Virginia Commonwealth University)

[19] Tapio Kääriäinen, J. (2007). Trust in the Police in 16 European Countries: A Multilevel Analysis. *European Journal of Criminology*, 4(409), 459–480.

[20] Roche, S., 2008, Performance Management in France: A Police or an Electoral Issue? Policing, Volume 2 (3), pp.331-339.

[21] GHK. (2010). Volunteering in the European Union.

[22] Helsloot, I. and Ruitenberg, A. (2004). Citizen Response to Disasters: a Survey of Literature and Some Practical Implications. *Journal of Contingencies and Crisis Management.* Volume 12, Number 3. (2004) p.98 – 111.

[23] Hasegawa, R. (2013). Disaster Evacuation from Japan's 2011 Tsunami Disaster and the Fukushima Nuclear Accident. *IDDRI.*

[24] Boulan H., (2015) Le questionnaire d'enquête: Les clés d'une étude marketing ou d'opinion réussi, *Dunot*, Paris.

[25] Schwarz, N., & Strack, F., (1999). Reports of subjective well-being: Judgemental processes and their methodological implications. in: Jones, L. and Tanner, T. (2015) "Measuring 'subjective resilience' using people's perceptions to quantify house-hold resilience. Working paper 423." *Overseas Development Institute,* London.

[26] Herrmann R. and Al. (1994). Words matter. *California Agriculture*, Vol. 58, Number 2.

[27] Quarantelli E.L. (1998). Major criteria for judging disaster planning and managing and their applicability in developing societies. *International Seminar on the Quality of Life and Environmental Risks* held in Rio di Janeiro, Brazil.

[28] Leavitt W., Kiefer J., (2006). Infrastructure Interdependency and the Creation of a Normal Disaster. The Case of Hurricane Katrina and the City of New Orleans. *Public Works Management Policy* April 2006 vol. 10 no. 4 306-314

[29] Transportation Research Board of the National Academies. (2014). The Role of Transit in Emergency Evacuation. Special Report 2014.

[30] Eskovitz, J. (2006). Evacuation Planning in Texas: Before and After Hurricane Rita. *House Research Organization Texas House Representatives Interm News.* N°79-2 pp. 1- 5. 14 February 2006.

Risk Assessment for Critical Infrastructure

Inga Žutautaitė, Linas Martišauskas
Lithuanian Energy Institute
Breslaujos g. 3
44403, Kaunas, Lithuania

Ričardas Krikštolaitis, Juozas Augutis, Vika Juričkaitė
Vytautas Magnus University
Vileikos g. 8
44404, Kaunas, Lithuania

Roberto Setola
Università CAMPUS Bio-Medico
via A. del Portillo, 21
00128 Roma, Italy

Abstract

In the paper, a general risk assessment procedure for critical infrastructure (CI) is based on the assessment of criticality of CI elements due to the consequences of loss of their functionality, and estimation of probabilities associated with these criticalities. Bayesian networks method was applied to estimate probabilities of unfunctionality of CI elements to capture the impact of various factors, which influence CI functionality. Implementation of the proposed approach is illustrated by pilot calculations for energy CI of Lithuania.

Keywords: Critical infrastructure, criticality assessment, unfunctionality probability of CI elements, risk assessment.

1. Introduction

Our societies largely depend on the functionalities of several infrastructures, which are generally indicated as Critical Infrastructures (CI). The importance of such infrastructure is emphasized by several governmental initiative including the European Council Directive 2008/114/EC (European Council 2008). Specifically this Directive asks for identifying and assessing the different infrastructures on the base of their risk considering the “most realistic worst case”. However, in the framework of the Directive noted no risk assessment methodology was developed and the Member States are following their own methodologies.

Energy critical infrastructure as a complex system requires being analysed (modelled and simulated) taking into account interconnections between elements of particular systems and cross-border dependencies and interdependencies. On the other hand, various factors, such as natural and technological hazards, socio-political and geopolitical threats, etc., can influence the functioning of energy system elements (and energy system as a whole). Thus, the all-hazard approach is essential to perform comprehensive risk assessment.

An approach of risk assessment for critical energy infrastructure as a continuation of previous work (Augutis et al. 2016) for criticality assessment of CI elements due to the loss of their functionality is presented in the paper. While the functionality of CI elements depends on various factors, the all-hazard approach was decided to be implemented by using Bayesian networks (BNs) as a technique capable of capturing the impact of various factors and much more, BNs are applicable to model cascading effects. Both probabilities of losing the functionality of CI elements and criticality leaded by the loss of particular CI elements contribute to comprehensive risk assessment for CI via risk matrix.

2. Risk assessment approach for critical infrastructure

In general, the classical procedure of risk assessment (scheme is presented in Figure 1) is universal and easily adaptable, and it is supposed to be sufficient for risk assessment for critical infrastructure as well.

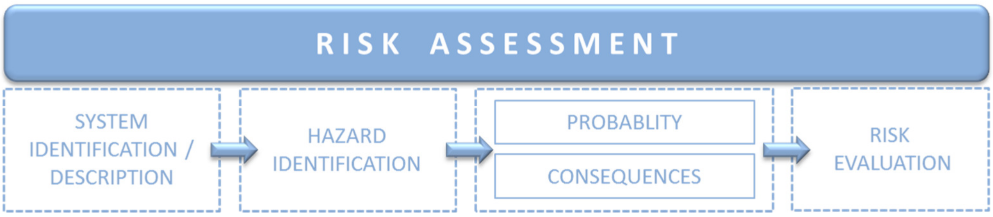


Figure 1. Scheme of risk assessment procedure.

Detailed description for each step of proposed risk assessment procedure is given in subsections 2.1 – 2.4 below.

2.1 System description

In the case of CI description, complex system, network, graph or even system-of-systems concepts can be applied. Generally, any CI can be characterized as a complex system (CS), which is defined as a system where the collective behaviour of its parts entails emergence of properties that can hardly, if not at all, be inferred from properties of the parts (Complex systems society).

CI as complex systems are rational, well designed, perform their functions over periods of time and under a variety of threats. Interconnected and interdependent critical energy infrastructures also can be defined as complex systems, consisting of physical facilities, transmission lines, roads, railways, human decision makers, etc. However, complex systems can be modelled as a network and defined as a graph, where nodes are components, connections and relationships are links.

Operations of any critical infrastructure can be dependent upon each of the other CI, i.e. dependencies and interdependencies between infrastructures exist, which have to be defined. There are various dimensions and types of CI interdependencies, which vary widely and each has its own characteristics. Usually, four principal classes of interdependencies – physical, cyber, geographic, and logical – are defined and examined (Rinaldi et al. 2001). However, more types of CI interdependencies exist in reality, such as economic, technological, social/human, political/policy/legal, organizational/business, etc. For example, in the energy CI, there is a physical dependency between electricity production generators and the gas supply system.
Usually, interdependencies are considered when examining the more general case of multiple critical infrastructures connected as a “system-of-systems”. A system-of-systems (SoS) consist of multiple, heterogeneous, distributed, occasionally independently operating systems embedded in networks at multiple levels that evolve over time (DeLaurentis 2007). Alternatively, the term “complex systems” is also used in defining SoS: “Systems-of-systems are large scale concurrent and distributed systems that are comprised of complex systems” (Kotov 1997).

System representation as a multigraph is widely used in order to perform simulations. Thus, directed multigraph is considered

$$G = (V, E), \tag{1}$$

where V – set of nodes (vertices), $V = \{z_1, \ldots, z_N\}$, E – set of edges, $E = \{l_1, \ldots, l_M\}$, which cover all elements of analyzed system(s) and relations between them.

2.2 Hazard identification

Hazard identification for critical infrastructure is also one of the steps in the risk assessment procedure. Hazard can be any “dangerous phenomenon, substance, human activity or condition that may cause loss of life, injury or other health impacts, property damage, loss of livelihoods and services, social and economic disruption, or environmental damage” (UNISDR 2009). Usually, hazard is referred as synonymous to threat for CI.

Every CI is surrounded by a variety of hazards of various origins. They depend on the country where the critical infrastructure exists, its geographic and political region/context. Relatively hazards for critical infrastructures can roughly be divided into several types as natural, technical, economic, socio-political and geopolitical (Table 1).

Table 1: Types of hazards for critical infrastructure.

Type of hazard	Description
Natural	Adverse and extreme natural phenomena, such as hazards occurring in the air (extreme wind, tornado, showers, extreme fluctuation of temperature, drought, lightning, fogs, storms, blizzards, frosts, etc.); hazards occurring on the ground and under the ground (earthquake, tsunamis, floods, movement of ground, volcanic eruption, subsidence of ground, erosion of coast, etc.); external fires (fires of the woods environmental the CI, fires of peat, etc.).
Technical	Caused by the unreliable functionality of CI and result from various accidents and failures that occur due to technical reasons and may cause serious disruptions of CI or even a complete termination of CI functioning.
Economic	Economic crises, isolation of the system, domination of a particular source of fuel, producer or supplier, the presence of monopolies in the case of critical energy infrastructure.
Socio-political, geopolitical	The existence (or imagined existence) of these hazards has a substantial impact on decision-making with regard to CI development. These hazards, albeit being not as evident as natural disasters or technical accidents, are significant and might have severe consequences. Terrorism and cyber-attacks can also be defined as socio-political threats.

Technical, economic, socio-political and geopolitical hazards usually may be referred to human caused hazards of two types: non malicious and malicious (Table 2).

Table 2: Human caused hazards for critical infrastructure.

Non malicious	Malicious
Explosions (explosions of gas, fuel, ammunition, chemical substances, etc.); transport accidents (aircraft crash, accident of automobile and water transport, failure on railways, etc.); failures related to transportation of a dangerous cargo (accidents in transportation of explosive, poisonous, toxic, radioactive, easily inflammable and other cargoes); emergency events on industrial and military objects (explosions, wreck of technical constructions, outflow of toxic and poisonous substances, explosions of the ammunition, the non-authorized shots of rockets, having dug gas and oil pipelines, etc.); loss of critical infrastructure.	Cyber-attacks, diversions and acts of terrorism.

The loss or disruption of critical infrastructure is considered separately as a human caused hazard (unintentional, accident) in this methodology. The inclusion of CI loss as a specific hazard highlights the fact that the probability of such an event is important in the CI risk assessment procedure.

2.3 Probability estimation and consequence analysis

Natural environmental of the system is full of potential hazards which may cause the negative effect to the particular elements of the system and to the system as a whole as well. Let us assume that the impact of hazards is considered as a disruption of functionality of particular element (or group of elements). Disruption (fully of partly) of the functionality of the whole system can be as a result of cascading effect due to dependencies and interdependencies of elements in the reference system.

Authors propose to simulate the functioning of the system when one element or group of particular elements is not operating (Augutis et al. 2014; Augutis et al. 2016): to assess system ability to cope with the loss of one or several elements in the sense of meeting the demands of final consumers for consequence analysis. For instance, disruption of gas supply for heat and electricity generation can be treated by a diversification of the fuel.

Criticality of element(s) in CI was introduced in previous works (Augutis et al. 2014; Augutis et al. 2016) as a measure to assess the impact of the loss of one or group of elements in the system due to its (or their) role in the system (more details are provided in the subsection 2.3.1).

Assessment of consequences is one of two key pillars in risk evaluation. The second component is probability of losing the functionality of one element or group of elements in the system for a particular period due to various hazards.

2.3.1 Criticality assessment as consequence analysis

Calculation of system element's criticality as a measure for quantitative consequence analysis due to the loss of this element (criticality of a group of elements can be calculated as well) was proposed in previous work (Augutis et al. 2016). Criticality of the k^{th} element is defined as

$$c^k(t) = 1 - \sum_{i=1}^{N_C} \frac{S_i^k(t)}{D_i(t)} \beta_i(t),\ 0 \le c^k(t) \le 1,\ k = \overline{1, N}, \tag{2}$$

where $D_i(t)$ – demand of i^{th} final consumer at time moment t (for instance, demand of energy (MWh)); $S_i^k(t)$ – supply to i^{th} consumer in the case when the k^{th} element is not functioning; N_C – number of final consumers in the analysed system; N – number of elements in the analysed system; weighted coefficient $\beta_i(t)$ is estimated regarding to the demand of consumers

$$\beta_i(t) = \frac{D_i(t)}{\sum_{j=1}^{N_C} D_j(t)}, \tag{3}$$

satisfying equality

$$\beta_1(t) + ... + \beta_{N_C}(t) = 1. \tag{4}$$

For example, $c^k(t) = 1$ means that an operation of the whole system are completely stopped, if the k^{th} element is not functioning; $c^k(t) = 0.15$ means that 85% of final consumers demands are met, if the k^{th} element is not functioning.

The approach is applicable to the assessment of criticality of a group of elements: for this purpose, $S_i^k(t)$ in eq. (2) is replaced by "supply to i^{th} consumer", when a particular group of elements does not perform their intended functions.

2.3.2 All-hazard approach for estimation of element unfunctionality probability

The functionality of system elements depends on various factors as technical reliability, internal and external hazards, the functionality of other elements, etc. Thus, approach to estimate probability of functionality of the element should capture all these aspects, i.e. all-hazard approach is required for the purpose. Bayesian networks (Pourret, Naim & Marcot 2008) as a powerful tool towards overall approach were proposed to estimate the probability of the functionality of each element in the system.

BNs are widely used for various critical infrastructures: modelling of water supply network (Francis, Guikema & Henneman 2014), risk analysis for maritime transport system, by taking into account its different factors (i.e., ship-owner, shipyard, port and regulator) and their mutual influences (Trucco et al. 2008), scenario analysis for energy sector (Cinar & Kayakutlu 2010), evaluation of cascading effects in a power grid (Codetta-Raiteri et al. 2012), vulnerability analysis considering cascading effects (Khakzad & Reniers 2015), operational risk assessment (Barua et al. 2016), etc.

A particular BN model is constructed to estimate the probability of functionality for each element. It consists of analysed i^{th} element as node-child and nodes-parents which represent external (human-made and natural) and internal hazards and related elements on the referred system (scheme is presented in Figure 2).

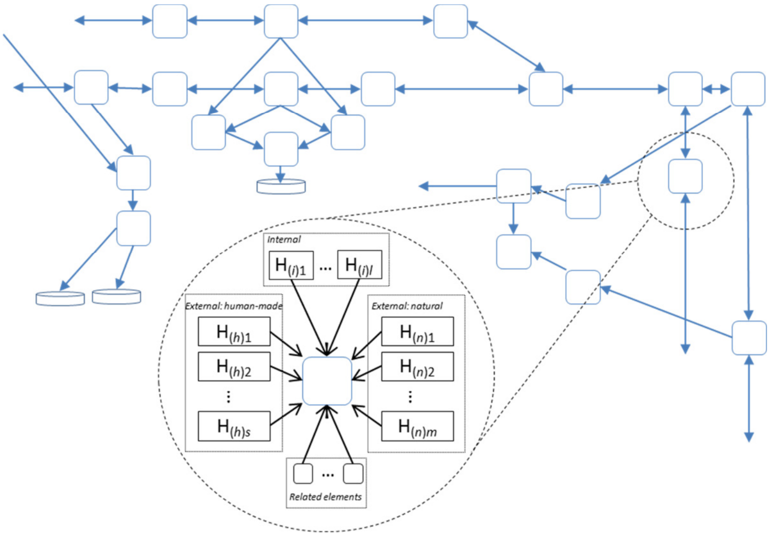


Figure 2. Fragment of the topological scheme of the reference system and Bayesian network for one its element.

Probability of unfunctionality of the j^{th} element is calculated as joint probability of its corresponding random variable Z_j to have value “False” (F)

$$
\begin{aligned}
&P(Z_j = F) = \\
&= \sum_{\mathrm{H}_{(h)1},\ldots,\mathrm{H}_{(i)l},Z_{k_1},\ldots,Z_{k_r} \in \{T,F\}} P(Z_j = F, \mathrm{H}_{(h)1},\ldots,\mathrm{H}_{(i)l}, Z_{k_1},\ldots,Z_{k_r}),
\end{aligned}
\tag{5}
$$

where random variables $\mathrm{H}_{(h)1}$, … , $\mathrm{H}_{(h)s}$, $\mathrm{H}_{(n)1}$, … , $\mathrm{H}_{(n)m}$, $\mathrm{H}_{(i)1}$, … , $\mathrm{H}_{(i)l}$ correspond to external (human-made and natural) and internal hazards respectively, and random variables Z_i, $i \in \{k_1, \ldots, k_r\}$, $1 \le k_1 < \ldots < k_r \le N$, correspond to the functionality of related elements in the system.

BNs of more complex structure are possible, once current node-parent(s) depend(s) on other factors. For instance, reliability of element, as one of the main internal factors having an impact on the functionality of the element, can be assessed via BN as well (Tien & Der Kiureghian 2016).

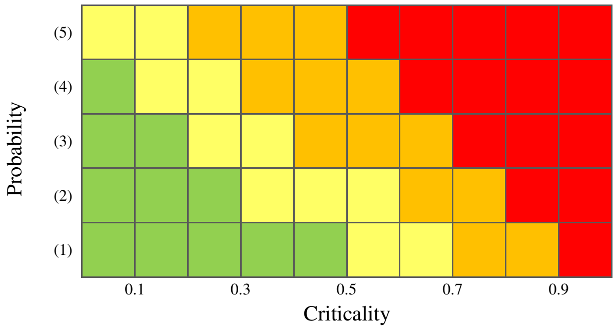
2.4 Risk evaluation

Certainly, a risk evaluation is based on the evaluation of risk metric(s), while risk metric serves two important functions: it enables to talk about risk; to communicate and discuss the results of risk analysis and the aspects of risk that are important and it facilitates decision-making by providing a quantitative measure for risk evaluation. The choice of risk metrics is essential as it directs what kind of information to get from the risk analysis and whether the results are considered as legitimate and informative by decision-makers and stakeholders (Johansen & Rausand 2014). The criteria were summarized in an overall discussion on informative, value-related, and analytical issues that affect the interpretation and choice of risk metrics by I.L. Johansen & M. Rausand (2014).

Indicators as importance measures (Fang, Pedroni & Zio 2016) and risk matrices (Kröger 2008; Kjøllea, Utneb & Gjerdea 2012; Theocharidou & Giannopoulos 2015) can be indicated as applicable and beneficial to CI analysis. Birnbaum's and Fussell-Vesely importance measures were used in previous works (Augutis et al. 2016). Importance measures approach very well identifies the most critical elements of the system in a quantitative way. Despite this merit, the approach based on importance measures give an incomplete picture of the possible risk associated to the loss of functionality of one or more elements in the system.

In this case, risk matrix distinguishes for its capability to capture two highly important components as a severity of consequences and probability of occurrence of these consequences (Theocharidou & Giannopoulos 2015). In general, risk matrix is $r \times c$ table (horizontal axis serves for categories of severity; vertical axis – categories of probability). Such classification of probability (Figure 3) is widely used in the risk assessment of various technical facilities. Meanwhile, number c (categories of consequences severity) strongly relies on chosen consequences analysis and calculated measures.

Risk matrix adapted to CI analysis is presented in Figure 3, where criticality of element(s) plays the role of the severity of consequences.



Classification of probability:

(1) – very unlikely:	expected to occur less than once in 10000 years
(2) – unlikely:	expected to occur at least once in 1000 – 10000 years
(3) – possible:	expected to occur at least once in 100 – 1000 years
(4) – likely:	expected to occur at least once in 10 – 100 years
(5) – very likely:	expected to occur at least once in 10 years

🟥 – very high, 🟧 – high, 🟨 – medium, 🟩 – low (tolerable) risk.

Figure 3. An example of adapted risk matrix for CI.

Results presented in the light of such risk matrix are more informative and easily understandable for decision-makers and stakeholders.

3. Pilot calculations

3.1 Energy system description

In this paper, Lithuanian energy system is analysed for risk assessment taking into account criticality of energy infrastructure elements. Lithuanian energy system can be identified as system-of-systems since it consists of the electricity system, the district heating systems, fuel supply system for electricity and heat production and other having connections with each other. The connections among systems are both physical (e.g., electricity transmission network connected with generation sources and distribution network) and functional (e.g., thermal power plant, which connects gas pipelines, district heating network and electricity supply network, by transforming primary energy into the heat and electricity, which are supplied to consumers). Reversible connections also exist among different energy systems, such as natural gas supply to power plants to produce electricity, which is correspondingly needed for proper functioning of the natural gas transmission system. In this paper, Lithuanian energy system is considered as a graph with different nodes representing infrastructure elements. Usually, energy system connections are depicted as network systems or graphs.

In the pilot calculations, elements of different energy system infrastructures in Lithuania are denoted as nodes: z_1, z_2, z_3, ..., z_N, where N – number of elements ($N = 157$). Elements of gas supply system – from z_1 to z_{90}, heat generation technologies in six main cities (which used the natural gas as the main fuel) – from z_{91} to z_{126}, power plants – from z_{127} to z_{133}, technologies of renewable energy sources – from z_{134} to z_{157}.

3.2 Criticality assessment

Assessment of criticality of elements (defined in subsection 2.3.1) with regard to electricity demand of final consumers was carried out according to *N*-1 and *N*-2 principles. "*N*-1" means that only one element out of *N* elements is not functioning (157 scenarios in analysed case, when $N = 157$), "*N*-2" – two elements in the system are not functioning at the time (12246 combinations in analysed case). A part of the results (Augutis et al. 2016) are presented in Figure 4: scenarios related to the highest values of calculated criticality of separate elements (1 scenario) and combinations of two elements (20 scenarios). The results of *N*-1 analysis revealed: the loss of functionality of the element z_{89} leads to the highest value of criticality. Element z_{89} represents pipeline connecting the highest capacity electricity generation technology with the main natural gas supply system. The values of criticality of other elements did not exceed 0.1 (in the case of *N*-1 analysis). *N*-2 analysis demonstrated that pair of z_{89} and z_{131} associates with exceptionally high criticality comparing to other pairs. Element z_{131} represents power plant unit with the highest capacity, which can generate electricity using the alternative fuel.

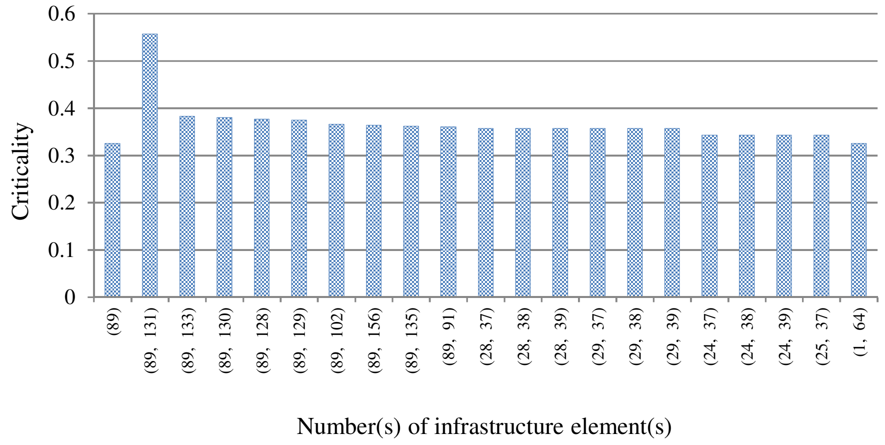


Figure 4. Scenarios of *N*-1 and *N*-2 analysis, associated to the highest values of criticality.

3.3 Probability of element's functionality

Even relatively high criticality not always associates with the highest risk, if only the probability of this situation is negligible. Aiming at this, the probability of the loss of functionality was estimated for each element.

In the paper, Bayesian networks for elements z_{89} and z_{131} are presented in more details. Element z_{131} is dependent on element z_{89}, i.e. one-directional dependence: $z_{89} \rightarrow z_{131}$. Performing *N*-1 analysis, first of all, we estimate the probability of functionality of element z_{89}, then probability of element z_{131}. Main hazards or factors, which may have an impact on the functionality of the elements z_{89} and z_{131} are listed in Table 3.

Table 3: Hazard identification for elements (z_{89} , z_{131}).

Type of hazard	**Identified hazards**	
	For element z_{89}	**For element z_{131}**
Internal	rupture probability[1]	technical reliability[2]
External (natural)	earthquake	flooding, extreme wind, earthquake
External (human-made)	sabotage or terrorist attack	sabotage or terrorist attack
Related elements in the system	z_{87} & z_{88}[3]	z_{89}[4] alternative fuel

[1] rupture probability can be estimated using approach, which captures results of non-destructive inspections and failure data (Dundulis et al, 2016);

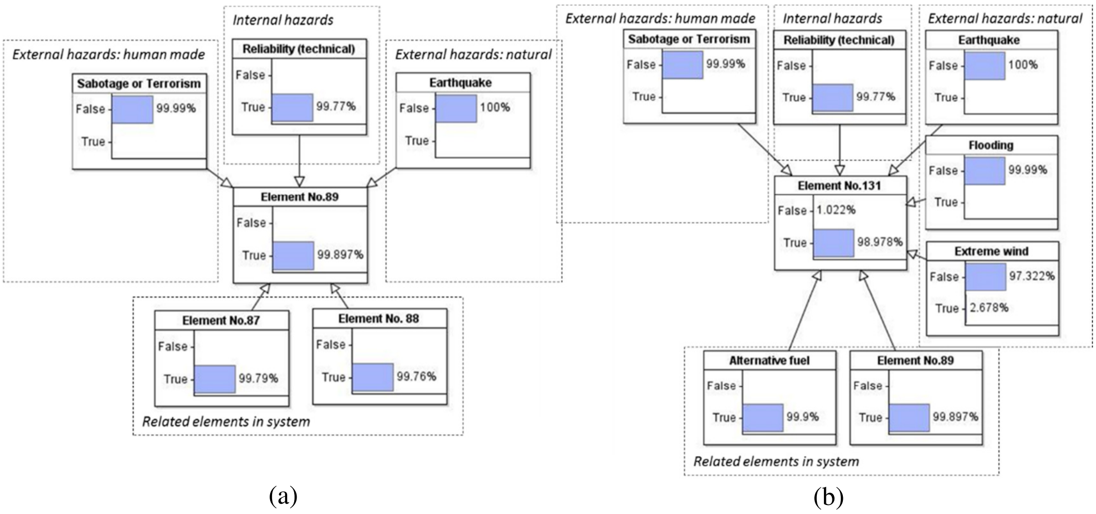
[2] power plant safety report can serve for quantitative evaluation;

[3] element z_{89} has direct connection with neighbouring elements z_{87} & z_{88} of natural gas transmission system;

[4] element z_{131} relies on the functionality of element z_{89}, which should ensure supply of primary fuel (natural gas).

Usually, initial probabilities of natural hazards such as extreme wind, flooding, are based on statistical analysis of historical data of the region, where analysed CI is located. The probability of earthquake occurrence in the territory of Ignalina nuclear power plant (in the north-east of the country) was applied to the whole territory of Lithuania (approx. 65300 km^2). This assumption was made, because Lithuania is not located in the seismically active zone.

Bayesian networks for elements z_{89} and z_{131} are presented in Figure 5 and Figure 6, respectively. A particular Bayesian network was constructed for each element in the analysed system towards estimation of probabilities of their functionality (N-1 analysis).



(a) (b)

Figure 5. Bayesian network for elements: z_{89} (a), z_{131} (b).

N-2 analysis is not straightforward, particular when failures of not independent elements are analysed. For instance, the particular case of *N*-2 considering the failures of elements z_{89} and z_{131} is possible in two scenarios:

1) element z_{89} fails (loses its functionality) and this causes a cascading effect to $z_{131,}$ probability of this case is equal to "$P(z_{89} = F)\cdot P(z_{131} = F \mid z_{89} = F)$";
2) failure of element z_{131} occurs while element z_{89} is still working, but after that failure of element z_{89} occurs as well, probability of this case is equal to "$P(z_{131} = F \mid z_{89} = T)\cdot P(z_{89} = F)$".

Summarizing total probability of the failures of both elements z_{89} and $z_{131}$is

$$\begin{aligned}&P(Z_{89}=F,Z_{131}=F)=\\&=P(Z_{89}=F)P(Z_{131}=F\mid Z_{89}=F)+P(Z_{131}=F\mid Z_{89}=T)P(Z_{89}=F),\end{aligned} \tag{6}$$

where probability $P(z_{89} = F)$ is estimated in *N*-1 analysis, $P(z_{131} = F \mid z_{89} = F)$ and $P(z_{131} = F \mid z_{89} = T)$ are estimated within BN (Figure 6), setting evidence that z_{89} has failed or is functioning respectively.

The same approach was used to estimate remaining probabilities of losing functionalities of any two elements (all possible combinations).

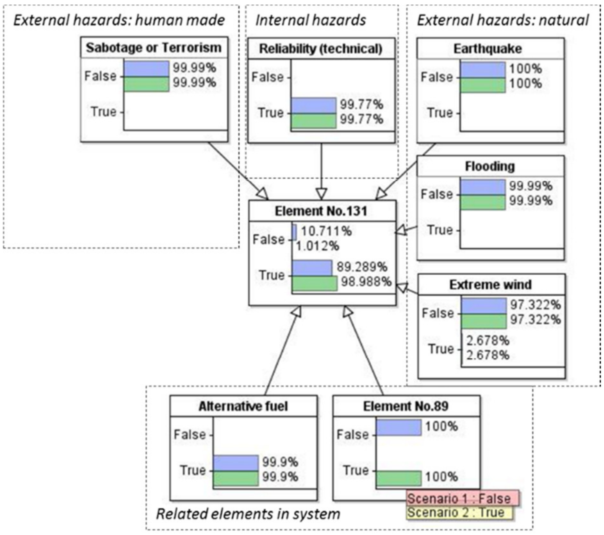
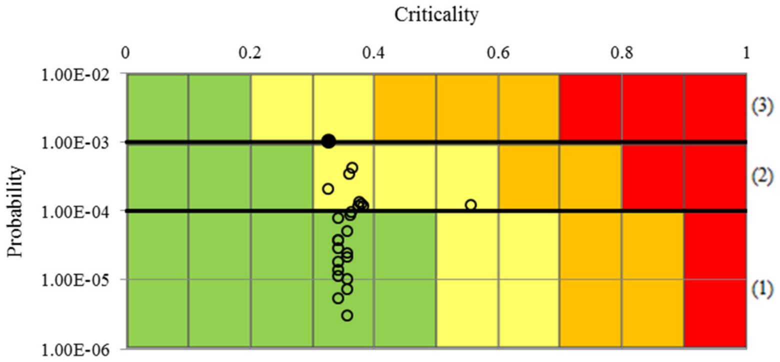


Figure 6. Bayesian networks for *N*-2 analysis: z_{89} & z_{131}: scenario 1 – setting evidence of failure of element z_{89} (=>$P(z_{131} = F \mid z_{89} = F)$); scenario 2 – setting evidence that element z_{89} is functioning (=> $P(z_{131} = F \mid z_{89} = T)$).

However, proposed approach assumes that failure probabilities in *N*-2 analysis do not depend on the operative condition of the network, as it may be illustrated by several episodes (e.g. the Italian Black-out in 2003). Due to the re-distribution of the flows some links are going to operate in overload conditions and this considerably increases the probability of failure. Proposed approach should be considered as a first crude approximation. To take into account such phenomena, future studies should consider the probability as condition dependent, i.e. the internal probability of fault will be increased in accordance with the increased load of the element.

3.4 Risk evaluation via risk matrix

Obtained probabilities of functionality of elements or their groups and associated criticalities are summarized into risk matrix (proposed in subsection 2.4). The results for analysed scenarios (21 out of 12403), associated to the highest value of criticality, are presented in Figure 7.



● – scenarios of *N*-1 analysis
○ – scenarios of *N*-2 analysis

Figure 7. Results of pilot case study over the risk matrix (logarithmic scale is used for vertical axis).

These pilot calculations demonstrate that most of all analysed scenarios of *N*-1 and *N*-2 analyses fall into the zone of tolerable risk and very few scenarios into zone of medium risk.

4. Conclusions

Risk assessment procedure for critical infrastructure based on CI criticality is presented in this paper.

Previous studies (Augutis et al. 2014; Augutis et al. 2016) demonstrated capabilities of CI criticality assessment to identify critical elements (or groups of elements) in the system. Nevertheless, CI criticality assessment approach has to be enhanced towards comprehensive risk assessment for CI. Thus, this paper contributes to the development of the approach used for risk assessment of energy CI.

Proposed approach is based on the assessment of criticality of CI elements and groups of them (as consequence analysis) due to the loss of their functionality, and estimation of probabilities associated with these criticalities. While the functionality of CI elements depends on various factors, such as technical reliability, internal and external hazards, functionality of other elements, etc., the all-hazard approach was implemented by using Bayesian networks as a technique capable of capturing all these aspects. Criticality of CI elements (as a measure of consequences) and probabilities of consequences occurrence are coupled within risk matrix that enables to evaluate the risk of CI.

Implementation of the proposed approach is illustrated by pilot calculations for energy CI of Lithuania.

References

Augutis, J., Jokšas, B., Krikštolaitis, R. & Urbonas, R. 2016. The assessment technology of energy critical infrastructure. *Applied Energy* 162: 1494-1504.

Augutis, J., Jokšas, B., Krikštolaitis, R. & Žutautaitė, I. 2014. Criticality assessment of energy infrastructure. *Technological and Economic Development of Economy* 20(2): 312-331.

Barua, S., Gao, X., Pasman, H. & Mannan, M.S. 2016. *Journal of Loss Prevention in the Process Industries* 41: 399-410.

Cinar, D. & Kayakutlu, G. 2010. Scenario analysis using Bayesian networks: A case study in energy sector. *Knowledge-Based Systems* 23: 267–276.

Codetta-Raiteri, D., Bobbio, A., Montani, S. & Portinale L. 2012. A dynamic Bayesian network based framework to evaluate cascading effects in a power grid. *Engineering Applications of Artificial Intelligence* 25: 683-697.

Complex systems society. Available online: http://cssociety.org/about-us/what-are-cs

European Council. 2008. 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. Online: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008L0114

DeLaurentis D. 2007. Role of Humans in Complexity of a System-of-Systems. In: Duffy VG, editor. Digital Human Modeling, HCII 2007, LNCS 4561, Springer-Verlag Berlin Heidelberg, 363-371.

Dundulis, G., Žutautaitė, I., Janulionis, R., Ušpuras, E., Rimkevičius, S. & Eid, M. 2016. *Reliability Engineering and System Safety*156:195-202.

Johansen, I.L., Rausand, M. 2014. Foundations and choice of risk metrics. *Safety Science* 62, 386–399.

Fang, Y.P., Pedroni, N. & Zio, E. 2016. Resilience-Based Component Importance Measures for Critical Infrastructure Network Systems. *IEEE Transactions on Reliability* 65(2): 502-512.

Francis, R.A, Guikema, S.D. & Henneman L. 2014. Bayesian Belief Networks for predicting drinking water distribution system pipe breaks. *Reliability Engineering and System Safety* 130: 1-11.

Kjøllea, G.H., Utneb, I.B. & Gjerdea O. 2012. Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies. *Reliability Engineering and System Safety* 105: 80-89.

Khakzad, N., Reniers, G. 2015. Using graph theory to analyse the vulnerability of process plants in the context of cascading effects. *Reliability Engineering and System Safety*143: 63–73.

Kotov V. 1997. Systems-of-Systems as Communicating Structures, Hewlett Packard Computer Systems Laboratory Paper, HPL-97-124.

Kröger, W. 2008. Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools. *Reliability Engineering and System Safety* 93: 1781-1787.

Pourret, O., Naim, P. & Marcot, B. 2008. Bayesian networks: A Practical Guide to Applications. John Wiley & Sons.

Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K. 2001. Identifying, Understanding, and Analyzing Critical Infrastructure Inter-dependencies. *IEEE Control Systems Magazine* 21(6): 11-25.

Theocharidou M., Giannopoulos G. 2015. Risk assessment methodologies for critical infrastructure protection. Part II: A new approach. JRC Science and Policy Report.

Tien, I. & Der Kiureghian A. 2016. Algorithms for Bayesian network modeling and reliability assessment of infrastructure systems. *Reliability Engineering and System Safety* 156: 134–147.

Trucco, P., Cagno, E., Ruggeri, F., Grande, O. 2008. A Bayesian belief network modelling of organizational factors in risk analysis: a case study in maritime transportation. *Reliability Engineering and System Safety* 93(6):845–856.

UNISDR. 2009. UNISDR Terminology on Disaster Risk Reduction. Published by United Nations International Strategy for Disaster Reduction (UNISDR). Online: http://www.unisdr.org/files/7817_UNISDRTerminologyEnglish.pdf

Degradation assessment of bridge components using Structural Health Monitoring

Christelle Geara
Ecole Supérieure d'Ingénieurs de Beyrouth (ESIB), Saint-Joseph University, CST Mkalles Mar Roukos,
PO Box 11-514, Riad El Solh, Beirut 1107 2050, Lebanon

Alaa Chateauneuf
Université Clermont Auvergne, CNRS, SIGMA Clermont, Institut Pascal,
F-63000 Clermont–Ferrand, France

Rafic Faddoul
Ecole Supérieure d'Ingénieurs de Beyrouth (ESIB), Saint-Joseph University, CST Mkalles Mar Roukos,
PO Box 11-514, Riad El Solh, Beirut 1107 2050, Lebanon

Abstract

The Structural Health Monitoring combines a variety of sensing technologies for the detection, localization and characterization of a damage and damaging phenomena in order to predict the residual life of the structure. One of the important issues in structural health monitoring consists in finding the defect parameters in a structure through an optimization problem. This paper presents an application of this optimization problem on a simply supported reinforce concrete bridge girder. Four different cases are considered in the present work, according to the position of the sensors and the defects. The location of the defect and its effect on the reduction of the rigidity have been obtained using genetic algorithm which is an effective procedure to solve such problems. The results have shown that the proposed method is able to detect the damage accurately considering possible sources of error.

1. Introduction

The level of safety of many in-service structures tend to be inadequate to current design documents. Therefore, one of the most important issues in civil engineering is the detection of structural damages, defined as changes in material properties and boundary conditions which adversely affect the system performance. So far, the most commonly used concept of monitoring is the periodical inspection which starts with a visual inspection [1]. More complex surveillance tasks can be realized with good cost effectiveness by using modern transducer and information technologies for monitoring with a high degree of automation.

The Structural Health Monitoring (SHM) is a set of techniques and methodologies for detection, localization, characterization and quantification of damages and damaging phenomena. These techniques are used, among others, to predict the residual life of the structure. SHM can be conceptually divided into two parts: first, the installation of sensing elements and of automated data acquisition system, and second, the interpretation of the acquired data which will lead to a comparison of measured and calculated data to validate model assumptions or to verify the effectiveness and efficiency of the monitoring system. In order to use a cost-effective maintenance strategy, the optimal solution consists of minimizing the total expected cost under the reliability constraints as follows [2]:

$$min\ C_E = C_{PM} + C_{INS} + C_{REP} + C_{FAIL}$$
$$\text{s.t. } \beta \geq \beta^*$$

where:

C_E : is the total expected cost,
C_{PM} : is the preventive maintenance cost,
C_{INS} : is the inspection and monitoring cost,
C_{REP} : is the repair cost,
C_{FAIL} : is the failure cost,
B, β : are structural and target reliability indexes.

The assessment of an existing structure follows a seven step process [3]:

- Preliminary on-site inspection
- Recovery and review of all relevant documentation
- Specific on-site testing and measurements
- Analysis of collected data to refine the probabilistic models for structural resistance
- Accurate (re-) analysis of the structure with updated loading and resistance parameters
- Structural reliability analysis
- Decision analysis

On-site inspection, as mentioned before, starts with a visual inspection followed by destructive and non-destructive testing to evaluate the properties of materials, components or system. The Non-Destructive Testing (NDT) are highly valuable techniques because they do not cause damage to the structure; however each one of these techniques has its advantages, disadvantages and limitations.

The objective of Structural Health Monitoring (SHM) technology is to develop autonomous systems for the continuous monitoring, inspection, and damage detection of structures with minimum human involvement. The results of structural conditions may be recorded through a local network or to a remote center automatically by determining different classes of recipients responsible for decision-making.

Thus, the most important advantages of monitoring systems are:

- real-time monitoring and reporting
- structural information on a continuous time basis (structural history)
- early detection of deteriorations and initializing deficiencies
- information for reliability based preventive maintenance operations
- saving in maintenance cost
- minimum human involvement
- reducing labor, visual inspection, downtime, and human error
- automation - improving safety and reliability
- calibration data for analytical models for validation and verification

2. Local and Global Structural Health Monitoring

SHM can be divided into two main approaches: (i) Local SHM and (ii) Global SHM. Local SHM techniques rely on direct evaluation of a structural member to evaluate its state with respect to the different possible defect and degradation types. Intermittent structural evaluation by mean of a visual inspection or by using various Non Destructive Evaluation (NDE) techniques that are applied directly by inspectors belong to the local approach. This approach also includes long term continuous monitoring using sensors embedded or attached to the structural member used to evaluate a specific performance parameter of the member.

For example, a bridge pile can be monitored for tilting using appropriate sensors, a bridge deck girder can be monitored for excessive deflection during its service lifetime using deflectometers or long base deformation sensors (the results of which can be integrated to obtain the deflection of the girder at different points of its axis). While providing relatively precise measurement for performance parameters which are directly observed or for which specific sensors were installed, this approach is not practical for complex structures having numerous structural members. The exhaustive instrumentation of such a structure would not be economically feasible most of the times. Also, some structures may include features that cannot be directly accessed and/or measured, in such cases the performance of the related structural members must be assessed indirectly by means of global SHM techniques.

In global SHM, a few sensors whose types, number and location must be judiciously chosen, are used to monitor the structure for the advent of specific failure modes. The parameters of the sensing scheme (types, numbers and location) must be optimized in order to maximize the following (sometime conflicting) objectives:

1- Increase the probability of detection of a defect;
2- Increase the reliability and precision of defect localization;
3- Increase the precision of the evaluation of defect extent.

Global SHM approaches can be further divided into: (i) direct methods and (ii) indirect methods. In Global SHM direct methods, measurement datasets are used directly to attain the above mentioned objectives.

Such methods usually involve one or several of the following techniques: pattern recognition, machine learning, classification algorithms etc. A typical global SHM scenario will consist broadly of the following steps:

1- A set of different failure modes is made up by one or several experts based on mechanical analyses and investigations, and/or historical behavior of similar structures;
2- For each failure mode specified in the first step, the corresponding predicted sensor measurements are calculated (via analytical models, Finite elements models, etc.);
3- Actual real measurements are compared (using for example pattern recognition techniques) to measurement sets calculated at step 2. If a match is successful, then one can infer that the corresponding failure mode has occurred.

The rational underlying global indirect SHM methods is the fact that under unchanging load conditions, any changes in variables measured by the sensors, is due to changes in the underlying structural characteristics (changing material properties, boundary conditions, etc.).

Thus, global indirect SHM methods focus on updating our knowledge of the structural characteristics given the measured data.

The great advantage of indirect methods is their ability to systematically and transparently take into consideration all uncertainties that affect the structural system as well as the measuring system. For example, one might face the following uncertainties in SHM problems:

1- Uncertainties related to the true values of structural parameters (Young’s modulus, stiffness, geometrical dimensions, etc.)
2- Structural model uncertainties that may affect predicted behavior of the structure for a given set of values of structural parameters;
3- Measurement uncertainties that may veil the true values of measurement variables.

A natural methodology that one might use in order to take into account the above mentioned uncertainties would be a Bayesian updating methodology that would take as a first step an initial subjective probability distribution of the structural parameters, and then, as new data becomes available the initial probability distribution will be updated accordingly.

3. Identification by genetic algorithms

The identification of the parameters of the sensing scheme (types, numbers and location) could be done by an effective algorithm, the genetic algorithm (GA). It is a search procedure that uses the mechanics of natural selection and natural genetics where chromosomes can be coded in two different ways: either as binary vectors or as real vectors. The sum of all bits, which represent one search variables, is called “Gene”, and the sum of all genes collected in a binary vector is called “chromosome”.

For the initialization, a starting population P(t = 0) of n individuals is stochastically generated based on uniform probability within the given bounds. Then, the evaluation and interpretation of the objective function value provides a measure for the "fitness value". So to evolve towards the next generation of generally better solutions, the GA selects the highest performing candidates from the current generation using "survival-of-the-fittest" learning and the selection probability for the recombination is calculated.

The best solutions are then recombined with each other through an operation called “crossover” to form some new solutions which are used to replace the worst solutions of the original population. This type of recombination is defined by two steps:

- at first individuals chosen for the recombination are mixed and then two by two individuals are chosen as parents;
- in the second step, the parents’ chromosomes are recombined according to different crossover schemes.

Another type of recombination is the mutation which consists on finding a new region of the search space and avoiding the convergence to a suboptimum by exchanging values in the chromosome.

In general, the population size is kept constant so it is necessary to decide which individuals should survive or be substituted for the next generation, this step is called “substitution”. There are different kinds of substitutions like the elitism or cancellation of n worst elements or cancellation of n stochastically chosen individuals, etc. The process is then repeated until the desired fitness value is reached.

4. Damage identification procedure

The occurrence of various crack patterns in a structure takes place during construction and/or after completion. A structure component develops cracks whenever the stress in the components exceeds its strength (Figure 1). Some types of cracking indicate a structural issue, when others do not indicate any type of issue other than normal weathering. Whatever the cause, it still remains important to detect a crack at its early age in order to avoid serious failures.

The loads can be divided into two categories: primary and secondary loads.

In the case of bridges, the sources of primary loading include the own weight of materials from which the structure was built, traffic, weather conditions, natural catastrophes and loading conditions experienced during construction. Some of these loads act permanently so they are considered as dead loads while the others are not permanent, so they are called live loads. However, the secondary loads are those due to temperature change, construction eccentricities, shrinkage of structural materials, settlement of foundation, or other such loads.

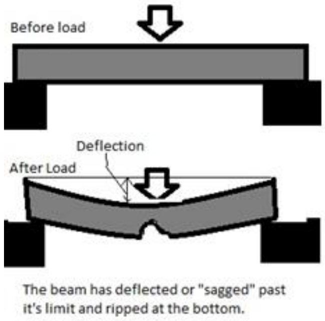

Before load
Deflection
After Load
The beam has deflected or "sagged" past it's limit and ripped at the bottom.

Figure 1: Cracks on a concrete beam after loading

Because of the applied loads, bridge structures accumulate damage during their service life and the actual structure response to loading is degraded from the predicted design performance. Some of the most frequent defects on the elements of a bridge structure are: lateral movements or rotation of the substructure, excessive vertical displacement of the superstructure, cracks and open joints between the segments of the concrete, concrete cover depth defects, corrosion of the reinforcement, etc.

For instance, if we want to study the case where cracks occur in a concrete bridge due to traffic loads:

> A defect d_j in the structure will cause a degradation in the structure which will affect its mechanical properties. To detect the damage, one or more sensors like the linear variable differential transformer (LVDT) can be implemented. The deflection v given by these sensors will depend on a number of parameters such as the load P_i and its location bl, the position of the sensor kl, the span l, the Young's modulus E and the moment of inertia I, in addition to the parameters characterizing the defect like its position cl and the induced reduction of the moment of inertia αI.

In order to identify the defect parameters, the optimization problem should be set such as its solution leads to the best fitting of the defect identification. The fitness function is defined by the sum of quadratic difference between the calculated and observed deflections; this function takes the form:

$$\mathrm{f} = \sum_{i=1}^{N}(v_{calculated} - v_{observed})^2 \qquad (1)$$

The best fitting is the one which leads to the minimum value of f, which should be ideally zero. However, due to uncertainties in the defect evolution and measurement techniques, the zero is never reached and the best solution will appear when f takes the closest value to zero.

As mentioned above, the genetic algorithms are effective to solve this problem. Figure 2 shows the flow chart of the genetic algorithm procedure. At first, a population of chromosomes is randomly created. Each chromosome containing several 8-bit variables, representing the defect parameters to calculate. Then, some individuals of the population are recombined by crossover with a given probability; this latter is chosen as 0.6. The others are subjected to mutation where one bit of the chromosome is switched to another bit (i.e. 0 is switch to 1, and 1 is switched to 0, at a single gene of the chromosome) with a given probability; a value of 0.3 is chosen herein for mutation probability.

The crossover and mutation will result in new offspring being created. Subsequently, a truncation selection is applied on the new population in order to select the individuals with the best fitness.

This procedure (i.e. population evolution) is repeated many times until the best fitness is reached. The computation time depends on the size of each population and the number of generations to reach convergence.

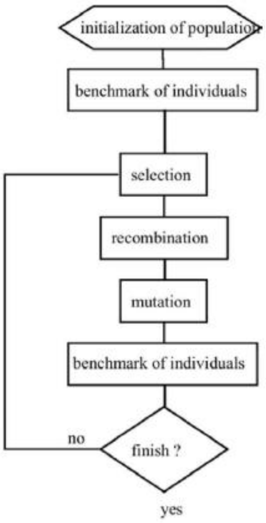


Figure 2: Flow chart of the genetic algorithm.

5. Application to bridge girder

The described procedure is now applied to a reinforced concrete bridge girder, presenting a damage for which the location and amount are unknown. The damage effect is the reduction of the moment of inertia of the affected cross-section. The applied SHM procedure aims therefore to identify the defect parameters: size and location.

Figure 3 plots the simply supported bridge girder with a length *l* and initial moment of inertia I_0. The girder is subject to a moving load *P* located at a distance *bl* from the left support (which will be taken as the reference point). The moving load *P* represents for instance the wheel loads due to heavy trucks or vehicles. At the cross-section affected by the damage, the moment of inertia decreases with time, and takes the value $\alpha(t)I_0$, where *α*(*t*) is a time-dependent reduction rate (between 0 and 1). The monitoring is considered by implementing, either one or two LVDT (Linear Variable Differential Transformer) sensors in the structure at a distance *kl* and *k'l* from the left support, in order to measure the deflections *v* at the sensor positions, and therefore to assess the damage at the unknown location c_l.

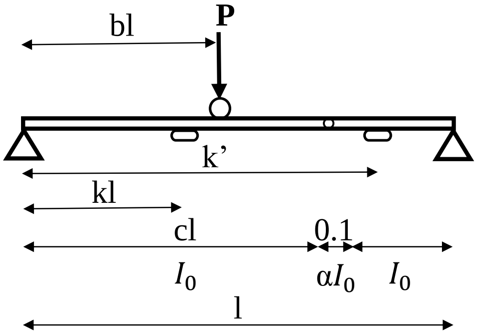


Figure 3: Defected beam implemented by sensors.

Four cases will be considered in this application, depending on the location of the sensor, applied load, defect, and number of implemented sensors. In each case, the deflection *v* is calculated using the virtual work principle, leading to the following formula:

$$v = \int_0^l \frac{M(x).\bar{M}(x)}{EI_0}\,dx \qquad (2)$$

where:

M(x) represents the applied bending moment due to the load *P*, $\bar{M}$(x) represents the bending moment under a unit load at the sensor location, *E* is the Young's modulus, I_0 is the initial moment of inertia of the girder.

In all the cases, it is assumed that *P*, *l*, *k*, *k'* and I_0 are known, and therefore the defect parameters are the only unknown of the problem:

c is the variable defining the defect position,

α(*t*) is the variable defining the decrease with time of the moment of inertia I_0

But since α is a function of the time *t*, it will be represented by a quadratic polynomial as follows:

$$\alpha(\mathrm{t}) = a_1 - a_2\,t - a_3\,t^2 \qquad (3)$$

Therefore, the optimization problem to solve is defined in terms of four variables c, a_1, a_2 and a_3.

The genetic algorithm used to solve the optimization problem described above is based on finding the parameter values corresponding to the best fitness value according to the following equation f = $\sum_{i=1}^{N}(v_{calculated} - v_{observed})^2$. So, the best results are given when *f* converges to zero.

First, the probability of two individuals being recombined by crossover and the probability of an individual being subject to a mutation are not fixed. As it can take values between zero and one, our first task is to find the best combination of these two probabilities which will give us, after many generations, a curve of the fitness converging to zero. After many numerical tests, it has been found that when the probability of crossover is 0.6 and the probability of mutation is 0.3, the curve of the fitness would converge faster. For that reason, these two probability values are considered in the numerical application.

Another issue to consider concerns the position where the crossover or the mutation would take place. Many crossover techniques exist like a single-point crossover or two-point crossover that defines which part of the chromosomes will be exchanged. In our case, since we have many variables to determine, we went through two options:

- the first one was to use a single-point crossover over the chromosome and,
- the second one consisted in using a single-point crossover on each variable (or gene) of the chromosome; so we have as many points as variables, each gene being subjected to a crossover.

The same procedure was applied to the mutation where the chromosome was once subjected to a single-point mutation and another time it was subjected to a single-point mutation on each gene. After comparing the results, we found out that the most effective technique was to apply the crossover and the mutation on each gene of the chromosome.

For the numerical computation, the values of the girder parameters are as following:

P	= 100 kN
L	= 16 m
E	= 33000 MPa
I_0	= 0.00858 m^4
B	= 0.5

In the following, four cases are considered, according to load and sensor locations. The values taken for the parameters k and k' vary, according to each the considered case:

- Case 1: k = 0.5
- Cases 2 and 3: k = 0.65
- Case 4: k = 0.25, and k' = 0.65

5.1. Case 1: load and sensor at mid-span sensor

In this case, the load *P* is also located at mid-span 0.5*l*, and also one sensor is implemented at the same location, i.e. 0.5*l*; in other words, *b*=*k*=0.5. The defect is located at an unknown position at the right half-length of the girder, Figure 4, i.e. *cl* > *0.5l*.

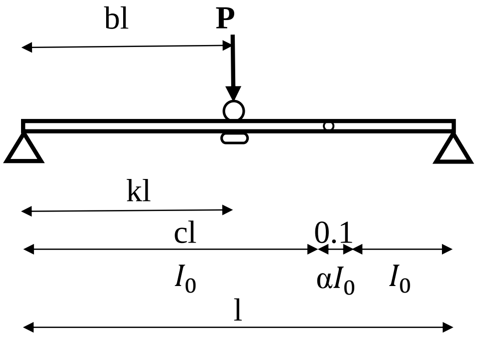


Figure 4: Load and sensor at the mid span of the beam

The deflection at mid-span is calculated by:

$$v = \frac{Pl^3}{12EI_0}(0.25 + ((c-1)^3 - (c-0.9)^3)(1-\frac{1}{\alpha})) \quad (4)$$

For this case, with a population of 100 individuals and after 10 generations, we were able to reach a fitness of 19.208. The convergence curve is given in the following graph, Figure 5, where 8 generations are sufficient to reach the defect identification.

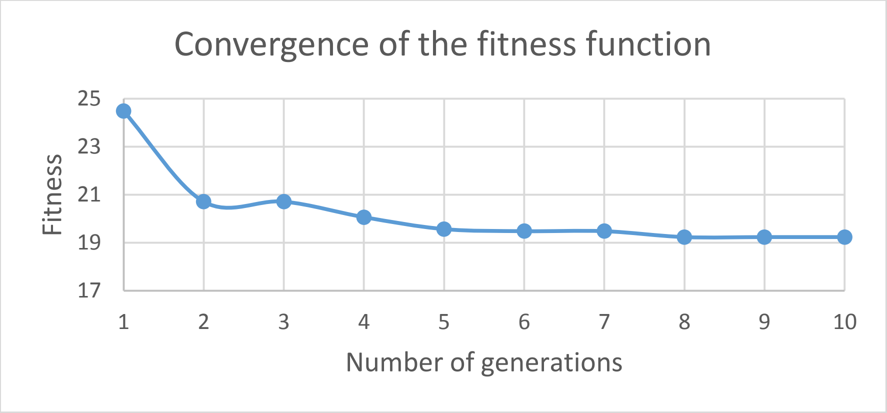


Figure 5: Convergence of the fitness function in case 1

The solution parameters take the values:

c = 0.563
a_1 = 0.996
a_2 = 0.008
a_3 = 0.00004

Therefore, the defect is located at 0.563 from the left support and the decreasing of inertia will be defined by the equation: $\alpha = 0.996 - 0.008t - 0.00004t^2$.

5.2. Case 2: sensor between the load and the defect

When the load, the sensor and the defect are located at various locations, *bl*, *kl* and *cl*, such that $b < k < c$, Figure 6, the deflection is given by:

$$v = \frac{Pbl^3}{3EI_0}((1-k)\big(-0.5b^2 + k(1-0.5k)\big) + k(1-\frac{1}{\alpha})((c-1)^3 - (c-0.9)^3)) \quad (5)$$

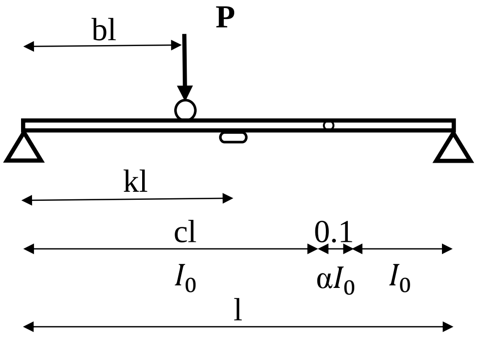


Figure 6: Load and sensor at a random position before the defect

The population is composed of 100 individuals and convergence is achieved after 15 generations, leading to the fitness of 12.486, Figure 7.

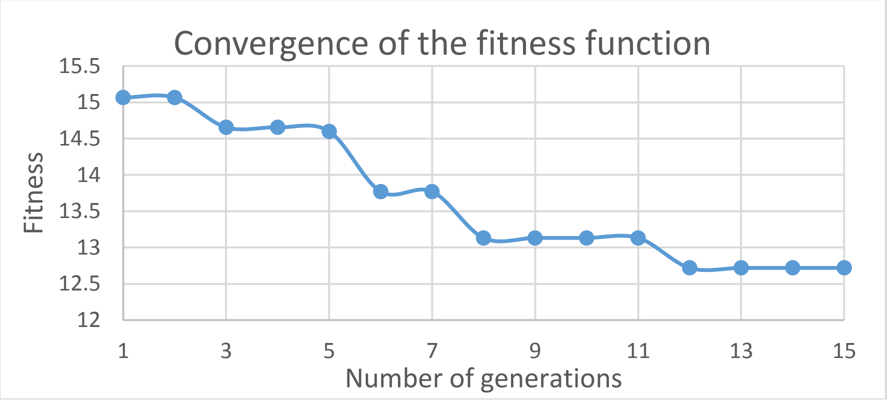


Figure 7: Convergence of the fitness function in case 2.

The obtained results are:

$c =$ 0.656

$a_1 =$ 0.996

$a_2 =$ 0.008

$a_3 =$ 0.00004

Finally, the defect is located at 0.656 from the left support and the decreasing of the moment of inertia is defined by the equation: $\alpha = 0.996 - 0.008t - 0.00004t^2$.

5.3. Case 3: sensor outside of the load and defect range

As in case 2, when the load, the sensor and the defect are located at various locations, *bl, kl* and *cl*, such that $c < b < k$, Figure 8, the deflection is given by:

$$v = \frac{Pl^3(1-k)}{3EI_0}(b(-0.5b^2(3-2b)+k(1-0.5k))+(1-b)((1-\frac{1}{\alpha})(c^3-(c+0.1)^3)+b^3)) \qquad (6)$$

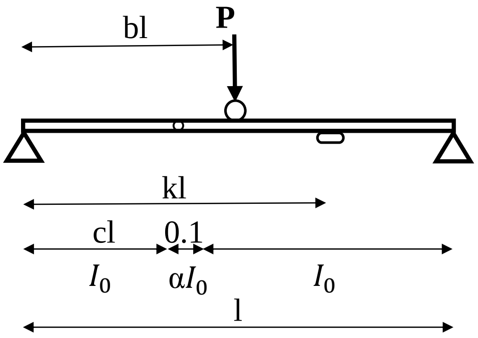


Figure 8: Load and sensor at a random position after the defect

With 100 individuals for each population, convergence is achieved after 17 generations, , Figure 9.

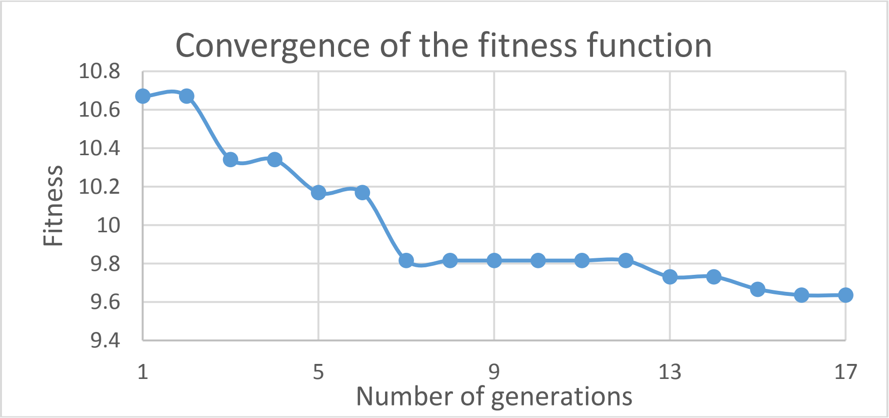


Figure 9: Convergence of the fitness function in case 3.

The solution is:

$c =$	0.363
$a_1 =$	0.996
$a_2 =$	0.008
$a_3 =$	0.00004

Here, the defect is located at 0.363 from the left support and the decreasing of inertia will be defined by the equation: $\alpha = 0.996 - 0.008t - 0.00004t^2$.

5.4. Case 4: two sensors

In this case, two sensors are implemented at different positions, respectively kl and $k'l$, while the load and the defect are located at bl and cl, with: $k < b < c < k'$, Figure 10.

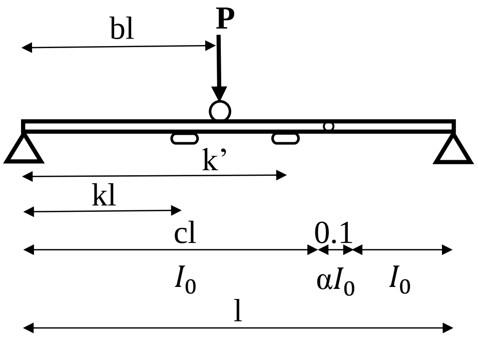


Figure 10: Two sensors implemented at a random position before the defect

The deflections at the sensor positions are computed as:

$$v = \frac{Pkl^3}{3EI_0}((1-b)(-0.5k^2 + b(1-0.5b)) + b(1-\frac{1}{\alpha})((c-1)^3 - (c-0.9)^3)) \quad (7)$$

$$v' = \frac{Pbl^3}{3EI_0}((1-k')(-0.5b^2 + k'(1-0.5k')) + k'(1-\frac{1}{\alpha})((c-1)^3 - (c-0.9)^3)) \quad (8)$$

With 100 individuals in each population, convergence is achieved after 20 generations, Figure 11.

The fitness minimum is achieved with the following parameters:

$c =$	0.711
$a_1 =$	0.996
$a_2 =$	0.02
$a_3 =$	0.00004

Hence, the defect is located at 0.711 from the left support and the decreasing of inertia will be defined by the equation: $\alpha = 0.996 - 0.02t - 0.00004t^2$.

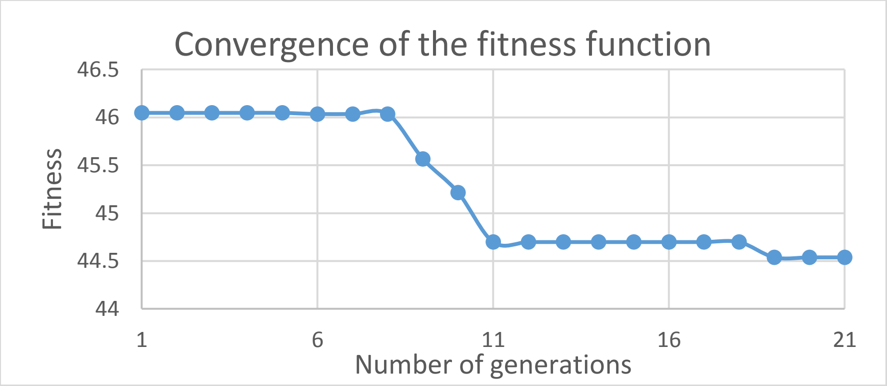


Figure 11: Convergence of the fitness function in case 4.

6. Conclusion

This paper shows the efficiency of the structural health monitoring in assessing the size and location of damage in infrastructures. The genetic algorithms are applied to solve the identification problem, and show high capabilities in solving properly the system. The numerical application on bridge girder shows the efficiency of the adopted procedure, whatever the location and the number of sensors, regarding load conditions and defect location and size. The procedure can be extended to considered several defects in more complex structures.

7. References

[1] Bergmeister, K. (2002) *Monitoring and Safety Evaluation of Existing Concrete Structures, State-of-the-Art Report*.

[2] D.M. Frangopol, *2000:Bridge Health Monitoring and Life Prediction based on Reliability and Economy*, International Workshop on the Present and Future in Health Monitoring, September 3rd-6th, 2000, Bauhaus-University Weimar, Germany.

[3] U. Santa, K. Bergmeister, A. Strauss, *Guaranteeing Structural Service Life Through Monitoring*, 1st fib congress in Osaka 13-19 October 2002, Japan

Pipe rupture and inspection sensitivity analysis

Gintautas Dundulis, Robertas Alzbutas
Lithuanian Energy Institute, Breslaujos str. 3,
LT-44403 Kaunas, Lithuania

Abstract

The in-service inspection of pipes, mechanical components or other components from various critical infrastructures and facilities (including nuclear power plants, water and gas supply systems, etc.) is very important to safe operation of these objects. Degradation is occurring in the piping system and various components by mechanisms such as stress corrosion, fatigue and erosion. An application of Non-Destructive Testing (NDT) methods are important to investigate the degradation mechanisms or to confirm the absence of degradation process and evaluate how defect growth will impact structural integrity during the time interval between inspections. For safe operation of piping it is very important to perform NDT of piping welds and to estimate the inspection frequency.

The main influencing parameters of the pipe rupture and inspection were analysed by use of different structural reliability models, considering a range of various dimensions, materials, degradation mechanisms, loading conditions, NDT reliability and inspection procedures. In such way, the features of Risk Informed (RI) In-Service Inspection (ISI) in Long Term Operation were also investigated. Sensitivity analysis was performed to identify the key influencing parameters under foreseeable variations and uncertain values. In particular, the sensitivity analysis was performed for the real pipe cases of Boiled Water Reactor (BWR). The analysis of the effect of the variation of various parameters influencing the probability of pipe leak and rupture was performed. For instance, flaw geometry, weld residual stress, weld loads, flaw stress, stress corrosion cracking growth rate, fracture toughness, ISI efficiency, leak detection limit were considered in the analysis.

Keywords: Pipe Rupture, Structural Reliability, Fracture Mechanic Analysis,
In-service Inspection, Probabilistic Assessment, Sensitivity Analysis.

1. Introduction

Effective maintenance, surveillance and in-service inspection are essential for the safe operation of a nuclear power plant or other critical infrastructures components. They ensure not only that the levels of reliability and availability of all plant structures, systems and components (SSCs) that have a bearing on safety remain in accordance with the assumptions and intent of the design, but also that the safety of the plant is not adversely affected after the commencement of operation. [1]. Over the plant's operating lifetime, the operating organization should examine SSCs for possible deterioration so as to determine whether they are acceptable for continued safe operation or whether remedial measures should be taken.

For application of a non-destructive examination (NDE) and in-service inspection of the components of critical structures, one of the most important objective is to be able to detect possible degradation at an early stage. For example, this may enable to prevent the damage, to avoid a leakage and/or a possible rupture of pipe. The inspection could be devoted to locations within the plant where one, at the design stage, has indicated that the likelihood of fatigue, high stresses or large plastic deformations is the greatest. However, experiences from detected degradations in critical infrastructures have shown that other causes, in general not anticipated during design, are responsible for most of the damages. Examples are stress corrosion cracking in austenitic stainless steel piping, erosion-corrosion in ferritic piping and thermal fatigue in mixing tees. Obviously, there is a need for an In-Service Inspection (ISI) program that has the capability of more accurately finding the components where the probability of degradation is the greatest.

In-service inspection is an integral part of defence in depth programmes for nuclear power plants, to ensure safe and reliable operation. Traditional in-service inspection programmes were developed using deterministic approaches. However, as probabilistic approaches are being developed, risk insights are being used to optimize in-service inspection programmes by focusing in-service inspection resources on the most risk significant locations [2]. It is recommended to use the results of the risk analysis to define a new risk-informed inspection program where the focus is set on the highest risk locations.

In this paper, the analysis of leak and rupture probability analysis of the BWR type reactor pipe was performed as part of risk studies. The influence of inspection to probability of leak and rupture of pipe was estimated. In this analysis, the stress corrosion cracking mechanisms for BWR pipe is considered. Software AutoPIFRAP was used for this analysis.

In order to ensure that components of critical infrastructures are reliable and safe in case of long term operation loading, it is very important to evaluate parameter uncertainty associated with loads, material properties, geometrical parameters, boundaries, degradation mechanisms and other parameters. Sensitivity analyses were performed to identify the key influencing parameters under foreseeable variations and uncertain values. The sensitivity analysis was performed for the real pipe cases of BWR. The analysis of the effect of the variation of various parameters influencing the probability of pipe leak and rupture was performed. For instance, flaw geometry, weld residual stress, weld loads, flaw stress, stress corrosion cracking growth rate, fracture toughness, ISI efficiency, leak detection limit were considered in the analysis.

2. Structural reliability models and software

AutoPIFRAP was used for leak and rupture probabilities analysis and the sensitivity analysis of the BWR type reactor pipe. AutoPIFRAP - a special Excel spread sheet program system, which can perform and administrate the risk evaluations, sensitivity analysis and investigate and compare different Risk Based Inspection (RBI) suggestions. One of the main AutoPIFRAP parts is the Subsystem of Integration. It must ensure the informational links between the AutoPIFRAP system and the PIFRAP Solver. The Subsystem of Integration can create the input file for each weld, start PIFRAP with this input file and read output file data (for the information flow see Fig. 1).

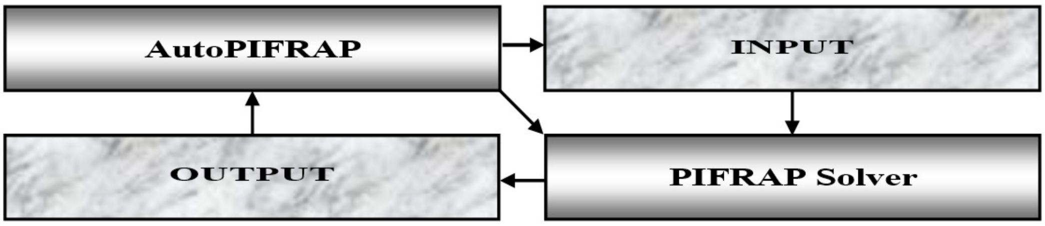


Figure 1. The scheme of information flow between AutoPIFRAP and PIFRAP**.**

In initial data preparation stage, the software for reliability analysis of growing cracks - PIFRAP (PIpe FRActure Probabilities) is used for obtaining the probabilities of leak and rupture. The probabilistic computer code PIFRAP [3; 4] is meant for evaluation of the leak and rupture probabilities of a specific cross section with a certain stress state and possibly containing a circumferential growing crack due to stress corrosion cracking (SCC).

PIFRAP is based on very detailed and complete deterministic fracture mechanical models describing crack growth, for estimation of the crack opening areas and leak rate for through wall cracks, and for evaluation of the event of fracture or plastic collapse. In general, failure of piping due to crack growth is, at normal operation conditions and in materials commonly used, first revealed by the event of wall penetration and leakage, and not by total fracture of the pipe. However, when load events in addition to the normal operation loading are considered, fracture is likely to occur even before wall penetration. Thus, in PIFRAP several load cases are defined and evaluated.

The leak rate in PIFRAP is calculated using the computer code SQUIRT developed by Paul, Ghadiali *et all* [5, 6]'.

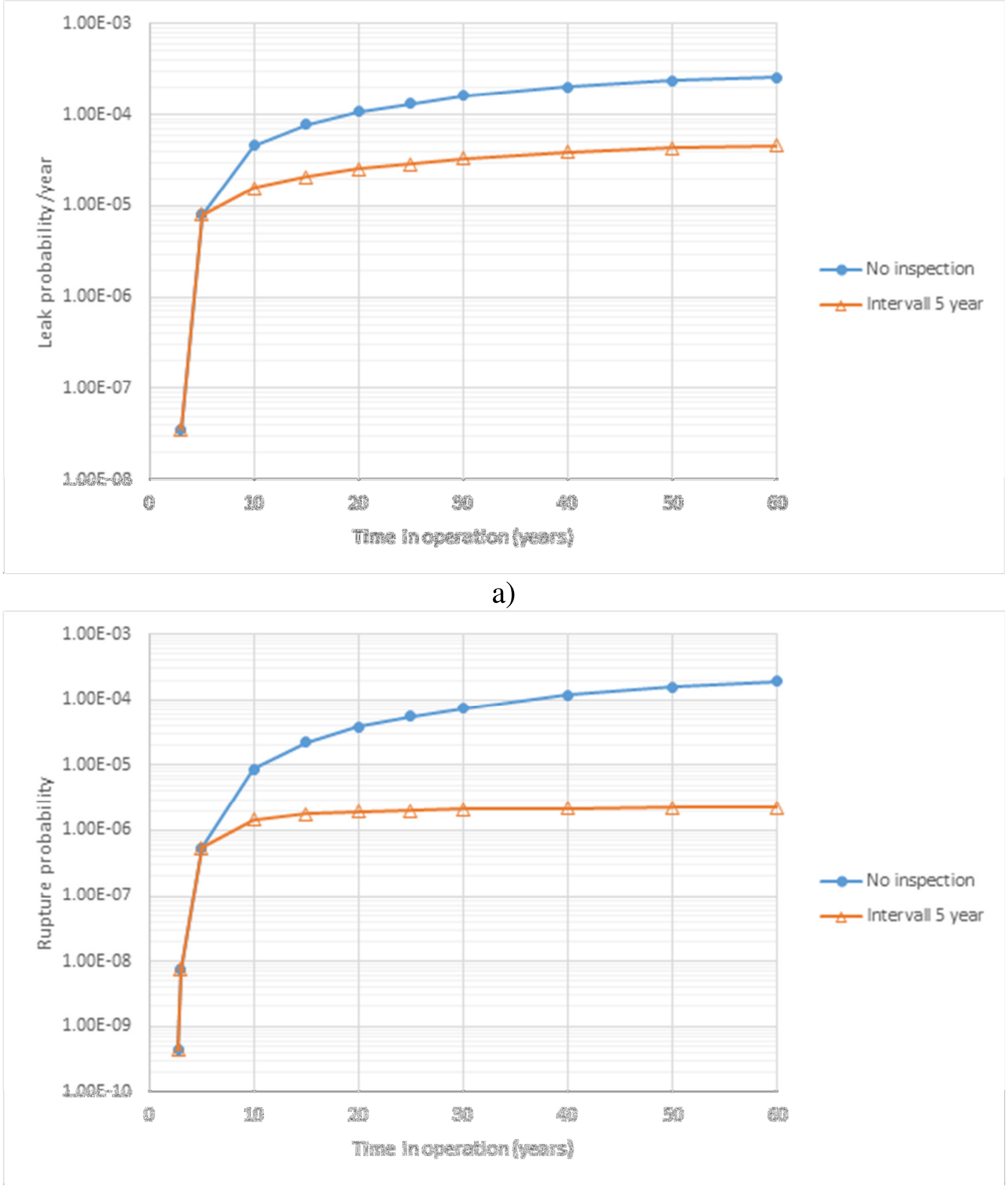
It is very convenient to perform sensitivity analyses by use of AutoPIFRAP. This may give valuable information of the relative importance of different input data to the failure probability. One quantity at a time is varied while the others are fixed to their respective reference values.

In the analysis of leak and rupture probabilities and the sensitivity analysis, the pipe the geometry data, weld stresses, materials properties, crack growth data, leakage limits, inspection and safety barriers were evaluated.

3. Analysis of leak and rupture probabilities

The analysis of leak and rupture probabilities was performed for the welds from BWR reactor small pipes. In this research the stress corrosion cracking as main degradation mechanism was considered. The circumferential, internal semi-elliptic surface crack (majority of SCC piping cracks are of this type, axial orientation is rarer case) in a pipe weld heat-effected zone (HAZ) was evaluated.

In the following fig. 2, the leak and rupture probabilities per year as function of time in operation are presented. Results of analysis demonstrated a clear advantage of ISI which ensures lower leak and rupture probability values. It was received a reduction of about one order of magnitude in leak probability values with inspections of 5 year interval for the BWR pipe welds (Fig. 2).



a)

b)

Figure 2. Results for the cases without inspections and with inspections. The probability per year as a function of time in operation for a) leak and b) pipe rupture.

4. Sensitivity analysis of pipe rupture probability

The sensitivity analysis was performed considering welds of the BWR reactor small pipes. The main influencing parameters of the pipe rupture and inspection were analysed by use of different structural reliability models, considering a range of various dimensions, materials, degradation mechanisms, loading conditions, NDT reliability and inspection procedures.

The sensitivity of rupture probability depending on flaw depth, flaw length, weld residual stress (WRS), flow stress, load level and growth rate of stress corrosion cracking (SCC) was evaluated. The sensitivity analysis results are presented in the following Fig. 3 (a – case with no inspection and b – case with 5 year inspection interval).

In case of no inspection it is observed that a larger flaw depth provides almost negligible effect on pipe rupture probability. It is quite clear considering the small wall thickness (t = 4 mm) for the BWR small pipe welds. Similar trends can also be observed for the flaw length variation as presented in Fig.3. The effect of the flaw length is most significant for the pipe rupture probability with ISI case. As expected, the flaw depth has a larger influence on rupture probabilities when ISI is taken into account. For the part of the flaws (‘Low’ case) the inspection makes it possible to detect and repair the defects, thereby providing the higher relative risk reduction. It can be concluded that variation of the flaw size does provide influence on the rupture probability with ISI case. However, it is important to assess the flaw size with good accuracy in order to decrease an uncertainty and influence on the risk reduction level.

The variation of WRS demonstrates a strong influence on the calculated probabilities suggesting that uncertainty of this parameter should be quantified for a better confidence of probabilistic assessment. However, the importance of WRS for rupture probability is larger than it may be expected. It can be observed in the Fig. 3 that weld residual stresses provide a significant effect on the probability absolute values of both cases, i.e. without and with ISI. A decrease in rupture probability by about 1 order of magnitude can be obtained by having a good control over WRS. This means that a proper validation and control of WRS by itself can provide an alternative strategy for managing risk for rupture in piping. Further risk reduction can be achieved by performing ISI with the appropriate inspection interval.

The sensitivity analysis for the loads (primary loads (P_m, P_b)) variation are performed too. As expected, the variation of loads provided a significant influence on the calculated pipe rupture probability as shown in the Fig. 3. Similar to the effect from WRS distribution, the variation in primary loads gives an influence on the probabilities in both situations; i.e. with and without ISI. The lower loads (‘Low’ case) provide a decrease in rupture probabilities of almost 1 magnitude in comparison to the ‘High’ case. In addition, the ISI performance contributes to further decrease in the rupture probabilities. Thus, in order to decrease an uncertainty associated with the loads and obtain a more realistic risk reduction level it is very important to quantify as much as possible the precise loads in the piping system.

The variation in the flow stress was achieved by the relative change in yield stress and ultimate tensile strength. As expected, the variation of flow stress provided significant influence on the rupture probabilities (Fig. 3). Rupture probability decreases with higher values of flow stress even for the situation without ISI.

The SCC growth rate demonstrated a strong influence on the rupture probabilities. For lower SCC growth rate, corresponding to the 'Low' case in Fig. 3 (a), the pipe rupture probability without ISI was 2.5 magnitudes lower in comparison with the values for the 'High' case. The SCC growth rate is often associated with a substantial uncertainty due to a complex nature of the SCC growth phenomenon.

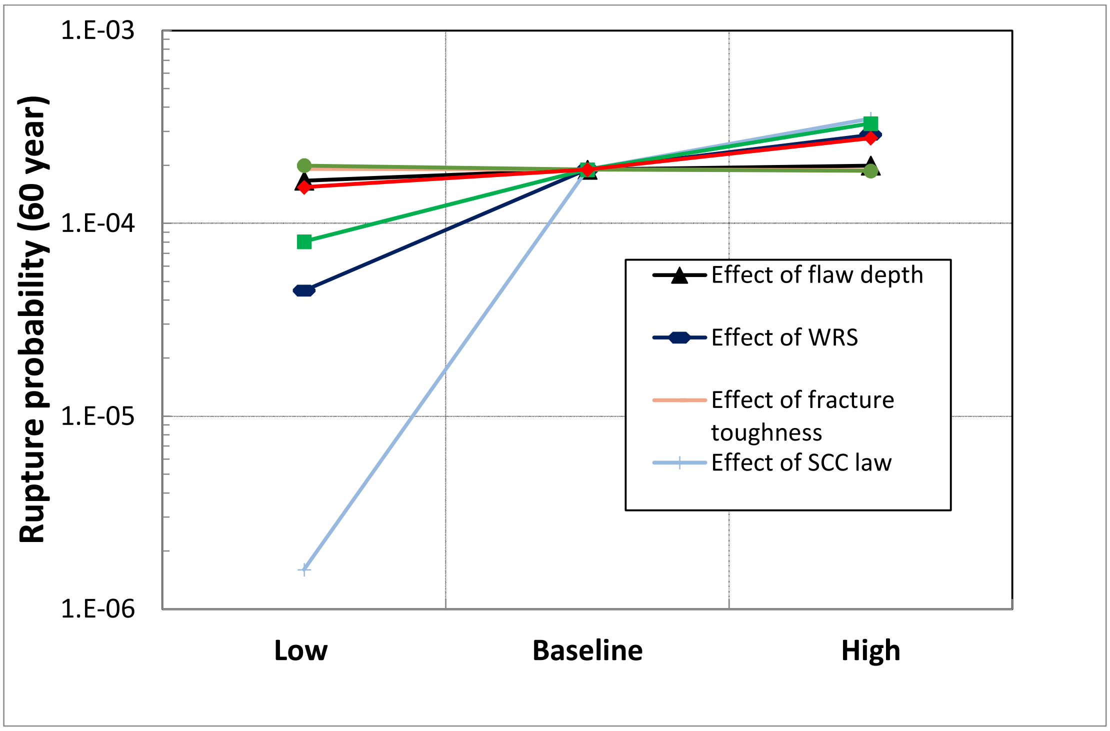
Therefore, this uncertainty is partly managed by ISI. The performance of ISI can contribute to a substantial reduction of the pipe rupture probability. It can also be observed from the Fig. 3 that the rupture probability without ISI for the lower SCC growth rate ('Low' case) corresponds to the rupture probability with ISI obtained for the 'Baseline' case. As expected, for higher SCC growth rate the effect of ISI on the calculated rupture probability becomes less significant, see the Fig. 3.

Fracture toughness governs the critical crack size and therefore, as expected, the variation of fracture toughness provided influence on the rupture probabilities, but not significant (Fig. 3).

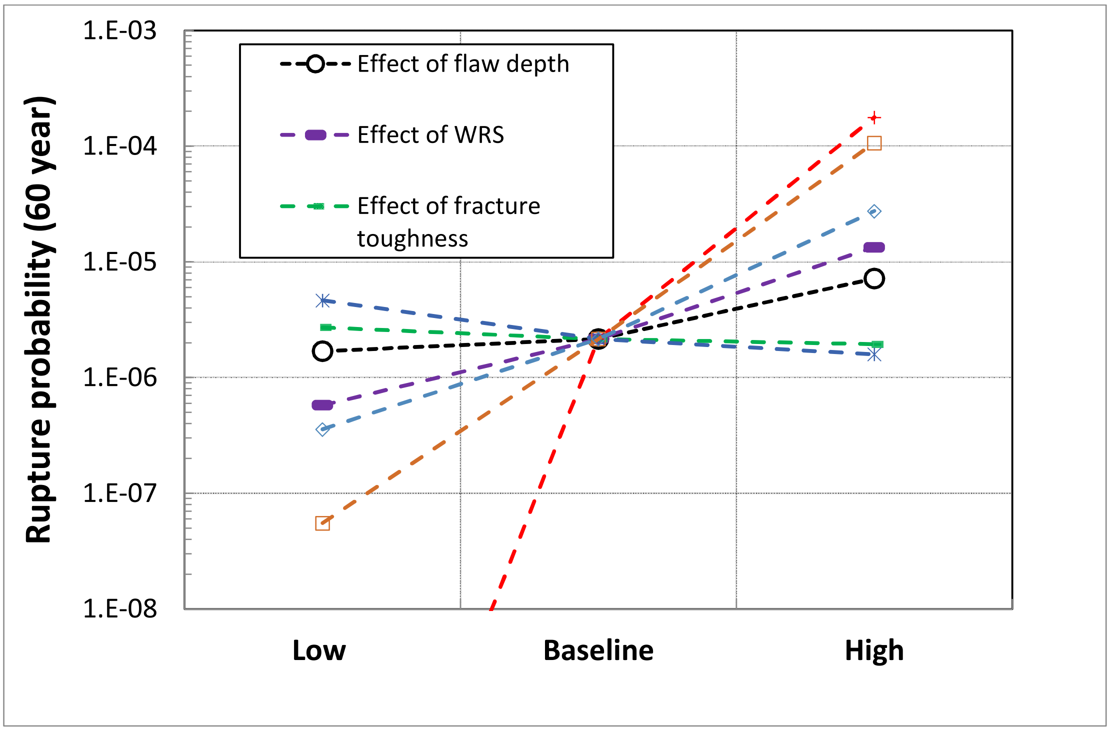
The influence of the ISI efficiency is investigated considering the NDT detection capability quantified in terms of the variation of ISI interval (see Fig. 4). For the rupture probability, the effect of the ISI interval has the strong influence.

The effect of leak detection limit is presented in Fig. 5. Variation of the leak detection limit provides a significant influence on the pipe rupture probability. Thus, the pipe rupture probability can be reduced by 1-2 orders of magnitude ranging from a poor leak detection limit to an advanced leak detection system with the limit of 0.03 kg/s.

This decrease in the rupture probability is obtained for the situation without performing ISI. When the ISI is performed, the rupture probability is even more decreased. It can be observed from Fig. 5 that the rupture probability for a weld with the ISI with 5 year interval and poor leak detection system is about the same as for a weld without the ISI but with good leak detection limit.



a)



b)

Figure 3. The sensitivity of rupture probability depending on flaw depth, flaw length, weld residual stress (WRS), flow stress, load level and growth rate of stress corrosion cracking (SCC), a- no inspection case, b- 5 year inspection interval case.

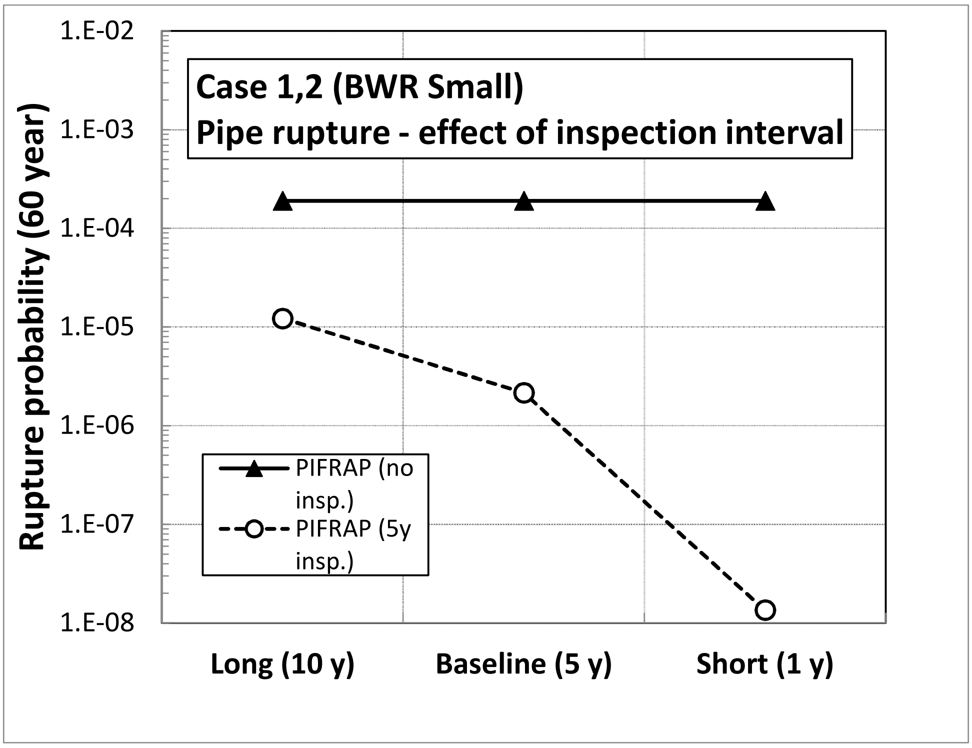


Figure 4. Effect of the ISI interval on the pipe rupture probability.

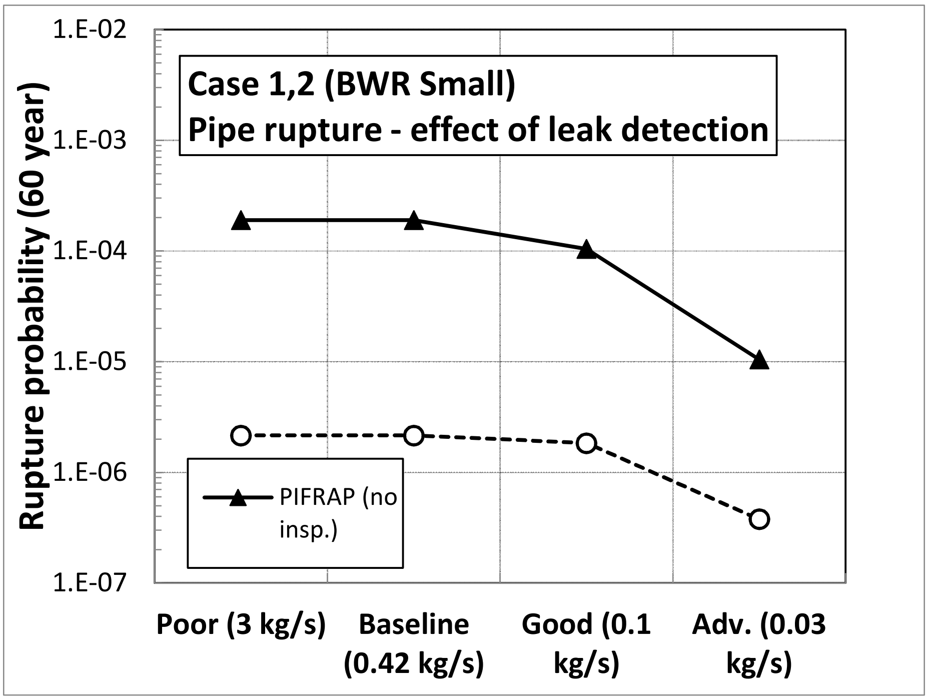


Figure 5. Effect of leak detection on the pipe rupture probability.

5. Summary

The analysis of the effect of the variation of various parameters, including inspection, influencing the probability of pipe rupture was performed. In particular, the sensitivity analysis was performed for the real cases of BWR pipes. Results of analysis demonstrated a clear advantage of ISI which ensures lower leak and rupture probability values. It was received a reduction of about one order of magnitude in leak probability values with 5 year interval between inspections for the BWR pipe welds.

The sensitivity analysis was performed to identify the key influencing parameters under foreseeable variations and uncertain values. The analysis of the effect of the variation of various parameters influencing the probability of pipe leak and rupture was performed. For instance, flaw geometry, weld residual stress, weld loads, flaw stress, stress corrosion cracking growth rate, fracture toughness, ISI efficiency, leak detection limit were considered in the analysis.

The large part of considered parameters demonstrates a strong influence on the calculated probabilities suggesting that uncertainty of these parameters should be quantified for the confidence of probabilistic assessment and practical decision making reducing the chance of pipe rupture.

ACKNOWLEDGMENT

This work was supported by NUGENIA PLUS project “Justification of Risk Reduction through In-Service Inspection” (REDUCE), Grant agreement No: 604965.

References

[1] IAEA Safety guide, No. NS-G-2.6. *Maintenance, Surveillance and In-service Inspection in Nuclear Power Plants.* 2002.

[2] IAEA Nuclear Energy Series, No. NP-T-3.1. *Risk-informed In-service Inspection of Piping Systems of Nuclear Power Plants: Process, Status, Issues and Development.* 2010.

[3] Bergman, M. *PIFRAP user’s manual, version 1.0, SAQ FoU-Report 97/07.* 1997.

[4] Bergman, M., Brickstad, B. & Nilsson, F. *A procedure for estimation of pipe break probabilities due to IGSCC.* SAQ/FoU-Report 97/06. 1997.

[5] Paul, D. D., Ghadiali, N. D., Ahmad, J. & Wilkowski, G. M., *Seepage quantification of upsets in reactor tubes, SQUIRT User’s manual, version* 2.2., Battelle, Columbus, Ohio, USA, 1992.

[6] Ghadiali, N. D. & Wilkowski, G. M., *Effect **of** crack morphology on leak rates,* Summary Report to SAQ Kontroll AB, Battelle, Columbus, Ohio, USA, 1996.

Energy Management Controller of a Resilient Micro-Grid for Critical Buildings

Lenos Hadjidemetriou, Nikolas Flourentzou
KIOS Research and Innovation Centre of Excellence,
University of Cyprus, 1 Panepistimiou Avenue,
20537 Nicosia, Cyprus

Elias Kyriakides
Department of Electrical and Computer Engineering,
University of Cyprus, 1 Panepistimiou Avenue,
20537 Nicosia, Cyprus

Abstract

The continuous growth of electricity demand and ever increasing society aware-ness of climate change issues directly affect the development of the electrical power systems. The adaptation of Renewable Energy Systems (RES) offers reduction to the gas emissions produced by the electricity production from fossil-fuel power generation but also causes vulnerability to the power system. Recent technologies can be embraced to enhance the robustness of electricity supply in critical buildings. This paper proposes a method which uses an advanced control scheme for enhancing the operation of the critical building micro-grid during power-cut by utilizing the RES production. The method offers two different power management strategies (depending on the expected power system recovery time) for a resilient hospital micro-grid that includes RES; achieving longest autonomy of the micro-grid in island mode, or maximizing the load served within the micro-grid. The proposed method will be verified by simulation and selected results will be presented.

Keywords: Critical Infrastructure Protection (CIP), micro-grids, power management, renewable energy sources (RES).

1. Introduction

One of the main objectives of this work is the utilization of the Renewable Energy Systems (RES) in micro-grid, which feeds one or more critical buildings. Two power management strategies are also studied for the micro-grid that can be benefit by maximum autonomy time and maximum load served during islanded operation. The resilience of the micro-grid is considered as priority of the study.

A micro-grid is a cluster of electrical loads with intelligent central management and the ability to operate on power utility mode and/or island mode. Unintentional islanding can result in power quality problems, serious equipment damage, and even safety from hazards to utility operation personnel. Therefore, a modern micro-grid requires active and passive algorithms that can used for islanding detection [1], [2]. This is conventionally achieved by the inverter(s) of RES, however, this paper proposes the Smart Hospital Controller (SHC).

The design and operation of a future electrical power system requires refinement to achieve resilience [3]. The management strategy requires further development when a critical building/load is contained within micro-grid. In the literature, there are major developments in control of power converters in AC micro-grids [4]. Advance techniques for controlling the synchronization of RES to the micro-grid have also been developed [5]. The management of variable sources of power generation and consumption is challenging and requires the involvement of not only the state-of-the-art technologies but also of the consumers [6].

Accordingly, the proposed method offers a solution that automatically priorities the loads according to their criticality. Therefore, the most critical loads assure uninterruptible power supply.

Despite the fact that the power system (which used to be hierarchically and unidirectional controlled), the RES (on both the distribution and the transmission grids), and communication between them (which requires not only physical but also cyber security) are nowadays assumed linked, the quality of service and power stability are actively controlled for local and global objectives [7]. This increases the complexity of the dependencies and proves the necessity of enhanced control strategies. Though [7] emphasise the importance of a main swathe between the micro-grid and the main power line, this paper also proposes load management strategies for better control of distributed generation.

Although the power systems were originally designed for local power supply needs, now are expanding beyond state borders and the power system is assumed a part of larger system [8]. According to the European Commission (EC) preparedness planning, the relevant equipment for ideal configuration on emergency management [9] requires a back-up power, with alternative solutions if the main electricity supply fails. The proposed strategy satisfies the requirements of the EC. The two strategies provide optimized balance between the maximum load served and the longest power supply autonomy for critical loads. These results are achieved by pre-defining the criticality level of the micro-grid loads.

The structure of this paper is as follows. The significance of the paper on next generation infrastructure design is documented in Section 2. The resilient micro-grid architecture along with its smart controller and hospital load categories are thoroughly investigated in Section 3. The power management strategies for achieving significant benefits from RES utilization is analysed in Section 4. Section 5 provides the verification of the controller method and strategies. The conclusion of the paper is provided at the end.

2. Eliminating Micro-Grid Vulnerabilities

Is there a need to increase our interest about the protection and resilience of infrastructures? This interest is strongly related to initiatives, by several governments that from the end of the 90s recognised the relevance of the undisturbed functioning of CI for the wellbeing of their population [10]. According to the policy framework for climate and energy of the European Commission [11] the Member States of the EU need flexibility to choose policies that are best-matched to their national energy mix and preferences. Otherwise, the continuous increase of fossil fuel consumption will not only increase the greenhouse gas emissions, but will also affect the security of energy supply.

The 20-20-20 targets, which are set by [12] aim for a 20% reduction in the overall fossil fuel consumption by the year 2020, compared to 1990 levels. According to the European Distribution System Operators' association (EDSO), Smart grids are a prerequisite to achieving the EU’s ambitious energy and climate objectives to 2020 and beyond. The European Strategic Energy Technology Plan (SET-Plan) aims to accelerate the development and deployment of low-carbon technologies. The European Technology Platform for Electricity Networks of the Future encourages the technology research and development pathways for the smart grids sector. Advancements of information and communication technologies (ICT) cause infrastructure owners to augment current infrastructures with such ICT, [13].

However, the introduction of smart grid technologies will be accompanied with many unexpected situations, which require years of experience to deliver reliable improvements [14].

The transition period, of existing infrastructure to smart grid technology, is critical for emergency buildings/areas (such as hospitals, emergency/crisis management headquarters etc.) where the reliability is a major priority. The method, which is proposed in this paper, offers significant advantages to the existing infrastructure. It introduces a large degree of redundancy and protection while improving the energy efficiency.

The proposed micro-grid is adoptable to the smart grid technologies and gives additional resilience to the next generation infrastructure concept, without compromising the efficiency of power consumption.

3. Micro-Grid Description

This paper focuses on enhancing the operation of a resilient micro-grid for critical buildings. In particular, a large hospital is considered as a case study. This section describes the structure of the hospital micro-grid, its main components and the main power management technique.

3.1 Micro-grid architecture

It is critical to ensure the uninterruptible power supply in a hospital. If the electrical installation of the hospital is designed as a micro-grid, it offers the advantages of being capable for an inter-connected and an islanded operation. To achieve these advantages, a number of technologies is required:

- Battery Storage Systems (BSS),
- Diesel Generators (DG),

- inverter based RES (e.g., photovoltaic systems (PV) and Wind Turbine Systems (WTS)),
- flexible loads, and
- a central controller (Smart Hospital Controller).

The single line diagram of the architecture is shown in Figure 1. In such a micro-grid structure it is assumed that the SHC measures the power exchanged with the grid (P_{GRID}), the power produced by the RES (P_{RES}), the power for charging (negative) or discharging (positive) the BSS (P_{BSS}), the power produced by the DG (P_{DG}) and the power demand by the hospital loads (P_{Load}). Further, it is assumed that hospital loads are flexible and can be controlled (on and off) by the SHC.

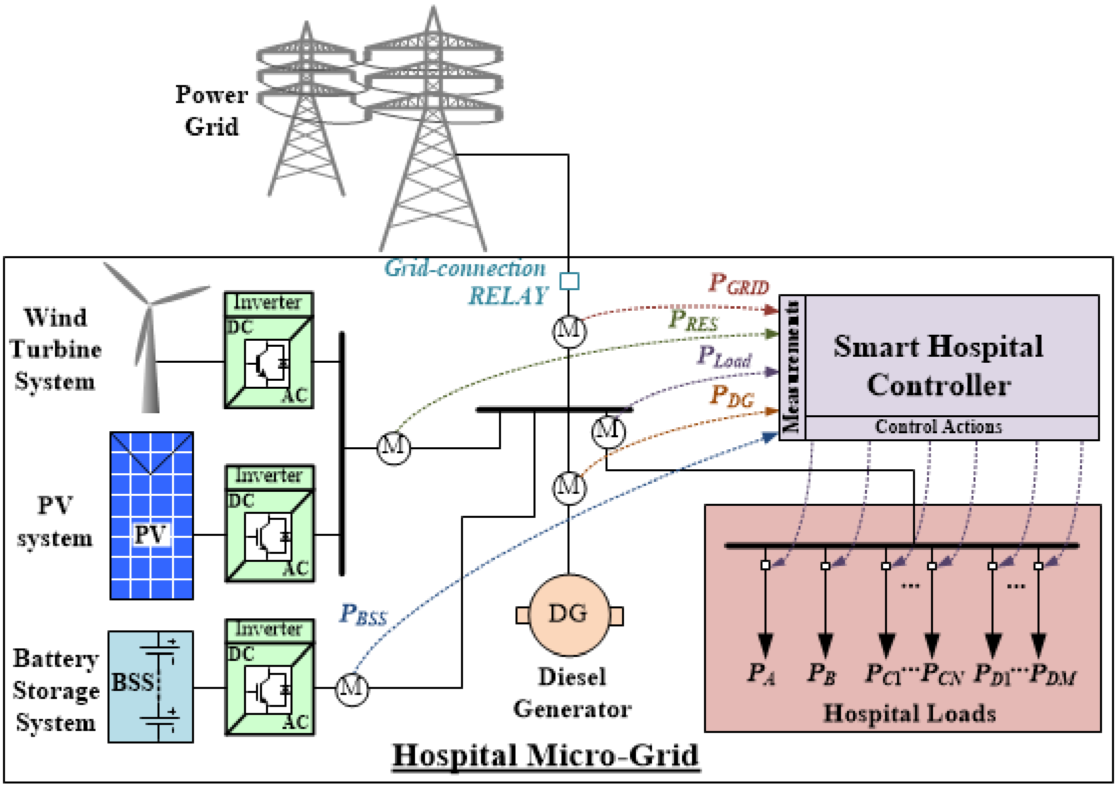


Figure 1. The main architecture of a hospital micro-grid

3.2 Load Categories

The loads of the hospital are divided according to their criticality level, as presented in Figure 2. There are four levels of load criticality, having the equipment with primary significance (e.g., intensive care unit) to be fed by *Level A* and equipment with secondary significance (but still very important) to be fed by *Level B. Level C* is for less crucial loads but still important for the normal operation of the hospital and *Lev-el D* is for the least critical loads that can postpone their operation. *Level C* and *Level D* are more flexible and are divided in *N* and *M* partitions (each partition can be turned on and off by the SHC), respectively, in order to achieve longest autonomy or maximize the load served by the micro-grid. The total hospital load in respect to the energy sources of the micro-grid is characterized by the following equation.

$$P_{Load} = P_{Grid} + P_{DG} + P_{RES} + P_{BSS} \tag{1}$$

The criticality levels are set according to the maximum installed capacity, e.g., *Level A* has maximum installed capacity $\hat{P}_A$ but the actual consumed power (P_A) is less when some equipment of *Level A* are not in use. Similar annotation has been used for the loads in each criticality level. The total hospital load with respect to the load criticality levels is characterized by the following equation:

$$P_{Load} = P_A + P_B + (P_{C1} + P_{C2} + \cdots P_{CN}) + (P_{D1} + P_{D2} + \cdots P_{DM}) \tag{2}$$

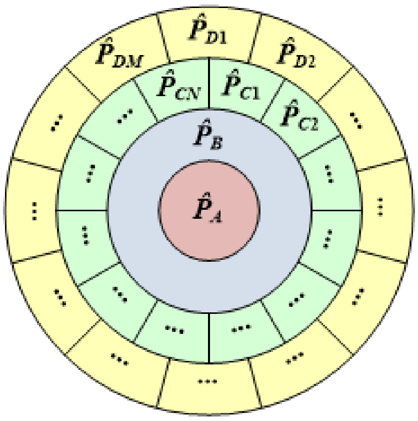


Figure 2. Hospital loads are divided to four levels of load criticality

3.3 Battery storage system

The Energy Capacity EC_{BSS} of the battery is chosen appropriately to satisfy the worst-case scenario:

$$EC_{BSS} \geq t_{start\_up} \cdot \hat{P}_A \tag{3}$$

The power range of the BSS inverter is represented by:

$$\hat{P}_{BSS\_charg} \leq P_{BSS} \leq \hat{P}_{BSS\_discharg} \tag{4}$$

where $\hat{P}_{BSS\_charg}$ is the maximum charging power and $\hat{P}_{BSS\_discharg}$ is the maximum discharging power.

According to the BSS technology for maximizing the battery lifetime, the charging power cannot be more than half of the discharging power.

$$\left|\hat{P}_{BSS\_charg}\right| \leq {}^{\hat{P}_{BSS\_discharg}}\!\big/_{2} \tag{5}$$

Combining (3) and (5) into (4), the inverter of the BSS has the following range:

$$-{}^{\hat{P}_A}\!/_{2} \leq \hat{P}_{BSS} \leq \hat{P}_A \tag{6}$$

3.4 DG and RES

For enabling the islanding and autonomous operation of the hospital micro-grid, at least a DG is required. The power ratings of the DG should be able to serve the loads within *Level A*, *Level B* and *Level C* (Section 2.2) in order to ensure the uninterruptible operation of the hospital during black-outs. Thus, the power-rating of the DG is given by:

$$\hat{P}_{DG} = \hat{P}_A + \hat{P}_B + \sum \hat{P}_{Ci} \tag{7}$$

Where $i = 1,2, \dots N$

The DG is equipped with a fuel tank that gives to a hospital few hours of autonomy without refilling the tank.

For extending the power autonomy of the micro-grid it is useful to have some inverter-based RES. Thus, the distributed power produced by the RES can by very useful either for extending the autonomy of micro-grid or for maximizing the load served during black-outs (as it is presented in Section 3).

3.5 Micro-grid operation

The operational modes of the micro-grid are listed in Table I. In normal operation, the SHC operates in Mode 0. During Mode 0 the hospital is interconnected with the utility, P_{Grid}, and the produced power by the RES is directly injected into the grid, which is the standard practice in conventional grids. The total hospital load in respect to the energy sources of the micro-grid is characterized by the following equation:

$$LS_{Mode0} = P_A + P_B + P_C + P_D = P_{Grid} + P_{RES} \tag{8}$$

Table I: Description of the operation modes of hospital micro-grid

Operation mode	Grid Condition	Micro-grid Operation	Starts	Ends	Comments
Mode 0	Healthy	Interconnected	-	-	Normal Operation
Mode 1	Black-out	Islanding	t_{BO}	$t_{BO} + t_{start-up}$	Time required for the start-up of the DG
Mode 2	Black-out	Islanding	$t_{BO} + t_{start-up}$	$t_{BO} + t_{start-up} + t_{charg}$	Time required for charging the back-up BSS after the DG is connected
Mode 3	Black-out	Islanding	$t_{BO} + t_{start-up} + t_{charg}$	$t_{recover}$	Time until grid is recovered
Mode 0	Healthy	Interconnected	$t_{recover}$	-	Grid is recovered Normal Operation

However, in case of power-cuts and Black-Outs (BO), the hospital micro-grid operation needs to be continued. Therefore, when the BO occurs (t_{BO}) the SHC detects the power-cut and instantly turns-off the Grid-connection Relay in order to proceed with an islanding operation. Immediately, the SHC activates Mode 1. During Mode 1, the inverter of BSS provides power from the battery pack to the hospital demand (positive values of P_{BSS} while the battery pack discharges) in order to serve all the critical loads included in *Level A* (P_A). Mode 1 ends when the DG starts up ($t_{start-up}$).

$$LS_{Mode1} = P_A = P_{BSS} + P_{RES} \tag{9}$$

Then, from $t_{start-up}$ until the t_{charg} (the instant when the State of Charge (SoC) of the BSS returns to 100%) the SHC operates in Mode 2. During Mode 2, the DG is operating and the battery is charging (power flows from the GD to the BSS providing negative values of P_{BSS}). In this mode, the requirements of the SHC are to serve all loads included in *Level A* and *Level B*:

$$LS_{Mode2} = P_A + P_B = \hat{P}_{DG} + P_{BSS} + P_{RES} \tag{10}$$

while P_{BSS} has a negative value.

Mode 3 is the interval from the moment t_{charg} until the recovery of the power grid, $t_{recover}$. During this period, the BSS is not charging or discharging and thus, the load is served mainly by the DG. The *LS* during Mode 3 is represented by:

$$LS_{Mode3} = P_A + P_B + P_C = \hat{P}_{DG} + P_{RES} \tag{11}$$

When the utility is recovered the micro-grid can safely return to interconnected mode (Mode 0).

4 Proposed Power Management Strategies

The SHC is designed to run in two power management strategies. The two strategies manage the use of the RES according to the needs of the hospital and the Black-out recovery time. Both strategies satisfy the requirements of Section 2.

One of the strategies offers the longest possible autonomy time for the micro-grid, which is very useful in cases when the recovery time of the black-out is unknown. The second strategy offers maximum load served which reduces the impact of the black-out on the hospital services. The differences between the two strategies are listed in Table II. The strategies are not applied for Mode 1. During Mode 1 the RES (if they generate any power) are reducing the BSS discharging rate.

Table II: Description of the operation in each mode

Operation mode	BSS	DG	RES	Master	Load Served (LS)	Fuel Consumption
Mode 0	Fully Charged	Not used	P_{RES} is injected into the grid	Grid	Normal Operation	-
Mode 1	Discharging to serve P_A	Starting-up	P_{RES} is used for serving the hospital loads	Inverter	$LS = P_A$	For starting-up the DG
Mode 2A	Charging	Operating	P_{RES} is used for extending the autonomy of DG	DG	$LS = P_A + P_B$	For serving $P_A + P_B - \mathrm{P}_{RES}$
Mode 2B	Charging	Operating	P_{RES} is used for serving extra hospital loads	DG	$LS = P_A + P_B$ $+P_{extra}$	For serving $P_A + P_B$
Mode 3A	Fully Charged	Operating	P_{RES} is used for extending the autonomy of DG	DG	LS $= P_A + P_B + P_C$	For serving $P_A + P_B + P_C - P_{RES}$
Mode 3B	Fully Charged	Operating	P_{RES} is used for serving extra hospital loads	DG	$LS = P_A + P_B$ $+P_C + P_{extra}$	For serving $P_A + P_B + P_C$
Mode 0	Fully Charged	Not used	P_{RES} is injected into the grid	Grid	Normal Operation	-

4.1 Strategy A for longest autonomy

The first power management strategy aims to achieve the longest autonomy possible during island mode. This strategy uses the power generated from RES to save the fuel of the DG. Therefore, the autonomy working time of the DG is extended. The autonomy extension is proportional to the generated P_{RES}. This strategy is preferred when the power system recovery is unknown.

During Mode 2, strategy A ensures power supply in *Level A* and *Level B*. All power generated by RES is used to reduce the power consumption by the DG, and therefore, save some fuel. During Mode 3, strategy A ensures power supply in *Level A*, *Level B* and *Level C*. All power generated by RES is used to reduce the power consumption by the DG, and continue to save some fuel until the utility recovers from the black-out.

This strategy can save a substantial amount of fuel when the power generated from RES is sufficient and it is significant when the black-out lasts for several hours.

4.2 Strategy B for maximum load served

The second power management strategy aims to serve the maximum load possible during the islanding mode. The idea of the strategy is to use the power generated from RES to serve additional loads within the micro-grid. This strategy is applied once the recovery time of the power system is known and the fuel of the GD sufficient until the recovery.

During Mode 2, strategy B ensures power supply in *Level A* and *Level B*. The power generated by RES is used to support additional loads from partitions of *Level C* (e.g., P_{C1}, P_{C1} etc.). Therefore, even when the BSS absorbs power (to charge the battery unit) SHC provides power to *Level C*. During Mode 3, strategy B ensures power supply in *Level A*, *Level B* and *Level C*. The power generated by RES is used to support additional loads from partitions of *Level D* (e.g., P_{D1}, P_{D1} etc.). Therefore, when RES generate full power, the SHC can provide power to even supply *Level D*.

5 Method Verification

The resilient Micro-grid method of Smart Hospital Controller described in Section 2 and the power management strategies described in Section 3 have been investigated using a simulation model in MATLAB. The model uses the values of Table III.

Table III: Design data of the test-bed simulated micro-grid

System	Data
RES	$\hat{P}_{RES} = 30$ kW connected through an inverter During simulation → $43\% < \hat{P}_{RES} < 83\%$
DG	150 kW, Fuel Tank for 6-hour autonomy with a Diversity Factor (DF) equal to 50%
BSS	$\hat{P}_{BSS\_discharg} = 50$ kW, $\hat{P}_{BSS\_charg} = 25$ kW, $EC_{BSS} = 12.5$ kWh
Installed capacity of Hospital Loads	$\hat{P}_A = 50$ kW, $\hat{P}_B = 75$ kW, $\hat{P}_{C1} = 3$ kW, $\hat{P}_{C2} = 4$ kW, $\hat{P}_{C3} = 5$ kW, $\hat{P}_{C4} = 6$ kW, $\hat{P}_{C5} = 7$ kW, $\hat{P}_{D1} = 12$ kW, $\hat{P}_{D2} = 15$ kW, $\hat{P}_{D3} = 18$ kW, $\hat{P}_{D4} = 21$ kW, $\hat{P}_{D5} = 24$ kW.
Diversity Factor (*DF*) of Hospital Loads	$DF_{P_A} = 0.6 \pm 0.2$, $DF_{P_B} = 0.65 \pm 0.15$, $DF_{P_{C1}} = 0.7 \pm 0.1$, $DF_{P_{C2}} = 0.625 \pm 0.125$, $DF_{P_{C3}} = 0.525 \pm 0.075$, $DF_{P_{C4}} = 0.675 \pm 0.075$, $DF_{P_{C5}} = 0.375 \pm 0.025$, $DF_{P_{D1}} = 0.6 \pm 0.1$, $DF_{P_{D2}} = 0.525 \pm 0.125$, $DF_{P_{D3}} = 0.4 \pm 0.1$, $DF_{P_{D4}} = 0.525 \pm 0.075$, $DF_{P_{D5}} = 0.4 \pm 0.05$.
Back-Out (BO) information	Black-Out (BO) occurs at $t = 5$ min Black-Out duration: 150 min

This section provides the results of the micro-grid powers in three cases during blackout. The study covers the graph lines of following values during the four modes:

- Power demand by the hospital,
- Power consumed by the hospital loads,
- Power supplied by the grid,
- Power supplied by the BSS,
- Power generated by the DG, and
- Power generated by the RES.

5.1 BO during the absence of RES

The analysis of a BO incident has been done during the absence of RES. The graphical representation of the results is shown in Figure 3. The graphs verify that the SHC offers uninterruptible supply to *Level A* which includes all the critical loads.

In Mode 2 the loads of *Level B* are supplied and the battery is charged. In Mode 3, all loads up to *Level C* are supplied until the recovery time of the BO.

The curve of the fuel while is consumed is also observed.

5.2 BO with strategy A

The analysis of strategy A has been done when a BO occurs while some RES. The graphical representation of the results is shown in Figure 4.

In Mode 2 the loads of *Level B* are supplied, the battery is charged, and the RES support the DG to save fuel. In Mode 3, all loads up to *Level C* are supplied until the recovery time of the BO.

The fuel slope shows a significant reduction in fuel consumption.

5.3 BO with strategy B

The analysis of strategy B has been done when a BO occurs while some RES. The graphical representation of the results is shown in Figure 5.

In Mode 2 the loads of *Level B* are supplied and some partitions of *Level C* are also supplied, and the battery has been charging. In Mode 3, all loads up to *Level C* and some partitions of *Level D* are supplied until the recovery time of the BO.

The curve of the load served is higher than the previous examples.

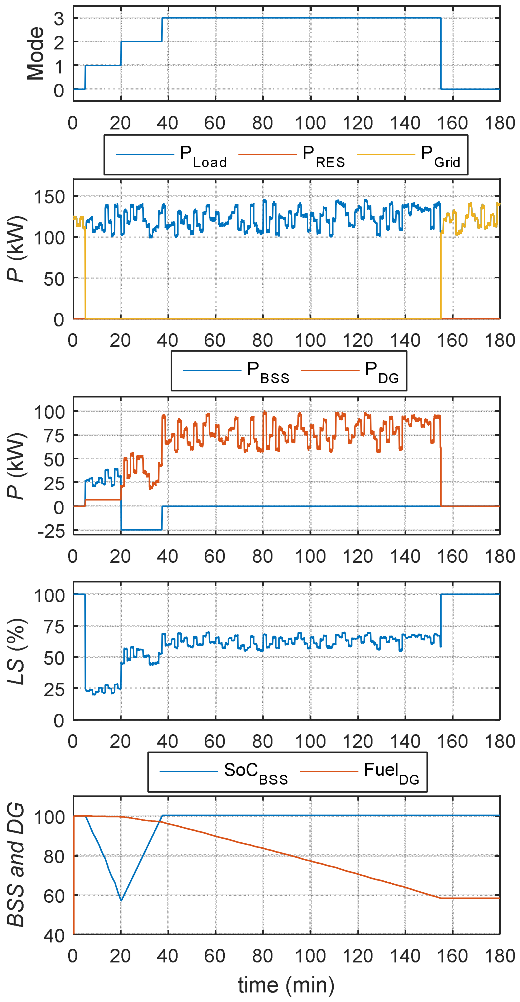


Figure 3. Hospital micro-grid operation when there is no RES production

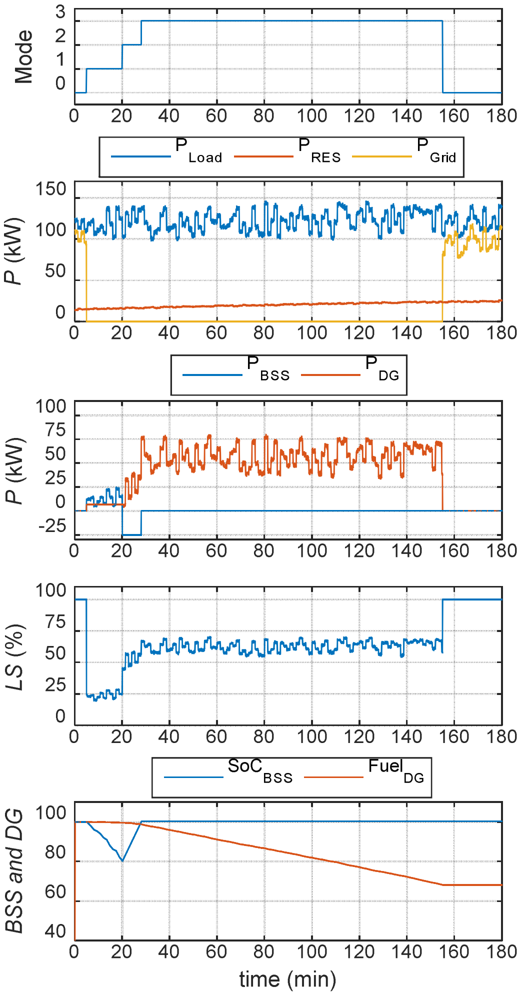


Figure 4. Hospital micro-grid operation when there is a 30 kW installed RES and when the power management strategy A is followed for extending the autonomy of the micro-grid

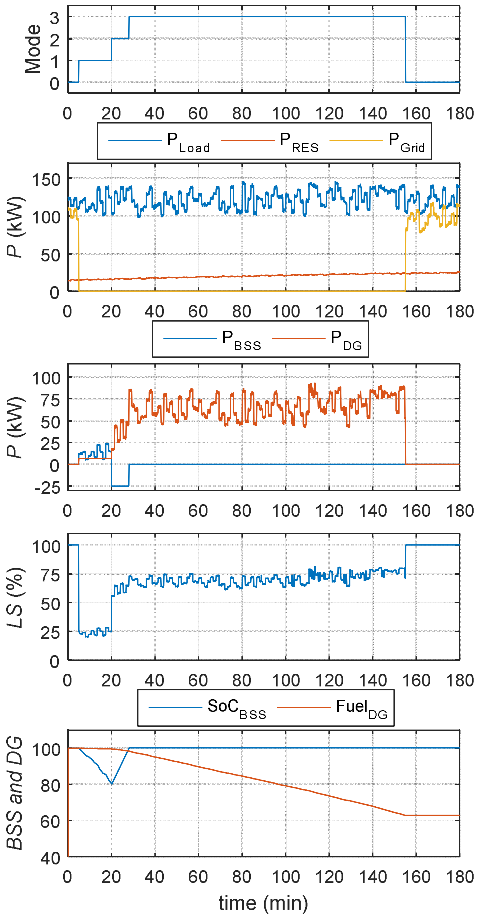


Figure 5. Hospital micro-grid operation when there is a 30 kW installed RES and when the power management strategy B is followed for maximizing the load served

5.4 Summary of the results

The significance of the SHC and the two strategies are shown in Table IV. It is observed that strategy B serves the maximum load and that strategy A saves more fuel.

It is also observed that the RES power support BSS to prevents large discharge of the battery units.

Table IV: Summary of the simulation results

Type of Micro-grid	$P_{RES} = 0$	$P_{RES} = 30$ kW **Strategy A**	$P_{RES} = 30$ kW **Strategy B**
Micro-grid Load Served during black-out (%)	57.7	58.4	65.4
Fuel Tank after Grid restoration (%)	58.3	68.2	62.9
Min SoC of the BSS (%)	57.2	80.3	80.3

6 Conclusion

Without compromising the benefits of the Smart Grid technologies, this paper proposes a method to enhance the resilience and the efficiency of a Micro-grid, towards the targets of the EU. The paper investigates a smart controller which measures and regulates the power demand of a critical building (using a hospital as case-study), the power consumed by the loads, the power supplied by the grid and by the battery system, and the power generated by the additional generator and by the RES.

The paper proposes two different power management strategies for a resilient hospital micro-grid that includes RES. The proposed methods offer an advanced control scheme for enhancing the operation of the hospital micro-grid during power-cut by utilizing the RES production. Depending on the expected power system recovery time, the first strategy reaches extended autonomy of the micro-grid in island mode, while the second strategy served more electrical loads within the micro-grid. The proposed methods were verified by simulation results and selected results were presented.

References

[1] Chen X. and Li Y., "An Islanding Detection Method for Inverter-Based Distributed Generators Based on the Reactive Power Disturbance" in *IEEE Transactions on Power Electronics*, vol. 31, no. 5, May 2016, pp. 3559-3574

[2] Do H.T., Zhang X., Nguyen N.V., Li S.S., and Chu T.T.T., "Passive-Islanding Detection Method Using the Wavelet Packet Transform in Grid-Connected Photovoltaic Systems" in *IEEE Transactions On Power Electronics*, vol. 31, no. 10, Oct. 2016, pp. 6955-6967

[3] Strasser T., Andrén F., Kathan J., Cecati C., Buccella C., Siano P., Leitão P., Zhabelova G., Vyatkin V., Vrba P., Marík V., "A Review of Architectures and Concepts for Intelligence in Future Electric Energy Systems" in *IEEE Transactions on Industrial Electronics*, vol. 62, no. 4, Apr. 2015, pp. 2424-2438

[4] Rocabert J., Luna A., Blaabjerg F., and Rodríguez P., "Control of Power Converters in AC Microgrids", in *IEEE Transactions on Power Electronics*, vol. 27, no. 11, Nov. 2012, pp. 4734-4749

[5] Hadjidemetriou L., Kyriakides E., and Blaabjerg F., "A Robust Synchronization to Enhance the Power Quality of Renewable Energy Systems" in *IEEE Transactions on Industrial Electronics*, vol. 62, no. 8, Aug. 2015, pp. 4858-4868

[6] Meng L., Sanseverino E.R., Luna A., Dragicevic T., Vasquez J.C., Guerrero J.M., "Microgrid supervisory controllers and energy management systems: A literature review" in *Renewable and Sustainable Energy Reviews* 60 (2016) 1263-1273

[7] Monti A. and Ponci F. (2015). Electric Power Systems. In E. Kyriakides and M. Polycarpou (Eds.), Intelligent Monitoring, Control, and Security of Critical

Infrastructure Systems: Studies in Computational Intelligence 565 (pp. 31-65). Berlin, Heidelberg: Springer-Verlag

[8] Korba P. and Hiskens I.A. (2009). Operation and Control of Electrical Power Systems. In M. Jamshidi (Ed.), System of Systems Engineering: Innovations for the 21st Century (pp. 385-408). Hoboken, New Jersey: John Wiley & Sons, Inc.

[9] EC Health and Consumers Directorate-General, "Strategy for Generic Preparedness Planning: technical guidance on generic preparedness planning for public health emergencies", in Public health and Risk Assessment, Apr. 2011.

[10] Setola R., Rosato V., Kyriakides E., Rome E. (Eds.): "Managing the Complexity of Critical Infrastructures A Modelling and Simulation Approach", Series: Studies in Systems, Decision and Control, Vol. 90, Springer, ISBN 978-3-319-51042-2, 2017.

[11] COM (2014) 15 final, A policy framework for climate and energy in the period from 2020 to 2030, Brussels, 22 Jan 2014.

[12] DIRECTIVE 2012/27/EU of the European Parliament and of the Council on energy efficiency, 25 October 2012.

[13] Luiijf, E. "Next Generation Information-Based Infrastructures: New Dependencies and Threats," in: P. Theron (ed.), *Critical Information Infrastructure Protection and Resilience in the ICT Sector*, pp. 304-317, Hershey, PA: IGI Global. doi:10.4018/978-1-4666-2964-6.ch015.

[14] Luiijf, E., "Smartgrids: And the bad news is?," (accepted for publication) in *the International Journal of Critical Infrastructure Protection (IJCIP)*, Elsevier, Sep. 2017.

Security of supply analysis of critical energy infrastructures by flow network approaches

Vytis Kopustinskas, Pavel Praks
European Commission, DG Joint Research Centre, Energy, Transport and Climate Directorate, Energy Security, Distribution and Market Unit
E. Fermi 2749, TP230, 21027 Ispra (VA), Italy

Abstract

The paper describes the flow network methodology approach and the results obtained by the probabilistic gas network simulator ProGasNet software tool. The ProGasNet has been applied to a number of test cases, all based on real gas transmission networks of the EU countries. The ProGasNet model provides an indication of the worst networks nodes in terms of security of supply and provides their numerical ranking. The paper shows an example of bottleneck analysis. The model is very powerful to compare and evaluate different supply options, new network development plans and analyse potential crisis situations. The flow network approach could be applied also to other commodity networks: power grids, water and heat supply networks.

Keywords: energy security, security of supply, gas transmission system, reliability, Monte Carlo.

1. Introduction

The Energy Union package [1] foresees building a resilient and secure energy infrastructure to serve the EU citizens. The EU energy security strategy explicitly defines resilient infrastructure as a backbone of the Energy Union. This is in particular important not only from technical perspective, like transmission network bottlenecks, but also in the light of new threats of this century: cyber-attacks, terrorism or climate change induced natural hazards.

A number of energy supply disruptions due to economic, political or technical reasons highlight the need to study energy infrastructure networks from the security of supply point of view. After consequent gas supply disruptions during 2004-2008 period and the major supply disruption in January 2009 due to the Russia-Ukraine dispute, the European Commission (EC) reacted by issuing Regulation 994/2010 [2] on security of gas supply, which requires the EU Member States to fulfil a number of requirements, including risk assessment, preventive action plan and emergency action plan, installation of cross border reverse flow capabilities, and supply and infrastructure standards based on the N-1 criterion. These and other measures proved to be important for the gas network resilience in a number of subsequent smaller supply disruptions (e.g. Libyan war in 2011, cold snap in early 2012).

In 2014 the EC released energy security strategy [3], highlighting strong EU dependence on imports and in particular on a few importers thus requesting the Member States to develop import diversification measures and emphasizing importance of liquefied natural gas (LNG) import terminals. In addition, the EC Connecting Europe Facility co-funds many energy infrastructure projects developed in particular to enhance security of supply in gas and electricity sectors.

Critical infrastructure (CI) issues have been recently addressed by various initiatives from research institutions and governments worldwide. The European Commission has taken the initiative to organize a network consisting of research and technology organizations within the European Union with interests and capabilities in critical infrastructure protection [4].

The JRC has started to develop an in-house software tool ProGasNet for probabilistic modelling of gas transmission network with the aim to address security of supply issues including network reliability, bottleneck analysis, vulnerability and other aspects. The tool is based on so called flow network approach that is a mathematical way to distribute available resources in the network to the demanding customers by using flow algorithms, many variations of maximum flow algorithm being one of the most popular algorithms in the field. The tool under development at the JRC is applied to natural gas transmission networks, but very similarly it could be applied also to power grids, water or heat distribution networks.

2. Methodology

From the computational point of view, the analysis of large infrastructure networks is very demanding. A review of simulation and analysis of interdependent critical infrastructures is presented in [5]. The literature overview in this field is very large and is growing analysing Cis from many perspectives: topological, flow based or physics based models. This illustrates diversity and complexity of the approaches proposed and problems to be solved.

The development of the ProGasNet software tool targets to address European gas transmission network reliability, risk, security of supply issues, described in detail in the JRC report [6]. The results of the test cases indicate potential of the proposed method for network analysis and the need for further research. The current paper presents some results of the flow network approach.

The ProGasNet uses a distance-based approach of a stochastic network commodity flow model. Priority based commodity supply pattern is based on distances from the source node, so nodes closer to the source are served first. This supply pattern is typical in gas transmission pipeline networks. In each Monte-Carlo simulation step, firstly component failures, especially pipeline failures, are sampled according to an empirical probabilistic law taken, for example, from a failure database. In order to estimate the maximum of transmitted flow from source nodes to sink nodes under reliability and capacity constraints given by the stochastically imperfect elements, which can randomly fail with known failure probabilities, we apply the maximum flow algorithm with multiple sources and multiple sinks. Moreover, in order to identify critical gas supply nodes, which are, under supply crisis conditions, normally geographically far from gas source nodes, we estimate the distance from the virtual source to sink nodes. We use a Dijkstra's algorithm for calculating the distance matrix. Then, we compute a permutation matrix of the graph isomorphism problem according to the distance from the gas source. In this way we transfer the original model to the distance-based approach by a dynamic reordering of nodes and lines of the network graph model [7]. This graph isomorphism task is performed by linear algebra operations. Consequently, we are able to compute the flow matrix of the Maximum flow algorithm. To finish the simulation step, the computed flow matrix is transformed back into the original problem by an inversion linear algebra operation.

Finally, Monte-Carlo simulations are used for estimating that the probability of less than demanded volume of the commodity (for example, gas) is available in selected network nodes. These simulated results are also used for the vulnerability (critical component) analysis. A combination of detected failures leading to the most dominant loss of the available gas is presented and analysed in depth by statistical methods.

3. Test case study

3.1 Description of the study network

Figure 1 shows topology of the test case gas transmission network. It is based on a real regional network topology and data, however location is not displayed. The transmission network topology is represented by a graph with nodes and links (edges).

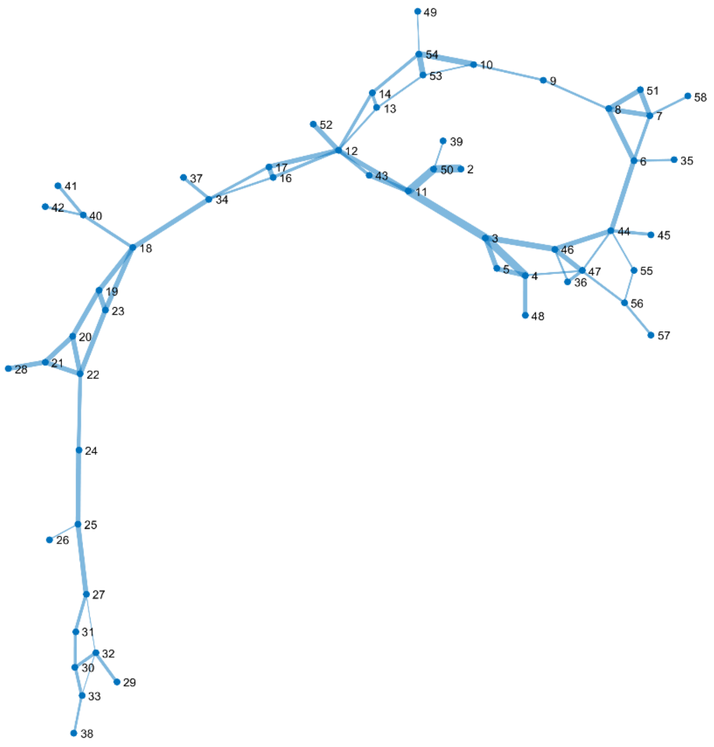


Figure 1. Topological layout of the study network. Thickness of the edges is proportional to the pipeline capacity.

The nodes in a gas network are the following elements:

- Demand nodes (consumers connected to the transmission network;
- Compressor stations;
- Junctions of crossings of several pipelines;
- Supply nodes (storages, LNG terminals, import points at cross-borders).

The node data entered in the model depend on the node type. The demand nodes require only daily demand value (Table I). This value is taken as peak demand value, but it could be also average winter or summer consumption value depending on the purpose of the model.

Table I: Network demand nodes, in millions of cubic meters per day (mcm/d).

Node	Demand	Node	Demand
4	0.1	34	0.5
5	3.2	35	0.1
6	0.1	36	4.2
7	0.3	37	1.3
9	0.1	39	0.3
10	1	41	0.6
13	0.5	42	0.6
17	0.1	43	0.2
18	8.5	44	0.7
20	0.6	45	1.3
25	0.5	47	0.5
26	0.8	48	1.8
27	3	49	0.2
28	6	51	7
30	0.5	52	0.6
33	0.5	53	0.1

Table II shows maximum capacities and type (pipeline, UGS or LNG) of input supply nodes. In case of underground gas storages (UGS), also the output values of not fully loaded storages can be used.

Table II: Maximum supply capacity.

Node	Type	Capacity, mcm/day
2	Pipeline	31
11	Pipeline	7
19	UGS	30
4	Pipeline	4
10	LNG	10.2

The total maximum supply capacity is 82.2 mcm/d. The total network peak demand is 45.8 mcm/d, so the network has certain degree of spare capacity to compensate supply disruptions. All pipeline sections including their estimated capacity and lengths are available in the model, but not shown due to space limitations. For each network component, failure data must be provided. The following components (nodes) are considered for failures with corresponding failure frequencies:

- Compressor station (CS) failure: 2.5E-01/yr;
- Underground storage failure: 1.0E-01/yr
- LNG terminal failure: 1.5E-01/yr
- Pipeline failure: 3.5E-05 /km/yr.

The model considers one month interval for computations. It is assumed that the same peak consumption in the network is constant during this one month period.

The CS failure rate was computed using a typical model of a CS station and industrial reliability data. The UGS failure estimate is an expert estimate. The LNG failure estimate is based on literature references [8]. The pipeline failure rate was taken from pipeline incident database [9] and assuming that rupture occurs 10 less frequently as incident.

The compressor station node is modelled as working or failed (on/off), for each state determining the corresponding capacity of the outgoing pipelines. The capacity reduction due to compressor station failure is normally estimated by hydraulic model computations or expert evaluation. As a consequence due to a CS failure, capacity reduction by 20% of the inlet pipelines and also the outlet pipelines until the next connection node is assumed. This assumption is based on physical flow models, however is not accurate in all cases and also multiple CS failures will have more severe effects on the network operation. Currently physical model is being developed in order to estimate the effect of the CS failures more precisely.

3.2 Security of supply evaluation

The pipeline import sources are not considered to fail due to lack of upstream network model, however they are modelled as on/off elements by scenario analysis. The following main 4 supply scenarios were analysed:

- Scenario A: All currently available sources. Scenario A represents basic scenario when all sources can be used for supply;
- Scenario B: All currently available sources, except Node 10. Scenario B runs the model with Node 10 (LNG) unavailable. This scenario provides an indication of the importance of the terminal for security of supply to the region. Such scenario can happen due to technical failure of the facility or connecting pipelines or failure to deliver LNG by sea;
- Scenario C: All currently available sources, except Node 2 supply. Scenario C models situation when supply from Node 2 is unavailable. This scenario can test the system when the largest supply source is unavailable;
- Scenario D: All currently available sources, except Node 19. Scenario D assumes that Node 19 (UGS) is unavailable due to technical problems, failures

or inability to fill it up during summer period. This scenario is used to demonstrate importance of the storage to the whole network.

The results also display scenarios E/F/G/H which equivalent to scenarios A/B/C/D respectively, but with Node 11 unavailable. This can be used to test importance of the source node 11.

The probabilistic model is run for 1 million times and collects statistical estimates of various parameters in the network. The same results can be presented in different ways: statistical tables, probability tables or cumulative distribution function (CDF) plot. All three types of results are derived from the same sample and represent the same results, but highlights different points of view of the results. The probabilistic and statistical results are computed for a period of one month. For this time period, peak demand is considered to be stable and represent a critical period of severe winter. This assumption is considered to be conservative. Regarding the component failures, no repairs are considered. All failures are considered to occur during a period of one month, although they do not occur at the same moment. This is again a conservative assumption, but as our focus is security of supply, conservative assumptions are widely accepted in the probabilistic studies.

Table III presents probabilistic results for the whole network demand and all scenarios. The network is well supplied in scenarios A/B/E and F, however scenarios D/H and C show obvious vulnerabilities in the network. The results indicate that supply in the region is not homogenous, but fragmented into two areas. The first area is strongly dependent on Node 2 supply source and the second – on Node 19 source. This is very evident because scenario C affects only one area and scenario D affects only the other area. These results are very evident when analysing not the total network supply, but area supply under given scenario. The probabilistic results are available for each scenario, but in the post-processing phase the CDFs are compared by Kolmogorov-Smirnov test and those that are not significantly different are represented by a single line meaning that there are no statistically significant differences among them, e.g. scenarios A/B/E/F in Figure 2. All scenarios supply at least 50% of the demanded gas by the network with acceptable security of supply: probability of having less than 50% of needed gas is in the range of 8E-03 – 2E-06 per month.

Table III: Probabilistic results for the whole network supply for all scenarios (D=45.8 mcm/d). D – demand volume, Mean – average available gas volume.

Scenario	D-Mean	P(X=0)	P(X<0.2D)	P(X<0.5D)	P(X<0.8D)	P(X<D)
DH	12.9	0	1.0E-06	2.4E-04	1	1
C	6.5	0	1.1E-04	8.3E-03	2.2E-02	1
G	0.3	0	0	8.3E-03	2.1E-02	2.7E-02
ABEF	0.1	0	0	2.0E-06	8.5E-03	1.2E-02

The same results can be explored graphically by CDF plots (Figure 2). The plot shows that scenarios D, H and C cannot supply all the needed gas and indicates the available maximum volume of gas. The scenarios A, B, E, F and G can supply all the needed gas, but with different reliability levels. Such results are available for each network node or specified area (e.g. one country, like in Figure 3).

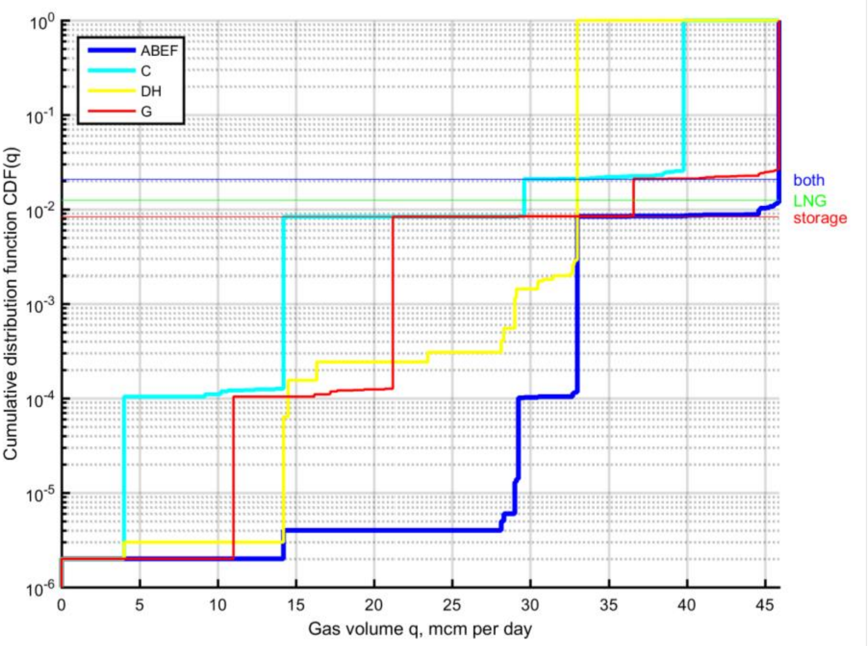


Figure 2. CDF plot for the total network demand of 45.8 mcm/d.

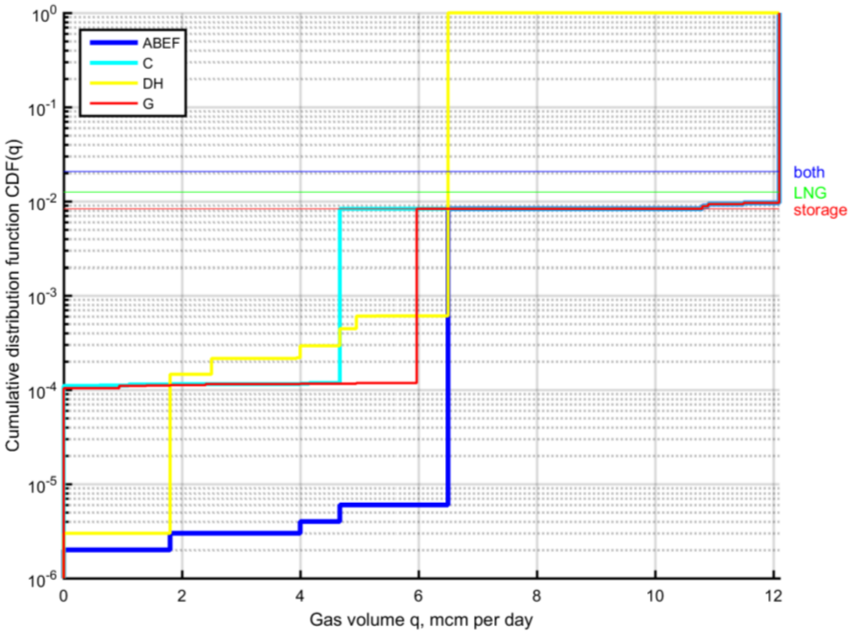


Figure 3. CDF plot for a part of the network (demand 12 mcm/d).

3.3 Bottleneck analysis of the study network

As ProGasNet algorithm computes flows in each network link, bottleneck analysis is a quite straight-forward task. A criterion for a potential bottleneck is pipeline free capacity factor (PFCF) – percentage ratio of the difference between maximum capacity and average flow in the pipeline segment to its maximum capacity eq. (1). The ProGasNet was adjusted to make these calculations for each scenario by aggregating parallel pipelines.

$$PFCF = \frac{Maximum\,Capacity - Average\,Flow}{Maximum\,Capacity} \times 100\% \qquad (1)$$

As a result, no bottlenecks were identified in the scenarios A, B, E and F, as all pipelines had rather high PFCF. However, in scenarios C, D, G and H a number of bottlenecks were identified. The results were filtered not to display source nodes and small pipelines to end users which are sometimes flagged as potential bottlenecks although they are not connecting any other network node. Below, an iterative bottleneck identification process will be described for scenario D:

- Step 1: Pipeline 17->34 (capacity 6.5 mcm/d) has PFCF=0%. Capacity is increased from 6.5 to 15 mcm/d;
- Step 2: Pipeline 34->18 (capacity 12.1 mcm/d) has PFCF=0.6%. Capacity is increased from 12.1 to 15 mcm/d;
- Step 3: Pipeline 17->34 (capacity 15 mcm/d) has PFCF=0.7%. Capacity is increased from 15 to 18 mcm/d;
- Step 4: Pipeline 34->18 (capacity 15 mcm/d) has PFCF=1.3%. Capacity is increased from 15 to 18 mcm/d;
- Step5: Pipeline 10->9->8 (capacity 2.8 mcm/d) has PFCF=1.2%. Capacity is increased from 2.8 to 5 mcm/d;
- Step 6: Pipeline 10->9->8 (capacity 5 mcm/d) has PFCF=1.4%. Capacity is increased from 5 to 8 mcm/d;
- Step 7: The calculations used values the previous step. No more potential bottlenecks were identified.

As clear from the above steps, some pipelines appear as bottlenecks several times after virtual increase of other pipelines capacity. Steps 5 and 6 indicate that selection of a new virtual capacity is a problem and might require several trials. Figure 3 shows the effect of Steps 1-2-4-7 to the whole network and the same network area as in Fig.2. The whole network benefits from all the process steps 1-7, however for the selected network area there is no statistically significant difference among the steps 2-7: the supply situation cannot be longer improved in that part of the network. Similarly, the results can be analysed for all the demand nodes and areas.

The bottleneck analysis iterative process for scenario C runs as follows:

- Step 1: Pipeline 34->17 (capacity 6.2 mcm/d) has PFCF=0.9%. Capacity is increased from 6.2 to 12 mcm/d;
- Step 2: Pipeline 18->34 (capacity 12.1 mcm/d) has PFCF=1.3%. Capacity is increased from 12.1 to 15 mcm/d;

- Step 3: Pipeline 34->17 (capacity 12 mcm/d) has PFCF=0.9%. Capacity is increased from 12 to 15 mcm/d;
- Step 4: The calculations used values the previous step. No more potential bottlenecks were identified.

Interestingly, bottleneck analysis for scenarios C and D identifies the pipelines 18-34-17 as major bi-directional bottlenecks in the network. This finding confirms the conclusion that the network is not homogenous and supply nodes 2 and 19 supply two different parts of the network with a bottleneck connection between them. Note that under normal operation condition of the network, no bottlenecks were identified and they appear only when major supply nodes are unavailable.

Scenarios G and H identify almost identical connections as bottlenecks, connection 18-34-17 being the most significant. This suggests that planned new connection in Node 11 might not be fully utilised by the network consumers due to existing bottlenecks in the system.

The other identified congested segments are limited by the source supply capacity which is outside the control of the system operator and require either expensive supply infrastructure development solutions or international agreements.

4. Concluding remarks

The paper describes the flow network methodology approach and the results obtained by the probabilistic gas network simulator ProGasNet software tool. The ProGasNet has been applied to real gas transmission networks of several EU countries however geographical information cannot be disclosed.

The ProGasNet model provides an indication of the worst networks nodes in terms of security of supply and provides their numerical ranking. It is recommended to use the results of the model in a qualitative (comparative) way rather than interpret numerical values directly. The model is very powerful to compare and evaluate different supply options, new network development plans and analyse potential crisis situations.

The model has a number of advantages and limitations that must be considered by interpreting the results. The model at this stage cannot model adequately consequences of failures of compressor stations. Currently, it is assumed that pipeline capacity is reduced by 20% in the nearest section, however this assumption needs to be validated by physical flow computations. Failures of two nearby compressor stations would have severe effect on the network capacity, but this event is not considered in the current version of the probabilistic model. Further work is needed to overcome these limitations.

References

[1] Energy Union Package. A Framework Strategy for a Resilient Energy Union with a Forward-Looking Climate Change Policy (2015). COM(2015) 80 final, Brussels, Belgium.

[2] EU Regulation (2010) Regulation No.994/2010 of the European Parliament and of the Council of 20 October 2010 concerning measures to safeguard security of gas supply and repealing Council Directive 2004/67/EC. Official Journal of the European Union, Luxembourg.

[3] European Energy Security Strategy (2014). Communication from the Commission to the European Parliament and the Council. COM(2014) 330 final. Brussels, Belgium.

[4] Lewis, A.M., et al. (2013) European Reference Network for Critical Infrastructure Protection, Int. J. Crit. Infrastruct. Protect., vol. 6, pp. 51-60.

[5] Ouyang, M. (2014) Review on modeling and simulation of interdependent critical infrastructure systems, Reliab. Eng. Syst. Saf., vol. 121, pp. 43-60.

[6] Kopustinskas, V. and Praks, P. (2014) Vulnerability, reliability and security of supply modelling of a gas transmission network, JRC technical report JRC93545, European Commission, Luxembourg.

[7] Deo, N. (2008) Graph Theory with Applications to Engineering with Computer Science. Prentice Hall.

[8] Jung, M.J., et al. (2003) “LNG terminal design feedback from operator’s practical improvements”, The 22nd World Gas Congress proceedings, Tokyo, Japan.

[9] EGIG report, (2011) 8th Report of the European Gas Pipeline Incident Data Group. Groningen.

Vulnerability Analysis methodology: The expected number of heavy storms and flood vulnerability prediction model of Rio de Janeiro city

Author 1: Dr. Eduardo Calixto
ECC (Eduardo Calixto Consultant)
Ravensburger Straße 12
89079, Ulm, Germany

Author 2: Dr. Gilson Brito Lima Alves
LATEC-UFF-Engineer University-Production Department
São Domingos 156
24210-240, - Niterói / Rio de Janeiro, Brazil

Abstract

The society's vulnerability to natural disasters is increasing since the environment, climate changing in the last 10 years. Nevertheless, the vulnerability perception of the society, including the public and private sector leaders is still low which can be realized based on the last catastrophic natural disaster events around the globe. Therefore, the first step in a direction to increase the authorities and leader vulnerability perception is to assess the expected number of future natural disasters as well as their consequences. In order to provide a methodology to approach this problem the paper proposes the prediction of the expected number of natural disasters based on the Crow AMSSA model as well as the final prediction of the vulnerability based on Bow Tie analysis. The vulnerability criteria are also proposed as a baseline to support leader to take decision regarding the necessity to reduce their vulnerability face of natural disasters.

Keywords: Vulnerability, expected number of storms, mean time between storms, Acceptable vulnerability, Bow Tie model.

1. Introduction

The Vulnerability is defined as a lack of protection or fragility that one system has and can be exploited by external forces. Such lack of protection or fragile are related to external events like nature catastrophes, security information and terrorism attacks or internal events like sabotage.

In case of Systems' infrastructure, vulnerability describes how a system faces problems to carry out its intended function when exposed to materialized threats (Hofmann, 2012). The vulnerability of critical infrastructures as shown in figure 1 can be divided into several dimensions to form a general framework for analyzing vulnerability that is:

- Threat / hazard and unwanted event;
- Exposure;
- Susceptibility;
- Coping capacity;
- Criticality.

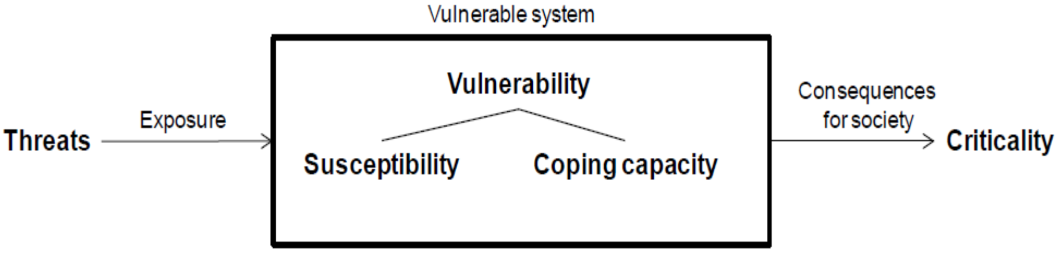


Figure 1: General Vulnerability Framework

Source: Hofmann, 2012.

Threat can be defined as any event with the potential to cause some damage to systems, society and environment. Threats can be categorized into nature/weather related threats, human threats and operational conditions threats. A threat may lead to an unwanted event, understood as a disruption of the system. The vulnerability regards threat susceptibility and loss of coping capacity. Concerning infrastructures, the susceptibility succeeds if a threat leads to a disruption in the system and is depending on, for instance the technical components, the working force and the organization.

On the system level, other factors like institutional and social factors also have an influence on the susceptibility. A system is susceptible towards a threat if the threat leads to an unwanted event in the system. The coping capacity describes the ability of the system itself to cope with an unwanted event, limit negative effects, and restore the function of the system to a normal state. The coping capacity can also be understood as resilience.

2. Natural disaster

Nature catastrophes are events triggered by nature forces like tsunamis, hurricanes, tornados, volcanic eruptions, earthquakes, thunderstorms and universe space threats (Woo 1999). Whenever such event occurs, industrial accident and public infrastructure rupture may take place which has extreme consequences for the whole society such as flooding area, transportation service disruption, environmental impact, health damages and death.

Throughout history, natural disasters have exacted a heavy toll of death and suffering and are increasing worldwide (Reyes, 2006). During the past 34 years, they have claimed about four million lives worldwide, adversely affected the lives of at least a billion more people, and resulted in property damage exceeding $50 billion (Guha-Sapir and Lechat 1986).

In general terms, in case of disaster events (natural catastrophes, terrorism attacks, sabotage) we need to consider the application tools and our entities of interest to define impact and the most appropriated response to mitigate such disastrous effect. The figure 2 below summaries issues that must be considered in respect to the vulnerability of the system.

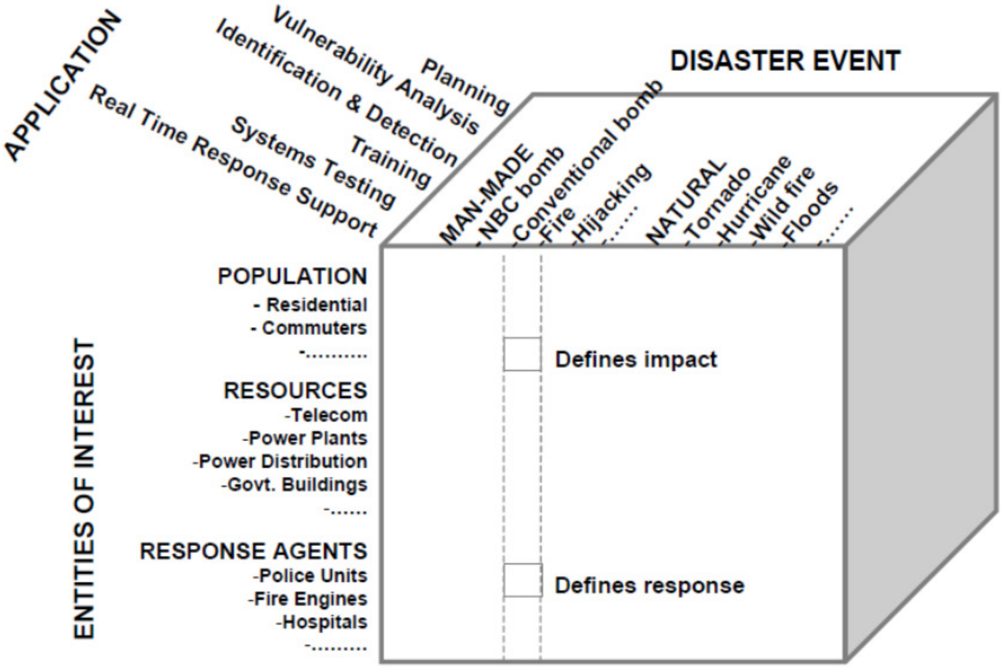


Figure 2: Integrated Emergency Response Framework (IERF) proposed by NIST

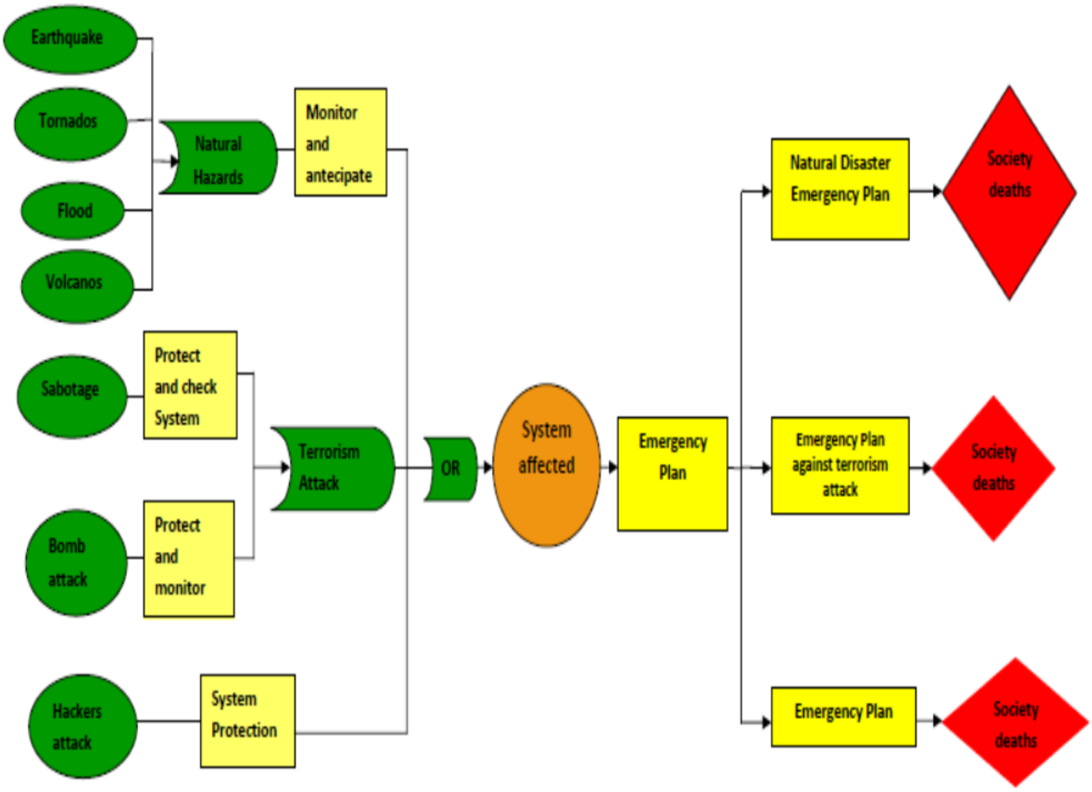
Source: Jain and McLean, 2003.

Considering that such threats really exist in the world, it is necessary to have a measure of system vulnerabilities to monitor and mitigate the susceptibility of the system and avoid the bad consequence for the whole society.

3. Vulnerability model

In order to consider all vulnerabilities such as the disaster event, entities of interest and their impact, it is necessary to have a model. A model is a representation of some reality in the real world which enables us an easier understanding and predict. Therefore, to model the natural disaster vulnerability, the Bow Tie model is proposed as shows figure 3. The Bow Tie methodology is usually applied to a risk analysis which considers on the left diagram side the probable cause of the incident, the incident in the middle and the consequences on the right size. Among the causes and incident are the control measures and between incidence and consequences are the recovery measures.

In case of vulnerability analysis, the causes are threats like natural disasters, terrorism attack and hacker's attacks. The control measures are protecting, check, monitoring and anticipate actions. The incident is the susceptibility of threats and recover measures a coping capacity to mitigate threats' effects. The figure 3 shows a Bow Tie model which describes the vulnerability of generic systems like industrial plants, trains, commercial building and aircrafts.



🟩 Potential Causes (exposure)
🟨 Control Measures
🟧 Loss of Control (susceptibility)
🟨 Recovery Measure (coping capacity)
🟥 Consequences

Figure 3: Bow Tie Vulnerability Analysis. Source: Calixto E, et al 2016.

The threats events can have multiple effects on different systems on the same location, in other words, city state or country. Because of that, is necessary to have a complete Vulnerability analysis considering all systems affected because is necessary for prior which location requires support and which kind of support. Therefore, a Multi Bow Tie is a more appropriate model and allows accessing all threats' effects on different systems with different consequences. The figure 4 shows the Multi Bow Tie model to have a complete Vulnerability analysis.

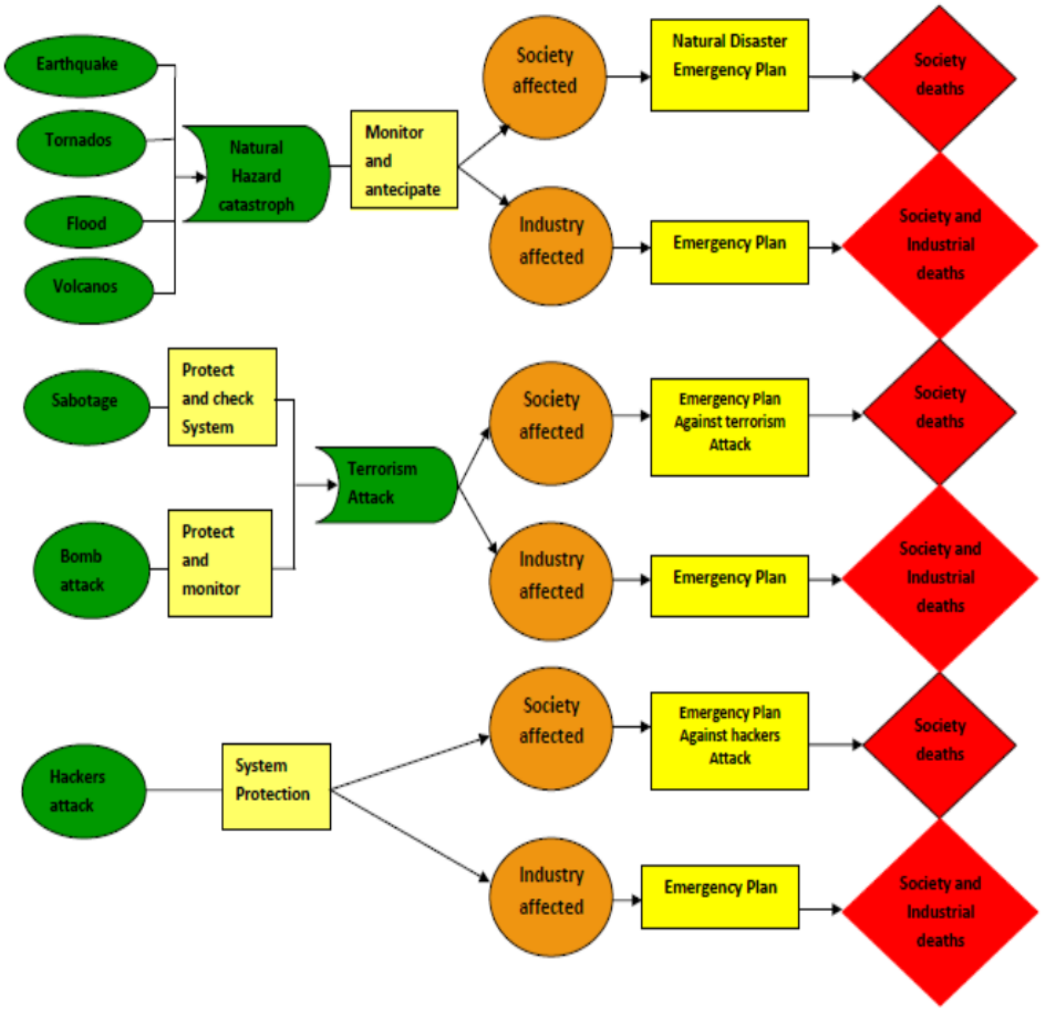


Figure 4: Multi Bow Tie Model for Vulnerability Analysis. Source: Calixto, et al 2016.

Considering that threats can affect system and society, it is necessary to consider different susceptibility for each threat group (Natural catastrophes, Terrorism Attack and Hackers Attacks). In addition, different emergency plans will be carried out depending on threat characteristics.

4. Vulnerability prediction

The vulnerability can be defined qualitatively as the capacity of a certain threat to be susceptible to a system or society and cause a negative impact in this system or society.

The system susceptibility can be described mathematically by the number of times that the threat tries to enter into the system and succeed during an interval of time t. Therefore, the susceptibility is a combination of threats number of success and control measures failure probabilities (coping failure probability). By this way, the System Susceptibility is defined in (1):

$$S_i = ENT_{t_i} \times CM_{i_j} \qquad (1)$$

$Where$:
i= threat
i=0, 1,2... n
j= threat´s control measure
J=0, 1,2... m
$S_i = System\ suceptibiliy$
$ENT_{t_i} = Expected\ Number\ of\ threat\ at\ time\ t$
$CM_{i_j} =$ Threat control measure failure probability

Since the threat is susceptible to the system, which means the control measure failed, the coping capacity is the last layer of protection to avoid that such threat causes a damage to the system or society. Therefore, the system or society's vulnerability is defined in (2):

$$V_{SO_i} = S_i \times CO_{i_k} \times END_i \qquad (2)$$

$Where$:
i= threat
i=0, 1,2... n
k= susceptibility´s coping capacity
k=0, 1,2... m
$V_{SO_i} = Society\ vulnerabiliy$
$S_i = System\ suceptibiliy$
$CO_{i_k} =$ Copy capacity failure probability
$END_i = Expected\ Number\ of\ deaths$

Depending on type of threat, it´s possible to mitigate the vulnerability by reducing the threat susceptibility success by increasing the control measure effectiveness or by increasing the coping capacity success. In case of natural catastrophes, it´s hard to reduce the susceptibility success by reducing the frequency of natural disaster or by avoiding their effect on systems. In this case, the control measure are not so efficient to reduce the threat susceptibility but it´s possible to mitigate the society's vulnerability by increasing the coping capacity, such as an effective emergency alarms evacuation and emergency response, which will lead the population to a safe place with low number of casualties. Concerning the natural disaster, the most effective vulnerability mitigation is to avoid as much as possible the threat consequences by dislocating the population to a safe place before the threat susceptibility takes place.

By the other hands, others threat like terrorism attack and hacker attach, the more effective is to reduce the susceptibility by monitoring the threats and reduce the frequency that such threats penetrate into the system. Once such threat is susceptible is very hard to predict or avoid the intended damage to the system or society.

Considering that different threats like Natural disasters, terrorism attacks and hacker attacks can affect society or Industrial plants in the same interval of time, the Multi

Bow Tie Model described in item 3, will consider such multi effect. Consequently, the Total vulnerability is the sum of all vulnerabilities as defined in (3).

$$V_f = \sum_{i=1}^{n} V_{so_i} \qquad (3)$$

$$V_f = \sum_{i=1}^{n} S_i \times CO_{i_k} \times END_i$$

$Where$:
Vf = final vulnerability

After defining the vulnerability, is also important to estimate properly the expected number of susceptible threats to help emergency response and security teams have a target and keep such number as low as possible. By this way it is possible to define the expected number of susceptibility in (4).

Let $N(t)$be the cumulative number of failures observed in cumulative test time t, and let $\rho(t)$be the failure intensity for the Crow-AMSAA model. Under the NHPP model, $\rho(t)\Delta t$ is approximately the probably of a failure occurring over the interval $[t, t+\Delta t]$for small Δt . In addition, the expected number of failures experienced over the test interval $[0, T]$under the Crow-AMSAA model is given by (Crow, L.H., 1974):

$$E[N(T)] = \int_0^T \rho(t)\, dt \qquad (4)$$

The Crow AMSAA Model assumes that the intensity of the event is approximately Weibull event rate, thus intensifying of event on time defined in (5):

$$\rho(t) = \frac{\beta}{\eta^{\beta}} T^{\beta-1} \qquad (5)$$

Considering the initial event rate as:

$$\lambda_i = \frac{1}{\eta^{\beta}} \qquad (6)$$

If we consider the event as a threat, the cumulative threat rate is approximately threat intensity we have:

$$\lambda_c = \beta \lambda_i T^{\beta-1} \qquad (7)$$

$$E(N) = \lambda_i T^{\beta} \qquad (8)$$

When β=1,

$$E(N) = \lambda_i T \qquad (9)$$

Where:
$E(N_s)$=Expected Number of susceptible threats
$\lambda_i = Initial\ failure\ intensity$
T=Accumulated time

The equation above describes the threat intensity and depends on β value its increase, decrease on keeping constant along time. Is very important to have in mind that β in Crow AMSSA Model describes threat intensity behaviour and have not relation with Weibull distribution shape parameter. In fact, β is a shape parameter of threat Intensity Function in Crow AMSSA Model. Thus, in this model when β>1 means higher threat because threat intensity is increasing, in other words, the frequency of threats increases and control measures and coping measures actions are not reducing the vulnerability. When β<1, threat intensity is decreasing along time, in other words, threats frequency is reduced or control measures and coping measures actions are reducing the vulnerability. When β=1, the threat intensity is not getting higher or lower.

To find the variable value in Crow AMSSA method, it is necessary to find the maximum value related to one parameter and that is achieved by performing partial derivation of the equation as follows:

$$\frac{\partial(\wedge)}{\partial(\theta_j)} = 0$$
$$j = 1,2,3,4...n$$

Applying the maximum likelihood method, we have (Crow, L.H., 1974):

$$f(T) = \frac{\beta}{\eta}\left(\frac{T_i}{\eta}\right)^{\beta-1} e^{-\lambda_i T_i^{\beta}} = \beta\frac{1}{\eta^{\beta}} T_i^{\beta-1} e^{-\lambda_i T_i^{\beta}} = \beta\lambda_i T_i^{\beta-1} e^{-\lambda_i T_i^{\beta}} \qquad (10)$$

$$L = \prod_{i=0}^{N} f(T) = \prod_{i=0}^{N} \beta\lambda_i T_i^{\beta-1} e^{-\lambda_i T^{\beta}} = \beta^N \lambda_i^N e^{-\lambda_i T^{\beta}} (\beta-1)\prod_{i=0}^{N} T_i$$
$$\Lambda = Ln(L)$$
$$\Lambda = Ln\left(\beta^N \lambda_i^N e^{-\lambda_i T^{\beta}} (\beta-1)\prod_{i=0}^{N} T_i\right) = NLn(\beta) + NLn(\lambda_i) - \lambda_i T^{\beta} + Ln(\beta-1) + \sum_{0}^{N} Ln(T_i)$$

$$\frac{\partial}{\partial\lambda_i}\Lambda = \frac{N}{\lambda_i} - T^{\beta} = 0 \qquad \text{Then,} \qquad \lambda_i = \frac{N}{T^{\beta}}$$

$$\frac{\partial}{\partial\beta}\Lambda = \frac{1}{\beta} - \lambda_i T^{\beta} Ln(T) + \sum_{0}^{N} Ln(T_i) = 0 \qquad \text{Then,} \qquad \beta = \frac{N}{NLn(T) - \sum_{0}^{N} LN(T_i)}$$

This paper proposes that the expected number of catastrophic consequences in a cumulative time must be between 0 and 0.1 to be acceptable. The different qualitative vulnerability class is defined in the table 1. Therefore, we can consider low vulnerability for values between 0 and 0.1, moderate vulnerability value between 0.1 and 0.5, high vulnerability for values between 0.5 and 0.7, very high vulnerability for value between 0.7 and 1 and unacceptable vulnerability for values equal or higher than 1.

Even in case of low vulnerability, the threat monitoring and data updated must be continuous but is not necessary for mitigations actions implementations.

In case of high and very high vulnerability is necessary not only for monitoring the threats but also to improve the existing control measures or implement additional control measures as well as coping capacity improvement to achieve a low vulnerability level whenever is feasible. In case of high or very high vulnerability it is necessary to monitoring the threat and try to eliminate or block them whenever it´s possible, improve existing control measures and coping capacity as well as implement new ones when the mitigation actions are not enough.

In addition, to mitigate the system and the society threat effect is recommended to shut down or isolate systems and dislocate the possible affected society to a safer location as much as possible.

Table 1 - Vulnerability Indexes and classification

Vulnerability Indexes	**Vulnerability Class**	**Vulnerability consequence**
≥1	Unacceptable	One or more deaths.
0.7≤Vi<1	Very High	Expected number of deaths very close to 1.
0.5 ≤Vi<0.7	High	Expected number of death close to 1.
0.1≤Vi<0.5	Moderate	Moderate expected number of deaths.
Vi<0.1	Low	Very low expected number of deaths.

In fact, if coping capacities are not able to eliminate threats, there will be consequences and society, industrial population or both will be affected. By this way, is also important to estimate the number of deaths, causalities and cost caused by threats to have complete consequence analysis of vulnerability effect. Thus, the vulnerability related to such threats can be measured by the combination of threat susceptibility with the expected number of deaths, causalities or cost. Concerning the number of deaths, it´s important to have a perception of the whole society's tolerance of such threats' effects. In fact, there's no any acceptance vulnerability criterion for events such as natural catastrophes, terrorism attack and hacker attacks. Nowadays and is a worldwide concept that as lower as possible better will be to the whole society.

5. Vulnerability methodology application: Rio de Janeiro Flood natural disaster

Once of the most frequent natural disaster which affect a large number of population every year around the globe is flood caused by heavy storms. In South America, it´s also a reality and especially in Rio de Janeiro, Brazil, this event has been intensified in the last ten years.

The first flood cause by heavy storms in Rio de Janeiro is dated in 1711 when no emergency response and neither report about such natural disaster was done. The two realities between the past 300 years and the last 10 years in Rio de Janeiro is the population density, which grew up specially in the last 50 years. As many of the main cities in South America such as Sao Paulo, Lima, Rio de Janeiro, Santiago, Caracás, Bogota e Buenos Aires, the high number of the population lives under bad social and economic conditions, which force a high percentage of such population to live in inappropriate and dangerous areas. In the case of Rio de Janeiro, huge part of the population, approximately 1.5 million people, around 24% of the population, live in favelas. Such reality is even worse in terms of vulnerability, because most of the favelas are on hills. Such areas have a high risk of landslides caused by heavy Storms which is facilitated by vegetation devastation which is motivated by houses construction as shows figure 5.

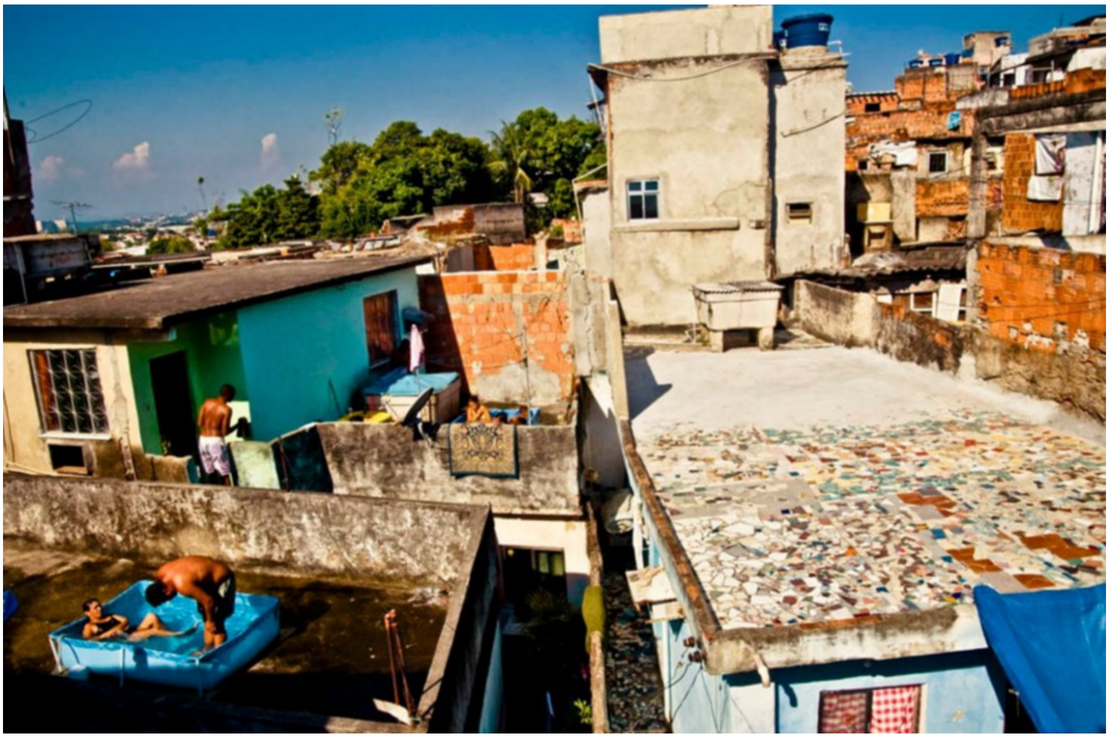


Figure 5: Rio de Janeiro Favela. Source: Calixto, et al 2016.

In order to define the natural disaster vulnerability, which in Rio de Janeiro city is a Heavy storm vulnerability, the last seventy years with the eleven worse heavy storms are summarized in table 2.

Table 2 – Heavy Storms in Rio de Janeiro effect (1966 – 2016)

Storm date	Concurrent Data	MTBE	Disaster description	Deaths	Injures	Families houses destroyed	Economy Losses
01/01/1966	255	0.00	Heavy Storm and flood area	250	Not defined	50 000	Not defined
01/01/1967	256	1.00	Laranjeira Hill slides	200	300	Not defined	Not defined
01/03/1982	271	15.00	Pau da Bandeira Hill landslides	6	Not defined	2	Not defined
20/03/1983	272	1.00	Heavy Storm and flood area	23	Not defined	150	Not defined
01/01/1987	276	4.00	Serrana Hill Region landslides	292	Not defined	20000	Not defined
01/02/1988	277	1.00	Serrana Hill Region land slides	289	734	18560	Not defined
01/01/1999	288	11.00	Serrana Hill Region land slides	41	72	180	Not defined
01/02/2003	292	4.00	Serrana Hill Region land slides	36	95	1693	Not defined
01/04/2010	299	7.00	Bumba Hill landslides	264	Not defined	Not defined	Not defined
14/01/2011	300	1.00	Serrana Hill Region land slides	1000	Not defined	14000	$300.000.000
09/01/2016	305	5.00	Heavy Storm and flood area	250	1000	50000	Not defined

Based on table 2 description, is noticed that the intensity of heavy rains has been increasing in the last fifty years and unfortunately, the consequence of the society has been catastrophic with a huge number of deaths and injured population, population without houses and economic losses. The main concern now is when the next failure will go to happen, and to predict vulnerability, the first step is to calculate the time when the next heavy storms will occur. The table 3 shows the summarized calculation of the CROW AMSSA model parameters based on the methodology description on the item 4 and the information defined in table 2.

Table 3 – Expected Number of Heavy Storms in Rio de Janeiro prediction basis.

N	T	b	λi	d	λc	N(t)	MTBFi
1	16	2.7725887	0.12618	0.227874402	2.64E-02	1.089	7.925
2	17	2.8332133	0.13288	-0.254969115	2.78E-02	1.219	7.526
3	21	3.0445224	0.15913	-0.377184473	3.33E-02	1.803	6.284
4	22	3.0910425	0.16557	-0.411144177	3.46E-02	1.966	6.040
5	33	3.4965076	0.23401	-0.871608438	4.89E-02	4.167	4.273
6	37	3.6109179	0.25800	-1.077460618	5.40E-02	5.151	3.876
7	44	3.7841896	0.29910	-1.485437273	6.26E-02	7.102	3.343
8	45	3.8066625	0.30489	-1.548606109	6.38E-02	7.404	3.280
9	50	3.912023	0.33357	-1.882510643	6.98E-02	9.000	2.998

The Crow AMSAA parameters base on table 3 are:

$$\beta = \frac{N}{NLnT - \sum_{i=0}^{N} LnT_i} = 1{,}85$$

$$\lambda_i = \frac{N}{T^{\beta}} = 0{,}006394$$

The time to have the next heavy storm is defined by the equation (11).

$$E(N_s) = \lambda_i \mathrm{T}^{\beta} \qquad (11)$$

$$T = \left(\frac{E(N_s)}{\lambda_i}\right)^{\frac{1}{\beta}} = \left(\frac{10}{0.006394}\right)^{\frac{1}{185}} = 52.9\ years \cong 53 \text{ years}$$

For the current time of 50 years (2016), we have nine failures. Therefore, in 3 years' time the next failure will happen as shows the figure 6.

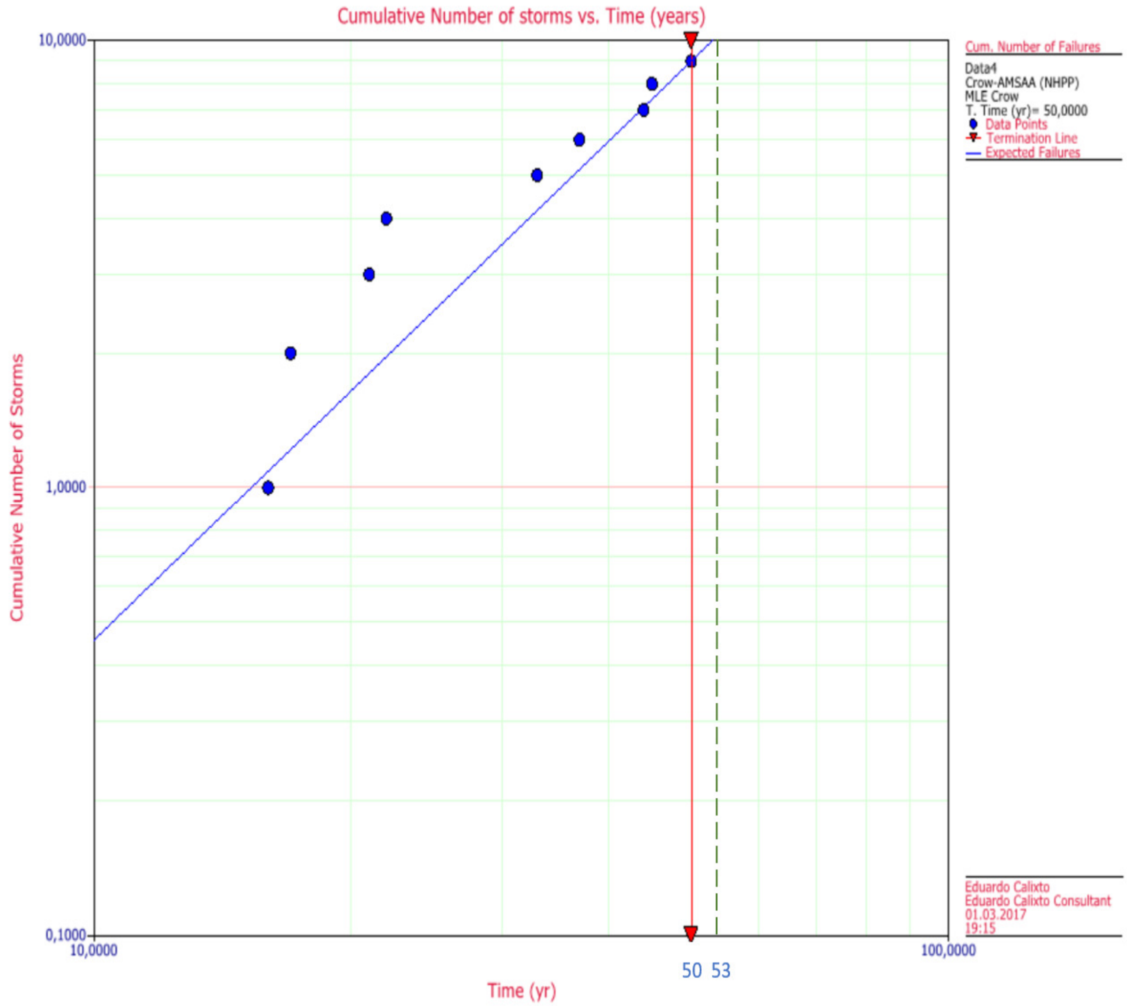


Figure 6: Cumulative number of Storms.

The confirmation of the increased number of heavy storms is demonstrated in the figure 7 which shows the decreasing interval between heavy storms (MTBS). Therefore, for the next three years it is expected to have one heavy storm, which will lead to such catastrophic consequences for the Rio de Janeiro society. The vulnerability calculation considers also the mitigation event's probability. Therefore, the Bow Tie model is applied to define the vulnerability of heavy storms based on the following definition:

- Potential Causes (exposure): Heavy Storm
- Control Measures (Control Measures): Monitoring weather, emergency alert and population reallocation
- Loss of Control (susceptibility): Probability of heavy rain affects the Rio de Janeiro city
- Recovery Measures (coping capacity): Emergency response
- Consequences: Deaths

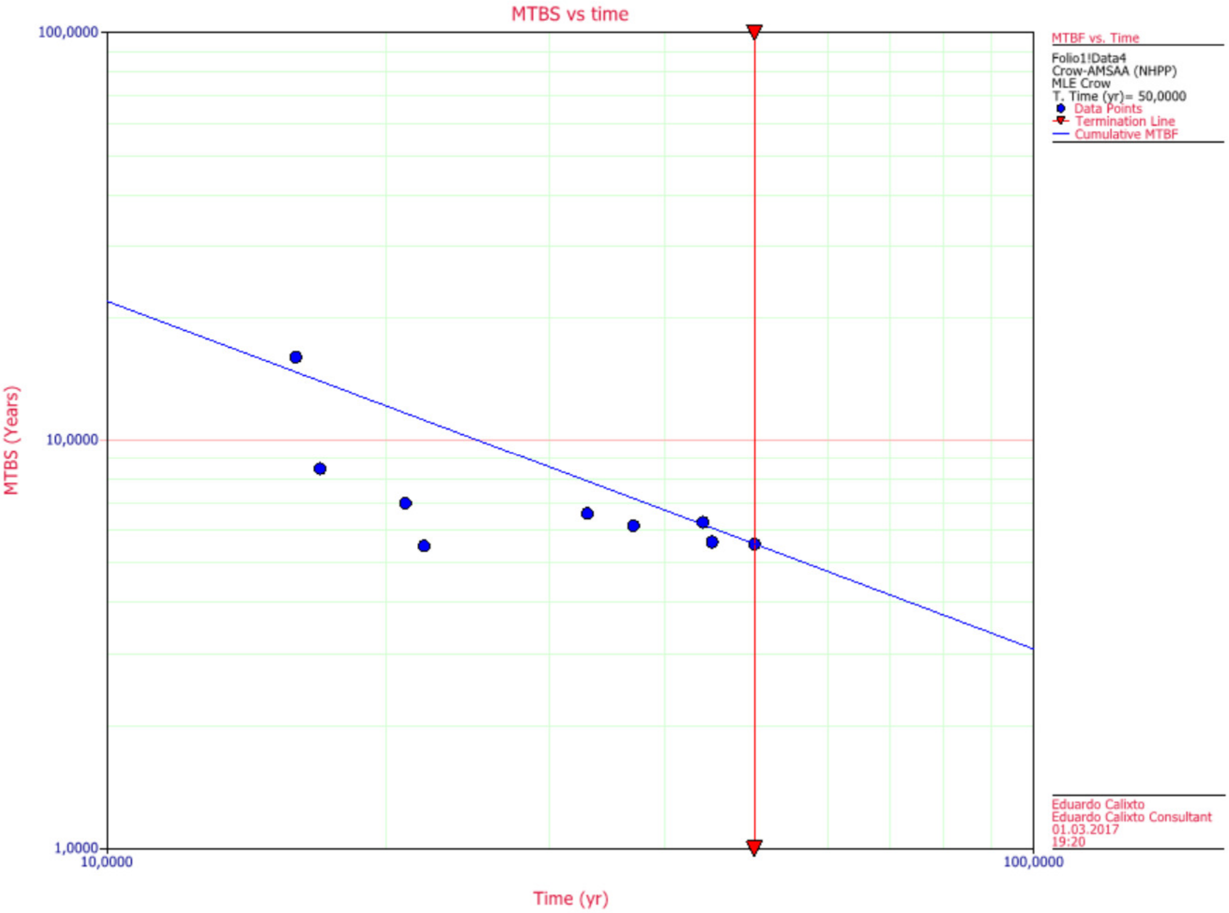


Figure 7: Mean Time Between Storms tendency.

Concerning the next five years, the expected number of heavy rain is 1.7, the following Bow Tie elements which the probability of failures values is defined below as:

- Potential Causes (exposure): Heavy Storm = 1.0
- Control Measures 1(Control Measures): Weather Monitoring and Alert = 100%
- Control Measures 2(Control Measures): Population reallocation = 100%
- Loss of Control (susceptibility): Probability of heavy rain affects the Rio de Janeiro city =100%
- Recovery Measures (coping capacity): Emergency response = 100%
- Consequences: Deaths = at least 1

The figure 8 below shows the Bow Tie model for the heavy storm in Rio de Janeiro.

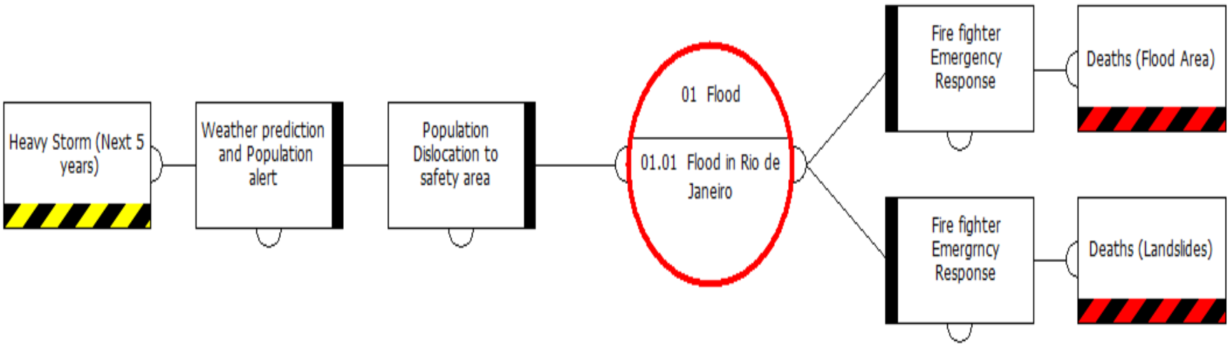

Heavy Storm (Next 5 years)
Weather prediction and Population alert
Population Dislocation to safety area
01 Flood
01.01 Flood in Rio de Janeiro
Fire fighter Emergency Response
Fire fighter Emergrncy Response
Deaths (Flood Area)
Deaths (Landslides)

Figure 8: Heavy storm Vulnerability.

Vulnerability = ENHS x CM1 X CM2 X Co1x END

Where:
ENHS=expected number of heavy storms
CM1 = Probability of control measure 1 (weather prediction and alert) failure
CM2 = Probability of control measures 2 (Dislocation to safety area) failure
Co1=Probability of Coping capacity (Fire Fighters emergency response) failure
END=expected number of deaths

Vulnerability = 1,0 x 1 (100%) x1 (100%) x 1 (100%) x1= 1 death in the next three years

It´s important to understand why the control measures and the coping capacity has 100% of failure for the last 10 years. Concerning the weather prediction and alert, it has not been effective because the limited weather prediction technology in Rio de Janeiro state as well as the ineffectiveness of the population alert.

In case of heavy storm detection on time, it´s not possible to dislocate the population for a safe area because there´s not enough available area for the 1.5 million of people who live in vulnerable areas in Favelas in the Rio de Janeiro state. In addition, most of the population are afraid to leave their homes being no more permitted to return to their homes after the natural disaster.

Regarding the coping capacity´s effectiveness, as we consider that only one death will bring the vulnerability level to an unacceptable level, despite the Rio de Janeiro fire fighters effectiveness during emergency response, they have not enough resource to avoid all deaths.

The expected number of deaths is very conservative when we look to the table 2 which shows the lowest number of deaths (six) occurred on 01-03-1982. In this case that was done to show how vulnerable the population is based on the final vulnerability number. In other words, even considering the lowest possible number of deaths, the vulnerability is still unacceptable.

6. Conclusion

The vulnerability of heavy storms in Rio de Janeiro analysis faces 2 natural disasters for the next three years. In order to reduce such vulnerability and bring this number of acceptable level, which means Moderate class, it´s necessary that the population be dislocated to a safe area in Rio de Janeiro city as well as the emergency plan effectiveness improves to be able to set up the alarm in risk areas in case of heavy rains and dislocate as much as possible the remain population to a safe place. In this direction, it´s necessary in a short time frame to develop a National Disaster Emergency Plan, which enable to coordinate resources to the affected area as much as possible and involve government authorities and local companies which would supply resources during this natural disaster. In long time period, it's necessary to dislocate the whole population in a safe area. That is the most effective action to reduce the vulnerability. Nevertheless, that involves investment to build new popular houses in safe areas of Rio de Janeiro with all necessary infrastructure for the population. As much as such population is dislocate to safe areas lower will be the vulnerability of the population to heavy storms.

References

Calixto E. Safety Science: Methods to Prevent Incident and worker Health Damage at Workplace. Bentham Science: DOI: 10.2174/97816080595221150101 http://www.benthamscience.com/ebooks/forthcomingtitles.htm

Crow, L.H., 1974. Reliability analysis for complex repairable systems. In: Proschan, F., Senfling, R.J. (Eds.), Reliability and Biometry. SIAM, Philadelphia, p. 379.

Guha Sapir, D., and Lechat, M.F. (1986). Reducing the impact of natural disasters: Why aren’t we better prepared? Health Policy and Plng., 1, 118.

Hofmann, M., Kjølle, G. and Gjerde, O., 2012, "Development of indicators to monitor vulnerabilities in power systems", Proceedings PSAM11 & ESREL 2012, Helsinki.

Jain, Sanjay and McLean, Charles R. (2003). Modeling and Simulation for Emergency Response: Workshop Report, Standards and Tools. Modeling and Simulation for Emergency Response Workshop. NISTIR 7071, December 2003. http://www.mel.nist.gov/msidlibrary/doc/nistir7071.pdf

Santos-Reyes, J.R. (2006). Edge Hill railway accident: A systemic analysis. Safety and Reliability for Managing Risk – Guedes Soares & Zio (eds).© 2006 Taylor & Francis Group, London, ISBN 0-415-41620-5

Woo, G. 1999. The mathematics of Natural Catastrophes. Imperial College. ISBN 1-86094-182 6

A methodological approach for assessing the resilience of the interconnected EU critical infrastructures to climate change

Theodoros Katopodis, Athanasios Sfetsos, Stelios Karozis, Georgios Karavokyros, Georgios Eftychidis, Georgios Leventakis, Ralf Hedel, Ifigenia Koutiva, Costantinos Makropoulos

INRASTES, NCSR Demokritos
Patr. Gregoriou E' & 27, Neapoleos str.
15341, Agia Paraskevi, Greece

Author 5: Georgios Eftychidis, Author 6: Georgios Leventakis
Center for Security Studies
P. Kanellopoulou 4
101 77, Athens, Greece

Author 7: Ralf Hedel
Fraunhofer Institute for Transportation and Infrastructure Systems
Dresden, Germany

Author 8: Ifigenia Koutiva, Costantinos Makropoulos
School of Civil Engineering, NTUA
Athens, Greece

Abstract

This paper introduces a methodological approach for identifying the resilience of interconnected EU critical infrastructures to climate change. The proposed approach tries to establish a consequence based modelling framework for assessing climate dependent causal relationships between CI operation and response to climate impacts with an aim to minimise disruptions to service flows under diverse conditions. The proposed approach also introduces a risk propagation element for capturing how heterogeneous CI are interconnected and interdependent and further expanded to introduce the element of resilience capabilities.

Keywords. Risk assessment ● Interconnection analysis ● Holistic impact anaysis ● European critical infrastructures ● Climate Change

1. Introduction

The main scope of the proposed approach is to propose a scientifically verified framework to estimate the resilience of critical infrastructures to climatic hazards. The proposed framework builds upon a comprehensive assessment of multiple climate risks and related natural hazards, such as floods, forest fires, droughts, etc. According to the recently published IPCC AR5 report1, climate change-related risks to infrastructures are increasing (including rising sea levels and storm surges, heat stress, extreme precipitation, inland and coastal flooding, landslides, drought, …) with widespread negative impacts on people (and their health, livelihoods and assets) and on local and national economies and ecosystems (WGII AR5 - Chap8, summary).

As CI are critical components to the normal functioning of modern EU societies, their resilience encompasses the operational component in addition to its structural integrity and its capacity to maximize business output under climate stressors. Critical infrastructures are commonly designed, built and maintained according to rigorous standards (CEN, 2014, 2007; Silvia Dimova et al., 2015) in order to withstand the climate and weather-related pressures, but shifts in climate characteristics may result in increases of the magnitude and frequency of potential risks, or expose specific CI to new risks not previously considered. A main objective of the proposed methodology is to provide scientific evidence in better understanding how future climate regimes might affect the interconnected CI during their lifespan accounting for the element of ageing, and assess the cost-effectiveness of different adaptation measures.

The increasingly dependent, interdependent and interconnected nature of European critical infrastructures exposes previously unseen risks, new vulnerabilities and opportunities for disruption across the CI networks. Current analysis of historical incidents indicates that CI vulnerability tend to be focused on extreme weather events that can disrupt the normal operation of infrastructures, while on the other hand causes impacts across infrastructures because of extensive interdependencies between them (DOE, 2012). Acknowledging that infrastructure's vulnerabilities and impacts go far beyond physical damages (Angela Queste and Dr. Wolfram Geier, 2005; Hokstad et al., 2012) our approach will provide an assessment of the impacts to the services provided by CI, addressing impacts associated with business continuity and also include the externalities of the infrastructures operation, societal costs, environmental effects, and economic costs due to suspended activities.

2. Relevant policies

Our proposed methodological framework is based on a synthesis of various policies for providing validated scientific support for national and European policies;

- The EU Strategy on Climate adaptation, as identified in COM(2013) 216 (EC, 2013a)- An EU Strategy on adaptation to climate change, and detailed in SWD (2013) 137 (EC, 2013b)- Adapting infrastructure to climate change

[1] http://www.ipcc.ch/report/ar5/

- National Risk Assessment Plans (NRA) as identified in SWD (2014) 134, Brussels, 8.4.2014 (EC, 2014), where CI have been identified as a national priority in several countries (DE, NL, IE,…)
- Directive 2008/114/EC (EC, 2008), on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, 8.12.2008
- Reports by the IPCC[2].

A synthesis of the above policy documents introduces to our approach the following elements:

1. The protection of CI is a collaborative process, where any change in its properties and operational characteristics to combat extreme weather phenomena shall by no means compromise other functions such as security levels, health and safety operations, and vice versa.
2. According to the "all hazards" approach, risk assessment should include any type of risk whether is man-made, technological accident or stemming from natural causes including climate related events, in a way that will allow prioritization of risk.
3. Risk Assessment should be comparable across sectors and diversified to capture the unique nature and characteristics of each CI type, whereas impacts should include as common best practices from NRA and Dir 114/2008.
4. As CI are projects scheduled to last for decades, the ageing element should be an inherent part of the analysis.

Additionally, a core component of our proposed methodological approach is to introduce the interdependencies of heterogeneous types of CI into this analysis.

3. State of the art review

The number of available methodologies and funded projects in risk assessment for CI is large. The majority of funded projects is focused on assessing impacts specific to certain types of infrastructures and with different scope and time frame of the analysis. Another complicated issue pertains to the complexity of the interconnected infrastructures (Bollinger et al., 2013), relating to the time and computational expressiveness of a modeling system to effectively analyze risk and resilience across large networks.

3.1 Past Research Projects

A number of past and on-going research projects focus on the performance and response of urban areas to natural disasters, even if they do not always make specific and direct reference to CI analysis. Research projects with impacts related to natural hazards & climate change in the same manner include ARMONIA (511208) MEDIGRID (FP6-2003-Global-2-004044) project, Na.RAs, EPSON, ENSURE (FP7/212045), FUME (FP7/243888), WEATHER project (233886), EWENT (233919), CLIM-RUN project (FP7-ENVIRONMENT 265192). Other ones are fo-

[2] https://www.ipcc.ch/report/ar5/

cused on the impacts on the urban environment, and CI such as RESIN (653522), PLACCARD (653255),

CIPRNET (312450), INFRARISK (603960), INTACT (606799), RAIN (608166), STREST (603389).

On a national scale several approaches and guidance documents exist such as the German from BMI (Protecting Critical Infrastructures – Risk and Crisis Management), the Dutch DHM (De Haagse Methodiek – The Hague Method) and NRB (Nasjonalt risikobilde - Norwegian national risk chart), the CPNI/UK Civil Contigencies Act, and the Norwegian Risk Vulnerability Analysis. Although all of them do focus on the analysis of a single infrastructure and most of them are fairly simplistic and guided by expert opinions & CI security officers, the general trend is to move towards a holistic protection framework rather than a basic risk analysis.

3.2 Brief overview

A set of quantitative probabilistic risk analysis of a single CI, such as the Risk and Vulnerability Analysis, the Preliminary Hazard Analysis (PHA), Probabilistic Safety Analysis and Quantitative Risk Analysis has been proposed but require specialized knowledge to be applied (Utne et al., 2011), while (Haimes et al., 2002) offer a methodological framework that identifies, prioritizes, assesses and manages risks to complex, large-scale systems. HAZUS-MH[3] is the main risk assessment tool used by FEMA.

(Rinaldi et al., 2001) first tried to model the interdependencies of CI as highly interconnected and mutually dependent systems, both physically and through a host of information and communications technologies. In recent years, some of the most prominent approaches are the following:

- Event-driven simulation, which mimic the behavior of their real-life counterparts, and prioritizing a queue as a buffer mechanism used to store a representation of "events" that are about to happen. (IRRIIS (128735), DIESIS (212830))
- Input – Output: The supply and demand approach represented though “nodes and edges” producing, consuming and transferring resources of the CI. (I2SIm simulator)
- Network based Markov-chain techniques are used in order to capture and model the change of state of interconnected infrastructures (Ouyang et al., 2009)
- Object oriented models, with close adherence to the reality of the coupled processes involved by integrating the spectrum of different stochastic phenomena which may occur (Casalicchio et al., 2010)
- Quantitative approaches: This analysis is based on the extensive definition of risk scenarios followed by filter and ranking by expert opinions, as determined by their likelihood and consequence DECRIS model (Utne, I.B et al., 2010), (Utne et al., 2008)

[3] http://www.fema.gov/hazus

4. Development of the methodological framework

The main idea of the proposed approach is that any asset within a CI can cause diverse impacts and affect other interconnected assets or networks. The applied modelling and simulation tools will estimate how the CI state (or its assets) are depended on its previous state and/or the states of its interconnected assets. The state of an interconnected asset is thus a result of the nature of the climatic pressure affecting the originating asset, the resilience of the asset / network under consideration (risk mitigation, means of immediate response, safety equipment) and the type of interconnection between the assets. A Consequence-based Risk Management approach will be followed as it is depicted in Figure 1, which incorporates uncertainty in all phases of climate risk modeling and quantifies the risk to societal systems and subsystems.

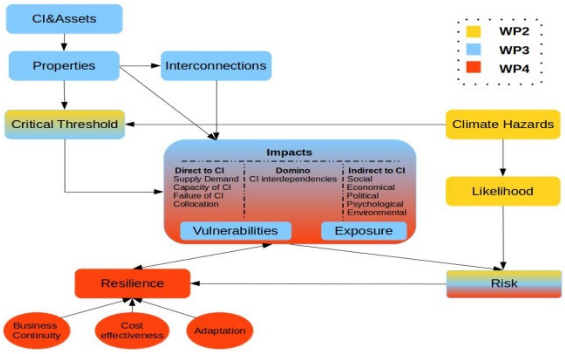


Figure 1. EU-CIRCLE framework high level description

The implementation of the methodological approach will be implemented on the CIRP platform[4], an innovative modular and expandable software platform that will assess potential impacts due to climate hazards; provide monitoring through new resilience indicators, and support cost-efficient adaptation measures. It is defined as an end-to-end collaborative modeling environment where new analyses can be added anywhere along the analysis workflow and present findings in a unified manner providing an efficient solution that integrates existing modeling tools and data into a standardized fashion.

A common point of the proposed methodology is to move towards a common representation of CI infrastructures placing emphasis on their role, the flow of services to the customers and other CI. Different CI types are displayed into parallel layers represent individual sectors those of the road, electricity and drinking water network. Figure 2 introduces the reference simulated environment of the EU-CIRCLE project, introduced as a testing platform during the development stage.

[4] http://www.eu-circle.eu/wp-content/uploads/2016/04/d5.1.pdf

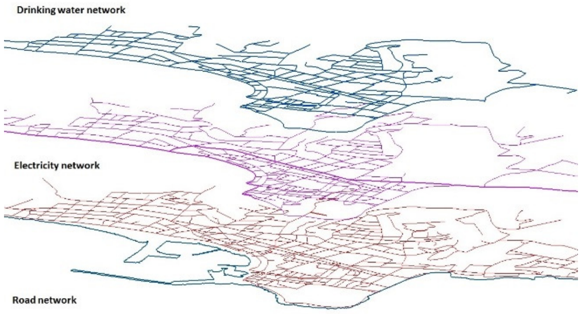


Figure 2. Infrastructure independencies for simulated environment

Within our approach each infrastructure is represented as a set of interconnected assets (e.g. power generation stations, power distribution stations, power lines, pumping stations, water pipelines, pipeline junctions, bridges, roadways, etc), and can be modeled as a network that consists of nodes and links. Through this approach network flow algorithms can be applied to ascertain network behavior given any climate change scenario.

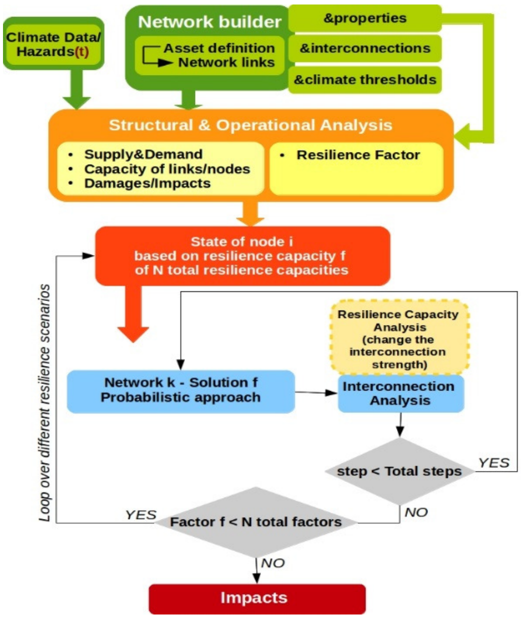

Climate Data/ Hazards(t)
Network builder
Asset definition
Network links
&properties
&interconnections
&climate thresholds
Structural & Operational Analysis
• Supply&Demand
• Capacity of links/nodes
• Damages/Impacts
• Resilience Factor
State of node i based on resilience capacity f of N total resilience capacities
Loop over different resilience scenarios
Resilience Capacity Analysis (change the interconnection strength)
Network k - Solution f Probabilistic approach
Interconnection Analysis
step < Total steps
YES
NO
Factor f < N total factors
YES
NO
Impacts

Figure 3. Generic methodological approach

The process in summary is the following in Figure 3:

1. Identify climate scenarios, and their probability of appearance (e.g. through extreme value theory, return period) through any related statistical measure.
2. Identify CI assets and their respective properties.

3. Define climate related impacts to the CI behavior and properties. These could influence the supply and demand of the CI, the bearing capacity of the CI assets and result in partial or total collapse of the capacity of the CI to serve.
4. Define impacts that do not influence the network flow, but are mandatory for evaluating risk (e.g. loss of life, economy, societal, environment).
5. Model the flow of the interconnected networks using network simulation models.
6. Estimate cumulative impacts and subsequently the risk.

Apply resilience options that could modify climate impacts to assets (step 3 & 4), operation of the CI (step 5) and their interconnections (step 5). These would result in effectively new simulations (step 1-6) using the modified properties of the CI network.

4.1 Climate Data & climate hazards analysis

The initial condition of the analysis is the climate scenario. Different climate information can be used as input to the risk assessment including:

- Output from GCM (usually at low spatial resolution) reaching up to the year 2100, and obtained from different RCP scenarios
- Dynamically downscaled RCM models with higher resolution and very low temporal analysis
- Statistically downscaled climate information (Benestad et al., 2008)
- Historical information, either derived from in-situ observations, satellite monitoring and re-analysis data sets

The output of the climate models include the likelihood of the event, and the related climate information (single value, spatial / temporal extend). Additionally it can provide input for secondary climate hazards models (forest fire spreading, flood modelling, drought, etc).

4.2 Registry of CI assets

An in-depth analysis of the elementary assets for the analysed critical infrastructure assets will be made applying a hierarchical classification. For each type of infrastructure, the following elements will be determined: direct assets, auxiliary assets, flow of people, goods and services, input / output, accessibility and capacity. Additionally the identification of interconnections, interdependencies and appointment of critical infrastructures assets will be identified depending on the type: physical, systems, geographical, logical (Rinaldi et al., 2001). Each asset has been attributed properties and values needed for the follow-on analysis.

4.3 Induced Damages functions

Under the proposed modelling framework, climate hazard conditions impact components of CI systems, causing damages and mal-functions in their capacity and/or also possible disruptions in supply&demand and capacity on the networks nodes which performs changes on the network attributes. These characteristics are generally described by impact models, fragility curves and damage-functionality relationships Figure 4.

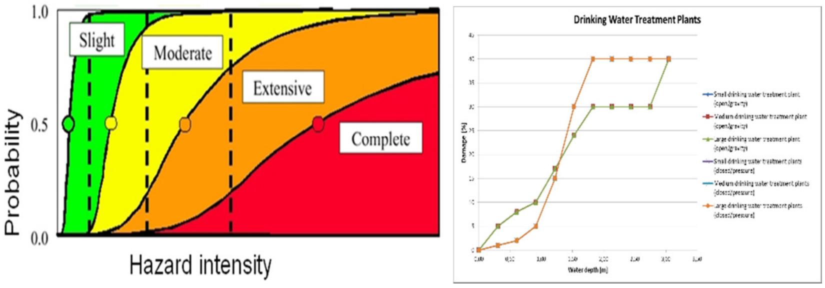


Figure 4. Generic damage curves according to HAZUS Methodology (FEMA, n.d.) and for Drinking Water plants

Two different sets of impacts are identified i) either on asset or network level

- Failure (total or partial) to the asset
- Change in the supply / demand properties of the network (e.g. change in electricity demand due to heat wave or in the energy supply of wind parks)
- Change in the bearing capacity of a network node (e.g. transmission line changes due to temperature)

ii) or on the impacts to CI and society in general and are critically used to identify and estimate in the impacts for the risk assessment.

The main functional representation within this approach are Fragility curves / damage functions / impact assessment models that describe the probability of failure / and or capacity change, conditioned on climate hazard value, over the full range of values to which a system might be exposed and provide a richer and more comprehensive perspective on system capacity (Schultz et al., 2010).

4.4 Network analysis

The proposed approach introduces a network interdependency analysis between different types of networks of CI as a core modelling component. The complexity of each type of network makes it difficult to create a universal algorithm for simulating the network behavior under normal and stress conditions. We employ a more generic approach, describing the network as a graph (nodes and links) with a characteristic value of flow for its link. This approach permits to solve the network using graph theory solutions, independent of the network type. Moreover, an interdependency network analysis can be performed with additional information, about interconnections (types and properties) between the separate networks. The type of network is inserted as flow in the links and damage / fragility property of the node.

The combined information produces a characteristic value that express the probability of a CI asset change of state during an extreme event. Moreover, in order to perform resilience assessment during the Network Analysis, a resilience factor has been proposed in Structural and Operational Analysis which can be used to examine resilience options and adaptation scenarios by modifying the damage/fragility curves of each network asset and the interconnections' accordingly in Figure 5 and Figure 6.

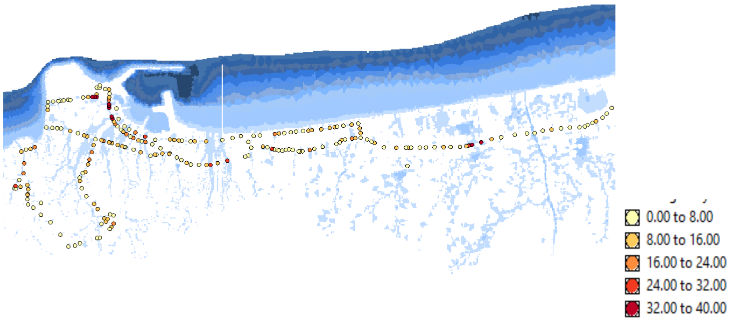


Figure 5. Damage (in %) in water network assets due to 40year return period flood event.

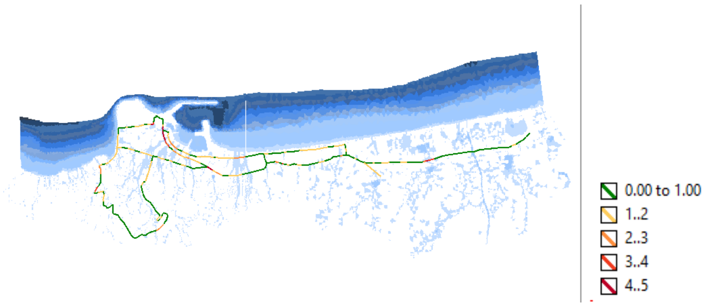


Figure 6. Network flow disruptions [ranked from 0-5 categories]

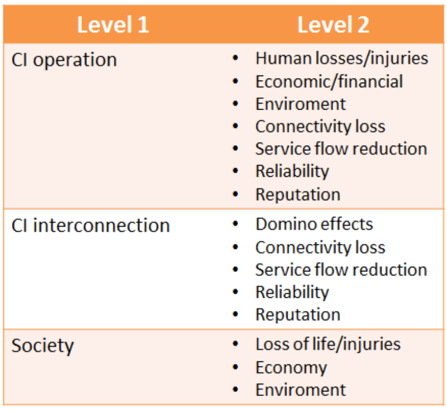
The proposed approach is based on a probabilistic network models performed for each scenario. For solving the basic scenario, and every proposed resilience based modification, the network analysis solves each network flow independently and then captures its interconnections depending on the type resolving each network. The expected result is the Connectivity Loss (CL) between nodes, and Service Flow Reduction (SFR). Connectivity Loss is a measure of the ability of every distribution node to receive from a generation node where as Service Flow Reduction (SFR) determines the amount of flow that the system can provide compared to what it provided before the "event" (Steelman et al., 2007; Young-Suk Kim et al., 2008).

A modification of the above Interconnected Network Analysis Model is proposed in order to automatically perform resilience assessment during the Network Analysis. A resilience factor can be introduced in the estimation of the damage function (step 3 &4) and also in the process of solving network interconnections due to the implementation of different resilience capacities. As a result, parallel network analysis can be performed in order to assess the most suitable CI adaptation scenario could be derived from the calculation of the necessary resilience indicator for the infrastructure.

4.5 Assessment of consequences

Climate change already has far-reaching impacts on infrastructure and can put the operation, capacity potential and reliability of various infrastructures at increased risk[5] (SWD(2013) 137 final) (De Groeve et al., 2015; Keith Williges et al., 2015; UNISRD, 2013). Infrastructure system performance can be measured with either simple metrics that only depend on the topological characteristics of a network system, or more elaborate metrics that depend on flow patterns (outcome of network simulation models - section 4.5) and supply/demand in addition to the topological characteristics. For utility systems, two system performance measures are adopted: Connectivity Loss (CL) and Service Flow Reduction (SFR). CL only requires network topology, while SFR considers flow capacity and the supply/demand of elements. With respect to the impacts on the CI and the society in general the following hierarchical structure is proposed:

Table I. Consequences hierarchical structure



Level 1	Level 2
CI operation	• Human losses/injuries • Economic/financial • Enviroment • Connectivity loss • Service flow reduction • Reliability • Reputation
CI interconnection	• Domino effects • Connectivity loss • Service flow reduction • Reliability • Reputation
Society	• Loss of life/injuries • Economy • Enviroment

4.6 Assessing Risk

The RAF has been conceptualized in accordance to NRAs and guidance found in Dir 114/2008, using an ordinal scale of 5 categories. The Risk Assessment Matrix applied here Table II, is a classic tool to conduct semi-quantitative risk assessment, widely applied in many different frameworks. Some basic principles that were adopted within the present RAF that the output risk index is determined only by the mapping of the consequences and the likelihood to a single risk level, all of which can be divided into different levels, respectively, with qualitative descriptions and scales.

[5] http://drmkc.jrc.ec.europa.eu/partnership/Disaster-Loss-and-Damage-Working-Group

Table II. Risk matrix

	CONSEQUENCES				
LIKELIHOOD	**NEGLIGIBLE**	**SMALL**	**HIGH**	**SEVERE**	**CRITICAL**
CERTAINTY	LOW	MEDIUM	HIGH	CRITICAL	CRITICAL
HIGH	VERY LOW	MEDIUM	MEDIUM	HIGH	CRITICAL
MEDIUM	VERY LOW	LOW	MEDIUM	MEDIUM	HIGH
LOW	VERY LOW	VERY LOW	LOW	LOW	MEDIUM
VERY LOW	VERY LOW	VERY LOW	VERY LOW	VERY LOW	LOW

5. Conclusions

This work introduces a methodological approach for assessing the resilience of European Critical Infrastructure to emerging challenges such as climate change. The work presents here the high level methodological aspects, as it is currently ongoing.

Acknowledgements

This project has received partial funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653824 - EU-CIRCLE

References

Angela Queste, Dr. Wolfram Geier, 2005. Vulnerability of modern societies towards natural disasters - the impact on critical infrastructures.

Benestad, R.E., Hanssen-Bauer, I., Chen, D., 2008. Empirical-statistical downscaling. World Scientific Pub Co Inc, New Jersey.

Bollinger, L.A., Bogmans, C.W.J., Chappin, E.J.L., Dijkema, G.P.J., Huibregtse, J.N., Maas, N., Schenk, T., Snelder, M., van Thienen, P., de Wit, S., Wols, B., Tavasszy, L.A., 2013. Climate adaptation of interconnected infrastructures: a framework for supporting governance. Reg. Environ. Change. doi:10.1007/s10113-013-0428-4

Casalicchio, E., Setola, R., Bologna, S., 2010. A Two-Stage Approach to Simulate Interdependent Critical Infrastructures. IEEE, pp. 76–78. doi:10.1109/COMPENG.2010.33

CEN, 2014. Business Plan, CEN/TC 250 STRUCTURAL EUROCODES, EXECUTIVE SUMMARY.

CEN, 2007. Newsletter of the European Committee for Standarization/Technical Committee 250-Structural Eurocodes.

De Groeve, T., Ehlrich, D., Corbane, C., European Commission, Joint Research Centre, Institute for the Protection and the Security of the Citizen, 2015. Guidance for recording and sharing disaster damage and loss data towards the development of operational indicators to translate the Sendai Framework into action. Publications Office, Luxembourg.

DOE, 2012. Strategic Sustainability Performance Plan.

EC, 2014. Overview of natural and man-made disaster risks in the EU (No. SWD(2014) 134). SWD(2014) 134,.

EC, 2013a. An EU Strategy on adaptation to climate change (COM(2013) 216 final). Brussels.

EC, 2013b. Adapting infrastructure to climate change (No. SWD(2013) 137 final). Brussels.

EC, 2008. Identification and designation of European critical infrastructures and the assessment of the need to improve their protection (No. EC Dir 2008/114/).

FEMA, n.d. Multi-hazard Loss Estimation Methodology Flood Model Technical Manual.

Haimes, Y.Y., Kaplan, S., Lambert, J.H., 2002. Risk Filtering, Ranking, and Management Framework Using Hierarchical Holographic Modeling. Risk Anal. 22, 383–397. doi:10.1111/0272-4332.00020

Hokstad, P., Utne, I.B., Vatn, J., 2012. Risk and Interdependencies in Critical Infrastructures, Springer Series in Reliability Engineering. Springer London, London.

Keith Williges, Stefan Hochrainer-Stigler, Junko Mochizuki, Reinhard Mechler, 2015. Modeling the indirect and fiscal risks from natural disasters for informing options for enhancing resilience and building back better. IIASA, UNISDR.

Ouyang, M., Hong, L., Mao, Z.-J., Yu, M.-H., Qi, F., 2009. A methodological approach to analyze vulnerability of interdependent infrastructures. Simul. Model. Pract. Theory 17, 817–828. doi:10.1016/j.simpat.2009.02.001

Rinaldi, S.M., Peerenboom, J.P., Kelly, T.., 2001. Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Syst. 26, 11–25.

Schultz, M.T., Gouldby, B.P., Simm, J.D., Wibowo, J.L., 2010. Beyond the factor of safety: Developing fragility curves to characterize system reliability. DTIC Document.

Silvia Dimova, Manfred Fuchs, Artur Pinto, Borislava Nikolova, Luisa Sousa, Sonia Iannaccone, 2015. State of implementation of the Eurocodes in the European Union- Support to the implementation, harmonization and further development of the Eurocodes.

Steelman, J., Song, J., Hajjar, J.F., 2007. Integrated Data Flow and Risk Aggregation for Consequence-Based Risk Management of Seismic Regional Loss. University of Illinois.

UNISRD, 2013. Probabilistic Modelling of N atural Risks at the Global Level: Global Risk Model (Global assessment report on disaster risk reduction). International Centre for Numerical Methods in Engineering & ITEC S.A.S. – INGENIAR LTDA. – EAI S.A, Geneva, Switzerland.

Utne, I.B., Hokstad, P., Kjølle, G., Vatn, J., Tøndel, I.A., Bertelsen, D., Fridheim, H., Røstum, J., 2008. Risk and Vulnerability Analysis of Critical Infrastructures-The DECRIS Approach, in: SAMRISK Conference, Oslo.

Utne, I.B., Hokstad, P., Vatn, J., 2011. A method for risk modeling of interdependencies in critical infrastructures. Reliab. Eng. Syst. Saf. 96, 671–678. doi:10.1016/j.ress.2010.12.006

Utne, I.B, Vatn, J, Hokstad, P, Guedes Soares, C, Briš, R, Martorell, S, 2010. A structured approach to modelling interdependencies in risk analysis of critical infrastructures'. Reliability, Risk, and Safety Theory and Applications. CRC Press.

Young-Suk Kim, B.F. Spencer, Jr., Amr S. Elnashai, 2008. Seismic Loss Assessment and Mitigation for Critical Urban Infrastructure Systems (NSEL Report Series No. Report No. NSEL-007).

Lifetime degradation and interventions for systems under random shocks

Dimos C. Charmpis
Department of Civil and Environmental Engineering, University of Cyprus,
75 Kallipoleos Str., P.O. Box 20537, 1678 Nicosia, Cyprus

Abstract

This work is concerned with the time-dependent degradation and the intervention needs of engineering systems deteriorating over time due to the effects of series of shocks. A probabilistic framework is implemented to deal with the randomness in arrival times (Poisson process) and sizes of the shocks considered. Corrective and preventive intervention actions are applied to maintain a system in operational and safe condition despite the shock-based damage accumulated during its lifetime. The focus of the paper is on the effectiveness of early repairs to prevent loss of system functionality and/or failure. Various cases of such preventive repair actions are investigated using a Monte Carlo simulation procedure. The numerical results obtained demonstrate the trade-off relationship between the system's improved performance and the corresponding numbers and extent of interventions required.

Keywords: life-cycle; deterioration; Poisson process; repair; maintenance.

1. Introduction

Engineering systems deteriorate over time due to the effects of natural and/or manmade hazards. During its lifetime, a system is expected to sustain actions causing practically continuous degradation (e.g. wear from normal use, fatigue due to repeated loading, corrosion due to aggressive environmental conditions, etc.), as well as sudden events due to shocks that result in discrete degradation (e.g. earthquakes, hurricanes, etc.). Despite its exposure to such degradation causes and the accumulation of damage with time, a system is required to be operational and safe for a certain period of time. In order to ensure that the system will meet these requirements, its condition needs to be monitored during its lifetime and appropriate interventions must be performed whenever needed, in order to restore its capacity and availability. Establishing an optimal maintenance strategy plays a crucial role in the cost-effective life-cycle management of the system. Therefore, intensive research efforts are internationally invested in this scientific area (e.g. Kleiner, 2001; Sanchez-Silva et al., 2011; Orabi & El-Rayes, 2012; Frangopol & Bocchini, 2012; Junca & Sanchez-Silva, 2013; Salem et al., 2013; Alogdianakis et al., 2016; Sánchez-Silva et al., 2016; Charmpis et al., 2016; Ait Mokhtar et al., 2016).

The present work focuses on engineering systems subjected to series of shocks during their lifetime. The shocks acting on a system arrive at random times (according to a Poisson process), while the intensity of each shock is also random. Due to the damage accumulated on the system after a number of shocks, loss of functionality and/or failure of the system may occur. Thus, corrective intervention actions (repair or even complete reconstruction) are required to restore the damaged system's capacity. In an effort to achieve a more cost-effective maintenance strategy for such a degrading system, the basic aim of this paper is to investigate the effect of preventive repair on the lifetime performance and intervention needs of the system. This type of repair is applied early on the system, before the occurrence of functionality loss and/or failure. The numerical investigation presented is performed using a Monte Carlo simulation procedure. At each simulation, shock arrival times and sizes are sampled from appropriate distributions.

The remainder of this paper is organized as follows. Section 2 describes the degradation process of a system subjected to random shocks. Section 3 explains how to identify loss of functionality and/or failure for a system under shock-based degradation. The implementation of corrective and preventive system intervention actions is discussed in section 4. Section 5 reports and discusses numerical results of an illustrative example. Finally, the overall conclusions of the paper are given in section 6.

2. System degradation due to random shocks

Stochastic processes are widely used to study the lifetime performance of engineering systems under uncertainty (e.g. Sanchez-Silva et al., 2011; Iervolino et al., 2013; Junca & Sanchez-Silva, 2013; Rafiee et al., 2016). In particular, the Poisson process is commonly employed to model arrival times of random events occurring to a system. In the present work, we consider a system subjected to random shocks that occur according to a Poisson process with rate λ (events/year). If t_i is the arrival time (time of occurrence) of the i-th shock (t_0=0), then the i-th inter-arrival time is expressed as: $x_i=t_i-t_{i-1}$. The inter-arrival times $x_1,x_2,\ldots$ is a sequence of independent, identically distributed exponential random variables with mean $1/\lambda$. This distributional property of inter-arrival times results from the fact that the Poisson process has no memory. Hence, the process of shock arrivals has the same distribution throughout the lifetime of the system (stationarity assumption). Moreover, since the inter-arrival times of the process are independent, any shock occurrence time does not depend on the occurrence times of past shocks and does not affect the occurrence times of possible future shocks.

When a shock arrives according to a Poisson process, the corresponding shock size is also controlled through a random variable, which is usually exponentially or lognormally distributed. In this paper, shock sizes follow an exponential distribution, which is assumed to remain unaltered throughout the lifetime of the system. Again, the memory-less property holds: any shock size does not depend on the past shock sizes and does not affect the possible future shock sizes. Moreover, the exponential distributions of shock sizes and inter-arrival times are independent.

Based on the above, a system subjected to random shocks deteriorates with time in a probabilistic manner, as it sustains shocks of various (random) sizes at various

(random) arrival times throughout its lifetime. Shock-based system degradation is actually realized by removing from the system an amount of capacity units, when a shock occurs. Hence, we consider a system with initial capacity C_0 that starts to operate at time t=0. The system is subjected to shocks that arrive at times $t_1,t_2,\ldots$ according to a Poisson process and cause degradation, which depends on the intensity of each shock. Thus, the shock occurring at time t_i results in system damage of size D_i (measured in capacity units), which is sampled from an exponential distribution. Shock after shock, damage accumulates on the system. By time t, the total damage accumulated can be expressed in terms of capacity units as:

$$D(t) = \sum_{i=1}^{n(t)} D_i \ , \tag{1}$$

where $n(t)$ is the number of shocks that have occurred by time t. Then, the corresponding residual capacity of the system is obtained by subtracting from its initial capacity the total damage sustained:

$$C(t) = C_0 - D(t)\,. \tag{2}$$

3. Failure and/or loss of functionality of degrading systems

The performance of an engineering system at any time t is typically assessed with respect to its safety and functionality by defining appropriate limit state conditions. In the present work, limit states are specified by choosing appropriate threshold values for the residual capacity $C(t)$ of a degrading system, which is a standard approach followed also in other studies (e.g. Sanchez-Silva et al., 2011; Rafiee et al., 2016). Hence, when the residual capacity falls below such a threshold due to the damage accumulated from a series of shocks, the system underperforms, as it violates the respective limit state condition. Two threshold values are applied herein:

- Functionality threshold C_{func}. A system is considered to be fully functional at any time t as long as $C(t) \geq C_{\text{func}}$. It is further assumed that a functional system operates in an as good as new state despite the damage possibly accumulated on the system. Loss of system functionality (but not necessarily system failure) is denoted by the condition $C(t) < C_{\text{func}}$, which implies that the system cannot operate or it is not safe to operate and is therefore put out of service.
- Failure threshold C_{fail}. Failure of a system is indicated by the condition $C(t) \leq C_{\text{fail}}$, which implies also loss of system functionality. Thus, when $C(t) > C_{\text{fail}}$ and $C(t) < C_{\text{func}}$, the system is not failed, but it cannot operate at all.

In general, threshold values have to be chosen in a way that $C_0 \geq C_{\text{func}} \geq C_{\text{fail}}$, although most commonly they are specified as $C_0 > C_{\text{func}} > C_{\text{fail}} = 0$.

In this paper, it is assumed that a failed system needs to be replaced, because it is not repairable (due to extensive damage sustained or even collapse) or it is uneconomical to be repaired. Therefore, the system has to be fully reconstructed, in order to operate again. Depending on the available budget, the system functionality needs, the experience gained from the occurred failure, etc., the newly constructed system may be ‘identical’ with the failed one (i.e. with the same initial capacity C_0) or it may be an

upgraded or downgraded version of it (i.e. with an initial capacity that is larger or smaller than C_0). It should be emphasized, however, that covering the direct cost associated mainly with the reconstruction of the system is not the most important consequence of the failure. Indirect consequences associated with injuries/fatalities, environmental issues, long loss of functionality, user inconvenience, delays, etc. are typically much more severe and costly.

In the case of loss of functionality without failure, the system is considered to be repairable, i.e. the option of repairing instead of replacing it is technically, economically, environmentally, etc. viable. In general, the repair of the system may be perfect (the initial capacity C_0 is fully restored and the system is in an as good as new condition) or imperfect (the initial capacity C_0 is partly restored) (e.g. Sánchez-Silva et al., 2016). In any case, the negative consequences sustained are basically due to the implications caused by the interruption of the availability of the system. Clearly, both direct and indirect consequences are much less severe when a system is non-operational and just needs some repairs compared to an overall failure inducing the need for system replacement.

4. Corrective and preventive system interventions

A straightforward approach to make a decision regarding an intervention (repair or reconstruction) at any time *t* on a system damaged by a series of shocks is to compare the system’s residual capacity at time *t* with the functionality and failure thresholds defined in the previous section. Then, assuming that repairs are perfect and replacement installs a new system that is ‘identical’ to the failed one, two simple intervention criteria can be specified:

- When a shock at time *t* causes system failure ($C(t)\leq C_{\text{fail}}$), reconstruction is decided and the failed system is immediately replaced with a new one having initial capacity C_0.
- When a shock at time *t* causes loss of system functionality without failure ($C(t)<C_{\text{func}}$ and $C(t)>C_{\text{fail}}$), repair is decided to immediately restore the initial capacity C_0 of the system.

These criteria allow only corrective intervention actions after undesired events have occurred: reconstruction is decided only after system failure; repair is decided only after loss of system functionality. Thus, we are forced to sustain (possibly devastating) consequences despite the intervention actions applied.

In this work, an additional threshold value is introduced, in order to specify also a preventive intervention criterion that allows repair actions to be applied earlier. Hence, when a shock at time *t* causes the system’s residual capacity to fall below the ‘repair threshold’ C_{rep} ($C(t)\leq C_{\text{rep}}$), repair is decided to immediately restore the initial capacity C_0 of the system. The threshold C_{rep} takes a fixed pre-specified value chosen in a way that $C_{\text{rep}}\geq C_{\text{func}}$. This criterion allows system repair to be decided before failure and/or loss of functionality occur, in order to prevent the negative consequences of these undesired events. This way, we gain control over the system's probabilities of failure and loss of functionality. Preventive intervention based on a condition threshold has

been used in other studies, mainly in an effort to mitigate the probability of system failure (e.g. Sanchez-Silva et al., 2011). The present paper, however, explicitly addresses also the highly important issue of system availability, as it investigates the effect of preventive repair on both probabilities of system functionality loss and failure.

It is pointed out that the new preventive intervention criterion based on the repair threshold C_{rep} is applied in addition to the two aforementioned corrective intervention criteria. Depending on the current capacity of a damaged system and the size of a new shock, any of the three criteria may be activated. More specifically, when the i-th shock arrives at time t_i and causes damage of size D_i on an already damaged system with residual capacity $C(t_i)$, then the new residual capacity of the system is $C(t_i)$-D_i and one of the following four cases applies:

- $C(t_i)-D_i>C_{\mathrm{rep}}$: no system intervention required;
- $C(t_i)-D_i\leq C_{\mathrm{rep}}$ and $C(t_i)-D_i\geq C_{\mathrm{func}}$: system repair required (preventive action);
- $C(t_i)-D_i<C_{\mathrm{func}}$ and $C(t_i)-D_i>C_{\mathrm{fail}}$: system repair required due to loss of functionality (corrective action);
- $C(t_i)-D_i\leq C_{\mathrm{fail}}$: system reconstruction required due to failure (corrective action).

Note that, for $C_{\mathrm{rep}}=C_{\mathrm{func}}$, the preventive repair criterion is actually deactivated and only corrective interventions can be applied. It should also be mentioned that damage, repair and reconstruction are all assumed to be 'instantaneous' events.

5. Illustrative numerical example

Consider a structural system (e.g. highway bridge) with initial capacity $C_0=100$ (measured in capacity units) at time $t=0$. During its lifetime, the system is subjected to a series of earthquakes with occurrence times following a Poisson process with parameter $\lambda=0.05$ events/year (i.e. one earthquake is expected per 20 years). The damage caused on the system by each earthquake is an exponentially distributed variable with a mean of 15 capacity units. The functionality and failure thresholds for this system are $C_{\mathrm{func}}=20$ and $C_{\mathrm{fail}}=0$, while various repair thresholds $C_{\mathrm{rep}}\geq 20$ are examined. The required lifetime of the system is 100 years.

A Monte Carlo simulation procedure is employed to study the probabilistic performance and intervention needs of the system for the period of 100 years. At each simulation, the system is subjected to a different series of shocks, whose inter-arrival times and sizes are sampled from exponential distributions with the properties given above; thus, damage accumulates on the system activating intervention actions as described in section 4. Six different test cases are specified by varying the C_{rep}-value; for every case, 100,000 Monte Carlo simulations are performed.

Table I presents results for the test cases investigated. The probabilistic system performance can be assessed by the expected numbers of failures and losses of functionality per Monte Carlo simulation. When preventive repair is not allowed (C_{rep}=20), there are unacceptably high probabilities for the system to be in a failed and/or non-operational condition within the period of study of 100 years. More

specifically, failure at any simulation may occur with probability of about 10%, while loss of functionality should be expected more or less at every second simulation. This situation can be improved by performing earlier preventive repairs (C_{rep}>20). A higher C_{rep}-value results in lower expected numbers of failures and losses of functionality. For instance, the choice of C_{rep}=40 reduces both numbers by more than 50% compared to those obtained for C_{rep}=20. For rather high C_{rep}-values (i.e. C_{rep}=70-80), the expected numbers of system failures and losses of functionality are one order of magnitude lower than those for C_{rep}=20.

The improved system performance, however, is not achieved at no cost. Table I shows that a higher C_{rep}-value generally induces the need for more interventions (repairs and reconstructions) within the lifetime of 100 years. Hence, for low C_{rep}-values (i.e. C_{rep}=20-30), the need for an intervention should be expected to arise more or less at every second simulation. On the other hand, for high C_{rep}-values (i.e. C_{rep}≈80), two interventions per simulation should be expected. Moreover, higher expected numbers of interventions are associated with larger expected amounts of capacity units to be restored. Indeed, for C_{rep}=20-30, a total amount of about 40 capacity units should be expected to be restored at each simulation; for C_{rep}=70-80, the corresponding amount is almost 70 capacity units. Thus, Table I demonstrates the trade-off relationship between the system performance metrics (expected numbers of system failures and losses of functionality) and the numbers and extent of interventions performed.

Figures 1-4 illustrate the system's capacity evolution with time due to damage accumulated from successive shocks for 4 characteristic Monte Carlo simulations. In the simulation of Fig. 1, preventive repair is not allowed (C_{rep}=20), therefore any intervention could only be corrective. Indeed, a corrective repair is performed at time t≈65 years due to loss of functionality after 3 shocks sustained by the system. Two more shocks arrive after the repair, but the corresponding capacity drops do not cause another functionality loss or failure. The loss of functionality observed in this simulation would be prevented with a choice of C_{rep}≥64.

Table I. Probabilistic results for system performance and intervention needs (expected numbers per Monte Carlo simulation)

C_{rep}	20	30	40	56	71	80
Expected number of						
Failures	0.11	0.07	0.05	0.02	0.01	0.01
Losses of functionality	0.43	0.28	0.18	0.09	0.05	0.04
Interventions	0.4	0.5	0.7	1.0	1.5	2.0
Restored capacity units	39	45	50	58	65	69

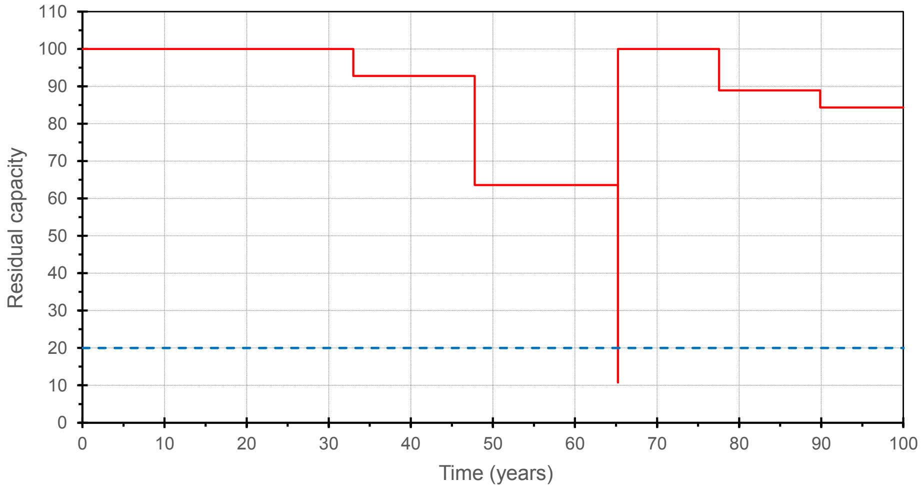


Figure 1. System's capacity evolution with time for C_{rep}=20 (one corrective repair performed).

In the simulation of Fig. 2 (C_{rep}=40), after damage is accumulated due to 4 shocks sustained by the system, a preventive repair is carried out at t≈85 years. The single shock that arrives after the repair (at t≈90 years) does not cause any functionality loss or failure. Notice, however, that the additional damage accumulated due to the shock at t≈90 years would cause loss of system functionality without the early repair at t≈85 years. Nevertheless, the use of a C_{rep}-value that is greater than C_{func} does not guarantee that functionality loss or failure will never occur. In the simulation of Fig. 3 (again with C_{rep}=40), the system becomes non-operational after the 4-th shock sustained at t≈68 years, therefore corrective repair is needed. This happens because the size of the shock at t≈68 years is large enough to jump over the capacity range (20-40) activating the choice for preventive repair. A choice of C_{rep}≥62 would prevent the loss of system functionality experienced in this simulation.

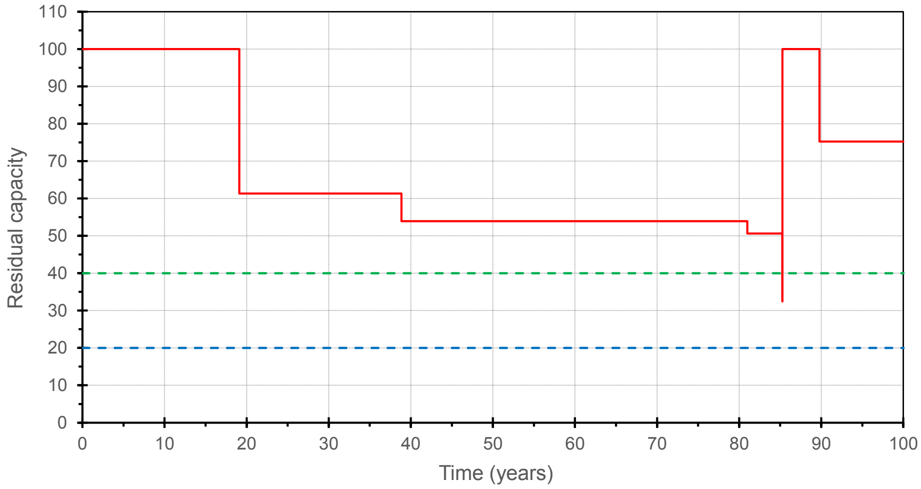


Figure 2. System's capacity evolution with time for C_{rep}=40 (one preventive repair performed).

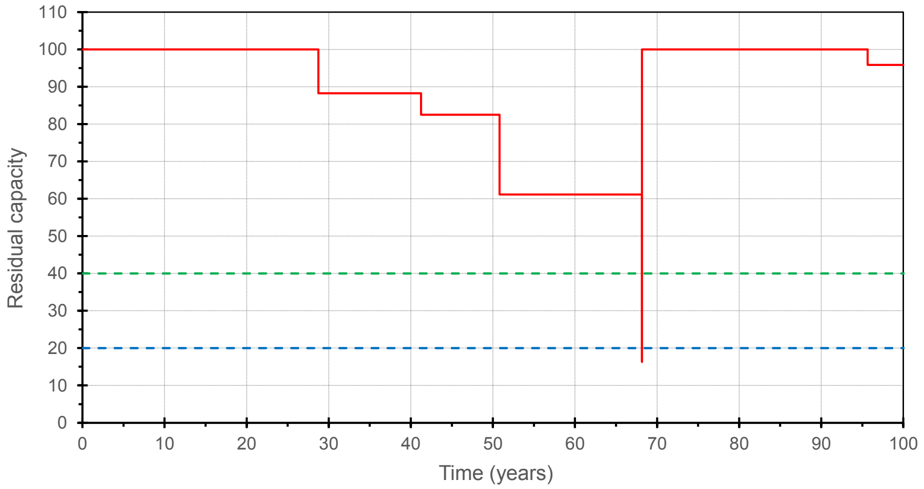


Figure 3. System's capacity evolution with time for C_{rep}=40 (one corrective repair performed).

In the simulation of Fig. 4 (C_{rep}=56), two system repairs are performed. At *t*≈47 years, the 3rd shock sustained by the system results in loss of functionality and induces the need for corrective repair. At *t*≈90 years, after two more shocks, a preventive repair is also carried out. Thus, in general, a mix of intervention actions (preventive repairs/corrective repairs/reconstructions) could be activated at a single simulation depending in any case on the way damage accumulates with time. Note that, with a choice of C_{rep}=65, the loss of system functionality at *t*≈47 years would be prevented, while another two preventive repairs would be performed until the end of the system's lifetime, avoiding this way any occurrence of non-operational or failed condition.

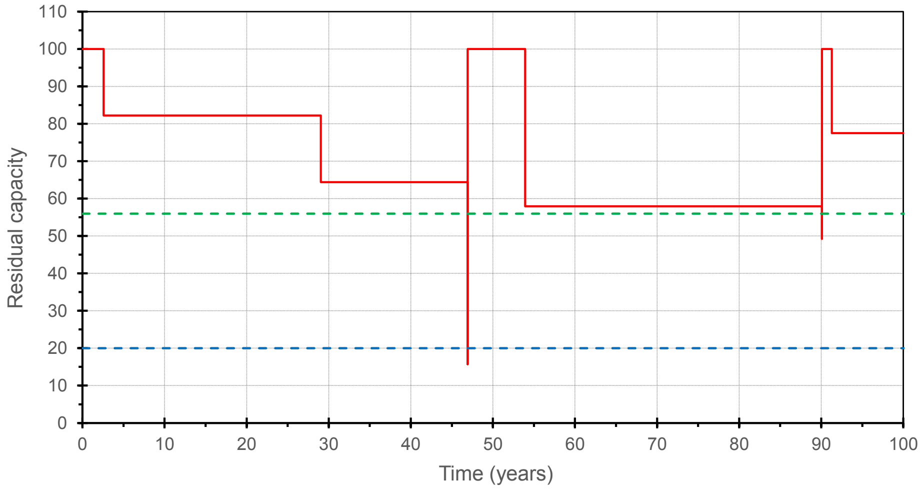


Figure 4. System's capacity evolution with time for C_{rep}=56 (one corrective and one preventive repair performed).

6. Concluding remarks

This paper presents an assessment of the effectiveness of preventive repairs on the lifetime performance and required interventions of an engineering system degrading over time due to random shocks. In an effort to prevent loss of system functionality and/or failure, a repair threshold is introduced to identify the need for early intervention on the system. This preventive repair approach improves the performance of the system in terms of its probabilities to be in a failed and/or non-operational condition within its lifetime. However, the overall required numbers and extent of interventions are increased. The current work provides a quantitative demonstration of this trade-off relationship. Reliable quantitative data for system behaviour and intervention needs form the basis for the optimal allocation of available funding to cost-effectively maintain infrastructure networks or stocks comprising of various individual systems (e.g. Faddoul et al., 2013; Charmpis & Dimitriou, 2015; Sánchez-Silva et al., 2016).

References

Ait Mokhtar, E.H., Laggoune, R. and Chateauneuf, A. (2016) Imperfect preventive maintenance policy for complex systems based on Bayesian networks. *Quality and Reliability Engineering International*, in press.

Alogdianakis, F., Charmpis, D.C. and Balafas, I. (2016) Using calibrated probabilistic deterioration information to optimize the rehabilitation schedule of bridges. In: *Proceedings of the 8th International Conference on Bridge Maintenance, Safety and Management (IABMAS 2016)*, Foz do Iguaçu, Brazil.

Charmpis, D.C. and Dimitriou, L. (2015) A stress-test of alternative formulations and algorithmic configurations for the binary combinatorial optimization of bridges rehabilitation selection. In: *Engineering and Applied Sciences Optimization*, Vol. 38 of Computational Methods in Applied Sciences (Springer), N.D. Lagaros, M. Papadrakakis (eds.), pp. 489-507.

Charmpis, D.C., Alogdianakis, F. and Balafas, I. (2016) Scheduling bridge rehabilitations based on probabilistic structural condition model, risk attitude and life cycle cost. In: *Proceedings of the 51st ESReDA Seminar on Maintenance and Life Cycle Assessment of Structures and Industrial Systems*, Clermont-Ferrand, France.

Faddoul, R., Soubra, A.-H., Raphael, W. and Chateauneuf A. (2013) Extension of dynamic programming models for management optimisation from single structure to multi-structures level. *Structure and Infrastructure Engineering*, Vol. 9, No. 5, pp. 432-447.

Frangopol, D.M. and Bocchini, P. (2012) Bridge network performance, maintenance and optimisation under uncertainty: accomplishments and challenges. *Structure and Infrastructure Engineering*, Vol. 8, No. 4, pp. 341-356.

Iervolino, I., Giorgio, M. and Chioccarelli, E. (2013) Gamma degradation models for earthquake-resistant structures. *Structural Safety*, Vol. 45, pp. 48-58.

Junca, M. and Sanchez-Silva, M. (2013) Optimal maintenance policy for permanently monitored infrastructure subjected to extreme events. *Probabilistic Engineering Mechanics*, Vol. 33, pp. 1-8.

Kleiner, Y. (2001) Scheduling inspection and renewal of large infrastructure assets. *ASCE Journal of Infrastructure Systems*, Vol. 7, No. 4, pp. 136-143.

Orabi, W. and El-Rayes, K. (2012) Optimizing the rehabilitation efforts of aging transportation networks. *ASCE Journal of Construction Engineering and Management*, Vol. 138, No. 4, pp. 529-539.

Rafiee, K., Feng, Q. and Coit, D.W. (2016) Reliability analysis and condition-based maintenance for failure processes with degradation-dependent hard failure threshold. *Quality and Reliability Engineering International*, in press.

Salem, O.M., Miller, R.A., Deshpande, A.S. and Arurkar, T.P. (2013) Multi-criteria decision-making system for selecting an effective plan for bridge rehabilitation. *Structure and Infrastructure Engineering*, Vol. 9, No. 8, pp. 806-816.

Sánchez-Silva, M., Frangopol, D.M., Padgett, J. and Soliman, M. (2016) Maintenance and operation of infrastructure systems: Review. *ASCE Journal of Structural Engineering*, Vol. 142. No. 9.

Sanchez-Silva, M., Klutke, G.-A. and Rosowsky, D.V. (2011) Life-cycle performance of structures subject to multiple deterioration mechanisms. *Structural Safety*, Vol. 33, pp. 206-217.

Network's Connectivity Dynamic Modelling using a Topological Binary Model: Critical Transitions Concept

Mohamed EID
Commissariat à l'Energie Atomique et aux Energies Altérnatives
CEA-DANS/DM2S/SERMA, Saclay
F-91191 Gif sur Yvette Cedex, France

Inga Žutautaitė
Lithuanian Energy Institute
Laboratory of Nuclear Installation Safety
Breslaujos str. 3, LT-44403, Kaunas, Lithuania

Dovilė Rafanavičiūtė
Vytautas Magnus University
Department of Mathematics and Statistics
Vileikos str. 8, LT-44404, Kaunas, Lithuania

Abstract

An approach is developed to assess network connectivity using basic concepts borrowed and adapted from graph theory and reliability theory. The basic concepts are the "Network Diameter" and the "Critical Transitions". The approach is called Topological Binary Modelling.
Based on the network diameter concept, a connectivity metric is then introduced, called the "nominal connectivity order".
The critical transitions are those resulting in a degradation in the connectivity of the network. Critical transitions increase the connectivity order. Higher connectivity order denotes lower network connectivity. Subsequently, it denotes lower operability/performance quality.
Having identified the critical transitions corresponding to a given connectivity order, the approach determines the likelihood of the occurrence of the critical transitions. One can then assess the network degradation probability with the time.

Keywords: network, connectivity, binary, topological, critical transition

1. Generalities and Basic Notions

An approach is developed to assess the connectivity of a network using classical concepts borrowed from reliability theory and graph theory. The first concept is the concept of "critical transitions". A critical transition is the transition that leads to a degradation in the network overall connectivity state. The approach measures the network overall connectivity state using the "nominal connectivity state".

The nominal connectivity state is defined as the state of connectivity of the network when all the nodes and the edges are available, as fixed by the designer and accepted by the operator.

The approach uses the well-known Node-to-Node model to work out a global connectivity measure as the target of the approach to assess the network overall connectivity state using a systematic modelling process.

A connectivity metric is then introduced, called the "nominal connectivity order-NCO". The NCO is the minimum order at which each node in the network is connected to all the others. The approach starts from the binary topological description using the "adjacency matrix" and proceeds to the determination of higher connectivity orders, using elementary tensor notations.

The definition of the NCO allows determining the degradation in the network connectivity due to losses of nodes and edges. This allows in turn to determine the critical transitions as the transitions that increase the connectivity order. Connectivity orders higher than the NCO denotes a degradation in the network overall connectivity. The approach uses logical cut-sets (paths) to determine the critical transitions.

Once, the NCO of the net is determined and the corresponding critical transitions are identified, the approach determines the likelihood of the critical transitions and permits assessing the network degradation probability with the time.

The details of the approach as schematically presented above is detailed below in the same chronological order.

1. Network Overall Connectivity

Following the notations of the graph theory, a graph $G(N,E)$ is composed of N nodes (vertices) connected through a set of E edges (links). The set of edges E contains all existing links in the network. Formally, the link $l_{(i,j)}$ denotes a direct link (i,j) while $l_{\{i,j\}}$ denotes an indirect link (i,j), between the two nodes i and j.in the paper, we will denote links without brackets such as $l_{i,j}$. The distinction between direct and indirect link is signalled by the order of the corresponding tensor describing the link, as will be explain later.

There are many useful metrics to measure graph connectivity. Among the well-known are degree distribution (Barabasi, 1999), characteristic path length (Watts, 1998), graph diameter [8] and clustering coefficient (Albert, 2002). These measures provide a useful set of statistics for comparing power grids with other graph structures.

The "graph diameter" is amongst the basic notations of the graph theory. It does particularly interest us. For any pairs of nodes i and $j \in N$, let $\delta_{i,j}$ denotes the path between i and j. The diameter D of the graph G is defined as the max of all $\delta_{i,j}$, $D = \max\{\delta_{i,j} / i, j \in N\}$. D is the highest of the lowest paths.

In this paper, a concept derived from the diameter D is used and measured using a metric called the "nominal connectivity order" and is explained in the following.

2. Network Connectivity Order

The "connectivity order" of a network is a metric proposed to measure the global connectivity of a graph.

In §2.1, the notion of the 1st order "binary connectivity tensor" is established based on the "adjacency matrix" from graph theory.

In §2.2, the process of determining the higher order "binary connectivity tensors" is explained.

In §2.3, the notion of the network nominal connectivity order, NCO, is introduced.

2.1 Network Binary Topological Description

Following the graph theory, we use the "adjacency matrix-A" to describe the topology of a given network such as: $e^1_{i,j} = 1$ if nodes i and j are directly connected, otherwise $e^1_{i,j} = 0$ $(i, j \in N)$. The exponent 1 in $e^1_{i,j}$ denotes that it is a 1st order connectivity element, i.e. it describes a direct link between the nodes i and j.

The topological mapping of the network, presented in Figure 1, is given in Table 1. The 1st order mapping represents the network as it should be in its nominal operability state. It is the nominal operability state after the design specifications, accepted by the operator and approved by other stakeholders. As one can see, not all the nodes are directly connected. However, all the nodes are still connected but at "higher connectivity orders". The idea, now, is how to determine in systematic way these existing higher connectivity orders.

2.2 Network Higher Connectivity Orders

Many nodes are not connected at the 1st order level, i.e. not directly connected. They have $e^1_{i,j}$=0. However, they are connected at higher orders, determined as following. Let u^{n+1}_{ij} $(i, j \in N)$ be the connectivity tensor describing the $(n+1)^{th}$ connectivity order between nodes and is determined following after (Eid, 2012) and (Eid, 2013), as following:

$$u^{n+1}_{ij} = e^1_{il} \bullet e^n_{lj} \tag{1}$$

Where, $e^1_{il} \bullet e^n_{lj} \quad = e^1_{i1} \bullet e^n_{1j} + e^1_{i2} \bullet e^n_{2j} + e^1_{i3} \bullet e^n_{3j} + \ldots + e^1_{i(m-1)} \bullet e^n_{(m-1)j} + e^1_{im} \bullet e^n_{mj}$.

Once, u_{ij}^{n+1} is determined, one proceeds to the determination of $e_{i,j}^{n+1}$ as following:

$$e_{ij}^{n+1} = \begin{cases} = 0 & if \quad i = j \\ = 0 & if \quad u_{ij}^{n+1} = 0, \qquad \text{and } n = 1,2,3,... \\ = 1 & if \quad u_{ij}^{n+1} > 0 \end{cases} \tag{2}$$

We, then, proceed to determining the minimum connectivity order of each couple of nodes, $n_{i,j}$, i.e. to determine the minimum value of n at which the value of the binary tensor $e_{i,j}^{n}$ switches to one for each couple in the net.

One can follow the evolution of the binary connectivity tensor in the tables from (1-a) to (1-e) related to the network described in Figure 1. As an example, for the couple of nodes 4 and 6, the minimum connectivity order is 3, i.e. $e_{4,6}^{1} = 0$ and $e_{4,6}^{2} = 0$ but $e_{4,6}^{n} = 1$ for all $n \geq 3$. Each couple of nodes has, then, its characteristic minimum connectivity order.

Having designed a systematic process to determine higher connectivity order tensors and the characteristic minimum connectivity order of each of nodes, we are going to define a metric to measure the network overall connectivity in the following section, §2.3.

2.3 Network Nominal Connectivity Order

Having determined the minimum connectivity order of each couple of nodes $n_{i,j}$ $i, j \in N$, one may be at that stage interested in establishing a measure of the network overall connectivity state.

The approach proposes a metric for measuring the network overall connectivity and denote it by the "Nominal Connectivity Order-NCO". The NCO is the lowest connectivity order, $\min\{n_{i,j}, i, j \in N\}$, at which each node is connected to all the others at which each node is connected to all others. Higher is the NCO, lower is the network connectivity quality.

The network overall connectivity quality decreases with the increase of the connectivity order and inversely. The network overall connectivity state is, also, directly related to the "network operability/performance state" that can be defined as "the likelihood" of the network to be in nominal operation mode at instant "t". Ultimately, the highest operability is attended when $e_{ij}^{1} = 1$ for all the nodes.

The NCO is the connectivity order at which the network's operability complies with the design requirements & specifications and consented by the operator and other concerned stakeholders. The network given in Fig.1 has a NCO equal to five while the corresponding graph diameter is three. The network contains 10 nodes and 15 edges. If each node was directly connected with all the others, the network would have had 45 edges. At a connectivity order equal to five, each node is connected with all the others. At that level of connectivity, each node sees the 14 other nodes, in the network described in Figure 1.

Once the NCO concept is well established and determined, one can proceed to the determination of the “critical transitions”.

3. Critical Transitions

Critical transitions are those transitions (failures/reparations of elementary components such as nodes/links) that result in a change (a decrease/an increase) in the network NCO. According to reliability theory, all failures/reparations of an elementary component that does not impact on the network NCO are not critical transitions.

It worth underlining that the approach is limited to the coherent networks in the sense of “reliability theory”. A network is coherent if no failure of any elementary component can improve (/decrease) the network connectivity order and no reparation of any elementary component can degrade (/increase) the network connectivity order.

4. Determination of Critical Transition Sets

The sets of critical transition can then be determined simply by switching each 1st order tensor $e_{ij}^{1} = 1$, and all possible combinatory of them, to zero, and examine the impact on the network nominal transition order.

Accordingly, one can determine the logical cut-sets leading to critical transitions. As demonstrated in the application given below in §6, one can identify cut-sets according to their orders.

5. Critical Transition Likelihood

Once the critical transition sets are identified, one can determine the probability of “losing the nominal connectivity” of a given network and its time profile. Given that the nominal connectivity is directly linked to the nominal operability/performance of the network. One needs certainly to know failure and repair rates of each link and node in the network.

The case study will demonstrate these practical aspects.

6. A Case Study

A network is described in Figure 1 and mapped in Table 1-a by its adjacency matrix. In the Tables 1-a to 1-e, one can follow the evolution of the connectivity order of the network.

The logical cut-sets leading to the critical transitions are then identified in the following sections and classified according to their orders: 1st order cut-sets, 2nd order cut-sets, etc. In our case study, one cannot expect a cut set equal to or higher than 5, Table 2.

Generally, the determination of the logical cut-sets is not an easy task for large networks. Many valuable R&D research work is available in the literature regarding algorithms to determine logical cut-sets in large networks (Guangban Bai et al., 2016).

6.1 1st Order Cut-Sets

Three transitions have been identified in the 1st order minimal cut-set. Any loss of these identified links results in a loss in the NCO. The set of the 1st order critical transitions, $\overline{S^1}$, is described by:

$$\overline{S^1} = \overline{l_{1,2}} + \overline{l_{1,6}} + \overline{l_{6,8}} \tag{3}$$

Where; $\overline{l_{i,j}}$ refers to the loss of the link between nodes (i, j) while "$\bullet$" and "$+$" are the Boolean operators intersection "$\cap$" and union "$\cup$", respectively.

6.2 2nd Order Cut-Sets

Similarly, the set of the 2nd order logical cut-sets, $\overline{S^2}$, is described by:

$$\begin{aligned}
\overline{S^2} \quad &= \left(\overline{l_{1,10}} \bullet \overline{l_{3,10}}\right) + \left(\overline{l_{1,10}} \bullet \overline{l_{6,7}}\right) + \left(\overline{l_{1,10}} \bullet \overline{l_{7,10}}\right) \\
&+ \left(\overline{l_{2,5}} \bullet \overline{l_{2,9}}\right) + \left(\overline{l_{2,5}} \bullet \overline{l_{3,10}}\right) + \left(\overline{l_{2,5}} \bullet \overline{l_{4,5}}\right) + \left(\overline{l_{2,5}} \bullet \overline{l_{5,8}}\right) \\
&+ \left(\overline{l_{2,9}} \bullet \overline{l_{3,10}}\right) + \left(\overline{l_{2,9}} \bullet \overline{l_{4,9}}\right) + \left(\overline{l_{2,9}} \bullet \overline{l_{8,9}}\right) \\
&+ \left(\overline{l_{3,4}} \bullet \overline{l_{3,7}}\right) + \left(\overline{l_{3,4}} \bullet \overline{l_{3,10}}\right) + \left(\overline{l_{3,4}} \bullet \overline{l_{4,5}}\right) + \left(\overline{l_{3,4}} \bullet \overline{l_{4,9}}\right) \\
&+ \left(\overline{l_{3,7}} \bullet \overline{l_{3,10}}\right) + \left(\overline{l_{3,7}} \bullet \overline{l_{5,8}}\right) + \left(\overline{l_{3,7}} \bullet \overline{l_{6,7}}\right) + \left(\overline{l_{3,7}} \bullet \overline{l_{7,10}}\right) + \left(\overline{l_{3,7}} \bullet \overline{l_{8,9}}\right) + \left(\overline{l_{3,10}} \bullet \overline{l_{7,10}}\right) \\
&+ \left(\overline{l_{4,5}} \bullet \overline{l_{4,9}}\right) + \left(\overline{l_{4,5}} \bullet \overline{l_{5,8}}\right) + \left(\overline{l_{4,9}} \bullet \overline{l_{8,9}}\right) + \left(\overline{l_{5,8}} \bullet \overline{l_{8,9}}\right) + \left(\overline{l_{6,7}} \bullet \overline{l_{7,10}}\right)
\end{aligned} \tag{4}$$

6.3 3rd Order Cut-Sets

In the category of the 3rd order transitions, the set of triplet failure cut-set is empty.
$\overline{S^3} \quad = \phi$

6.4 4th Order Cut-Sets

In this category, one can identify four logical cut-sets. The set of 4th order transitions, $\overline{S^4}$, is defined as following:

$$\begin{aligned}\overline{S^4} &= \left(\overline{l_{1,10}}\bullet\overline{l_{2,5}}\bullet\overline{l_{3,4}}\bullet\overline{l_{8,9}}\right)+\left(\overline{l_{1,10}}\bullet\overline{l_{2,9}}\bullet\overline{l_{3,4}}\bullet\overline{l_{5,8}}\right)+\left(\overline{l_{2,5}}\bullet\overline{l_{3,4}}\bullet\overline{l_{6,7}}\bullet\overline{l_{8,9}}\right)\\ &+\left(\overline{l_{2,9}}\bullet\overline{l_{3,4}}\bullet\overline{l_{5,8}}\bullet\overline{l_{6,7}}\right).\end{aligned} \tag{5}$$

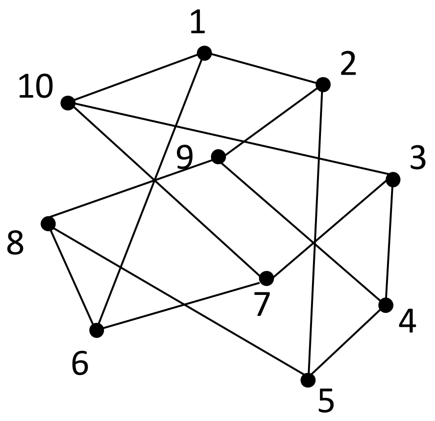


Fig. (1)
A schematic representation of a network

e_{ij}^{1}	1	2	3	4	5	6	7	8	9	10
1	0	1	0	0	0	1	0	0	0	1
2	1	0	0	0	1	0	0	0	1	0
3	0	0	0	1	0	0	1	0	0	1
4	0	0	1	0	1	0	0	0	1	0
5	0	1	0	1	0	0	0	1	0	0
6	1	0	0	0	0	0	1	1	0	0
7	0	0	1	0	0	1	0	0	0	1
8	0	0	0	0	1	1	0	0	1	0
9	0	1	0	1	0	0	0	1	0	0
10	1	0	1	0	0	0	1	0	0	0

Table (1-a)
The binary topological connectivity tensor (1st order)

e_{ij}^{2}	1	2	3	4	5	6	7	8	9	10
1	0	0	1	0	1	0	1	1	1	0
2	0	0	0	1	0	1	0	1	0	1
3	1	0	0	0	1	1	1	0	1	1
4	0	1	0	0	0	0	1	1	0	1
5	1	0	1	0	0	1	0	0	1	0
6	0	1	1	0	1	0	0	0	1	1
7	1	0	1	1	0	0	0	1	0	1
8	1	1	0	1	0	0	1	0	0	0
9	1	0	1	0	1	1	0	0	0	0
10	0	1	1	1	0	1	1	0	0	0

Table (1-b)
The binary topological connectivity tensor (2nd order)

e_{ij}^{3}	1	2	3	4	5	6	7	8	9	10
1	0	1	1	1	1	1	1	1	1	1
2	1	0	1	0	1	1	1	1	1	0
3	1	1	0	1	0	1	1	1	0	1
4	1	0	1	0	1	1	1	0	1	1
5	1	1	0	1	0	1	1	1	0	1
6	1	1	1	1	1	0	1	1	1	1
7	1	1	1	1	1	1	0	0	1	1
8	1	1	1	0	1	1	0	0	1	1
9	1	1	0	1	0	1	1	1	0	1
10	1	0	1	1	1	1	1	1	1	0

Table (1-c)
The binary topological connectivity tensor (3rd order)

e_{ij}^{4}	1	2	3	4	5	6	7	8	9	10
1	0	1	1	1	1	1	1	1	1	1
2	1	0	1	1	1	1	1	1	1	1
3	1	1	0	1	1	1	1	1	1	1
4	1	1	0	0	0	1	1	1	0	1
5	1	1	1	0	0	1	1	1	1	1
6	1	1	1	1	1	0	1	1	1	1
7	1	1	1	1	1	1	0	1	1	1
8	1	1	1	1	1	1	1	0	1	1
9	1	1	1	0	1	1	1	1	0	1
10	1	1	1	1	1	1	1	1	1	0

Table (1-d)
The binary topological connectivity tensor (4th order)

e_{ij}^{5}	1	2	3	4	5	6	7	8	9	10
1	0	1	1	1	1	1	1	1	1	1
2	1	0	1	1	1	1	1	1	1	1
3	1	1	0	1	1	1	1	1	1	1
4	1	1	1	0	1	1	1	1	1	1
5	1	1	1	1	0	1	1	1	1	1
6	1	1	1	1	1	0	1	1	1	1
7	1	1	1	1	1	1	0	1	1	1
8	1	1	1	1	1	1	1	0	1	1
9	1	1	1	1	1	1	1	1	0	1
10	1	1	1	1	1	1	1	1	1	0

Table (1-e)
The binary topological connectivity tensor (5th order)

6.5 Loss of Nominal Operability Expression

Having identified the totality of the critical transitions and determined the corresponding logical cut-sets, one can proceed to assess the probability of the event "Loss of Nominal Operability" of the network.

The overall network set of critical transitions is:

$$\overline{S} \quad = \overline{S^1} + \overline{S^2} + \overline{S^3} + \overline{S^4} \, . \tag{6}$$

Where; $\overline{s^n}$ refers to the set of critical subsets of the n^{th} order and "$+$" is the Boolean operators and union "$\cup$".

The loss of nominal operability, $\overline{S}$, is logically described by 32 logical cut-sets, Table 2.

Table 2: Number of critical cut sets classified according to their order**.**

	1st Order	**2nd Order**	**3rd Order**	**4th Order**
Cut-sets	3	25	0	4

6.6 Loss of Nominal Operability Probability

For simplicity sack, we assume that: nodes do not fail and links are identical. The application involves identical links whose failure rates are equal to $10^{-4} h^{-1}$ and treats two situations: with repair rates equal to $\mu_0 = 10^{-1} h^{-1}$ and with stressed repair rates equal to $\mu_{stressed} = 10^{-3} h^{-1}$. This is expressing two operating situations, respectively: the normal operation situation and a crisis situation (the network is stressed by a threat). The likelihood of the loss of the NCO in both situations are compared in Figure 2-a. The time profiles are almost similar in both situations, for short time, but significantly diverse after 10 hrs. The asymptotic likelihood of losing the NCO increases by almost two decades under stress.

We may take advantage of the assumption that links are identical, as well, and express the loss of nominal operability as a function of one-single link failure probability (S-L unavailability), Figure 2-b. The resultant profile, Figure 2-b is a characteristic curve. It characterises this specific network.

This academic case study demonstrates the applicability of the binary topological model and gives some indications about its originality and potentialities.

We would still like to put the proposed model in comparison with some other well-known and widely used approaches in network robustness/connectivity analysis. However, an exhaustive comparative assessment is out of scope for this introductory paper.

A more exhaustive comparative study should be the subject of a specific paper to prepare. In the following section §7, we report on a brief comparative assessment with the "effective graph resistance" approach, widely used to assess network robustness.

7. Comparison with the Effective Graph Resistance Approach

The effective graph resistance is selected to perform a brief comparative assessment with the topological binary model, for two reasons: both are proposing metrics to measure the network global connectivity and both use algebraic techniques.

The use of the tensors of different orders by the topological binary model and the graph Laplacian by the effective graph resistance show an evident similarity between both models. That would most likely produce a meaningful comparative assessment.

Ellens et al. (2011) proposed a metric, the effective graph resistance, as highly valuable in the analysis of various network problems, such as vulnerability, robustness and criticality of the network.

The notion of effective graph resistance is driven from the field of electric circuit analysis where it is defined as the accumulated effective resistance between all pairs of some given vertices. The effective graph resistance is also called Kirchhoff index, named after Kirchhoff's circuit laws.

The fundamental notions of the effective graph resistance are briefly laid down in the following section before proceeding to the comparison between both approaches.

7.1 Definition of Effective Graph Resistance

The formal definition of the effective graph resistance is the sum of pairwise effective resistances, which measures, in some way, the connectivity between two vertices (Klein et al., 1993) . The pairwise effective resistance takes both the number of paths between any two vertices and their length into account. Subsequently, the number of back-up paths as well as their quality is considered (Ellens et al., 2011).

For a simple undirected graph $G = (V, E)$ the Laplacian Q is defined as the difference $\Delta - A$ of the vertices degree matrix Δ and the adjacency matrix A, such as:

$$Q_{ij} = \begin{cases} \delta_{ii}, & \text{if } i = j, \\ -1, & \text{if (i, j)} \in E, \\ 0, & \text{otherwise} \end{cases} \tag{7}$$

Where δ_{ii} is degree of vertex *i*.

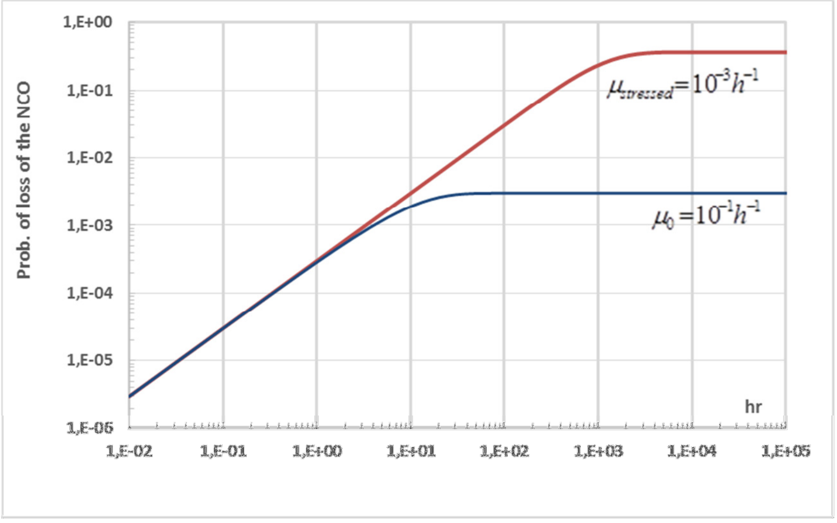


Figure 2-a. Loss of the NCO time profile ($\lambda = 10^{-4}h^{-1}$).

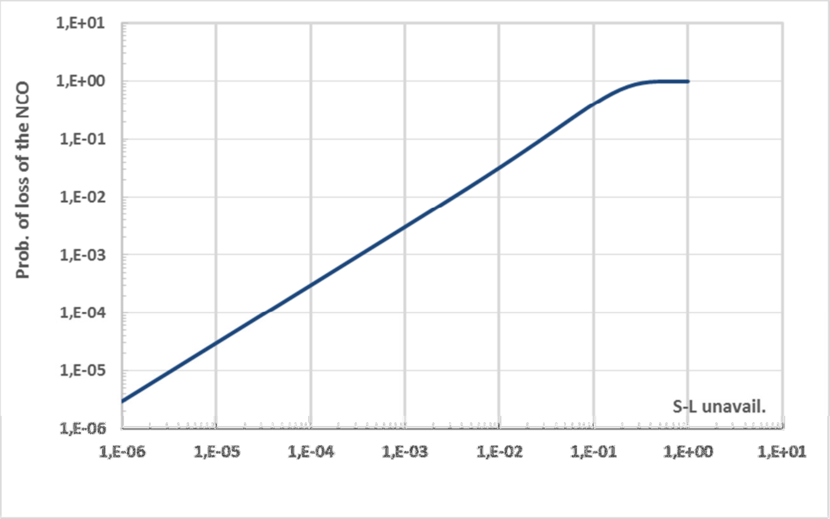


Figure 2-b. The loss of the network NCO vs the single link unavailability.

For a graph with non-negative weights w_{ij} of edges, the weighted Laplacian $L = S - W$, where W is the weighted matrix w_{ij} and S is the diagonal matrix of strengths $s_{ii} = \sum_{j=1}^{N} w_{ij}$.

A good survey on the Laplacian is given in Mohar (1991) while more information about graph spectra are available in P. Van Mieghem (2011).

For our purpose, we have applied the graph Laplacian, Eq.(7), rather than the weighted Laplacian.

The effective resistance R_{ij} between nodes *i* and *j* is computed as:

$$R_{ij} = Q_{ii}^{+} - 2Q_{ij}^{+} + Q_{jj}^{+}, \tag{8}$$

where Q^{+} is the generalized inverse of *Q* obtained by the Penrose pseudo-inverse operator (Moore, 1920). Subsequently, the effective graph resistance R_G of a network is computed by summing up all the effective resistances between all pairs in a network

$$R_G = \sum_{i=1}^{N}\sum_{j=1}^{N} R_{ij} \, . \tag{9}$$

Ellens et al. (2011) suppose that the effective graph resistance is a good measure for network "robustness".

However, it is important to understand how Ellens et al. use the term "robustness". Ellens (Ellens et al., 2011) states that "the effective graph resistance strictly decreases when edges are added or edge weights are increased.

Algebraic connectivity for example does not show this strict monotonicity" and adds "complete graphs are most robust, unconnected graphs least, trees are the least robust connected graphs, star graphs are the most robust trees, and path graphs are the least robust."

Indeed, Ellens et al. use "robustness" to express the "connectivity": "adding edges" or "increasing edges weight."

We will use the term "connectivity" rather than "robustness" because it is in fact the object of our measuring efforts. Still, we admit that higher is the connectivity of a network, higher is its robustness. But, network robustness is not just a connectivity.

7.2 Critical Transitions Identification via Effective Graph Resistance

The effective graph resistance can then be used to determine the criticality of components in a network as used by Koc et al. (2014). The criticality of a link *l* in a network *G* is determined by the relative increase in the effective graph resistance $\Delta R_G(l)$ that is caused by the failure of link *l*:

$$\Delta R_G(l) = \frac{R_{G-l} - R_G}{R_G}, \tag{10}$$

where R_{G-l} is the effective graph resistance of the network that is obtained from *G* by removing particular link *l*. The most critical links are associated to the highest increase in the effective graph resistance ΔR.

7.3 Verification of Critical Transitions Identification via Effective Graph Resistance (A Case Study)

Connectivity order was calculated for network described and mapped in Figure 1 in each case, when one link ($M-1$ analysis) or couple of links (all possible combinations; $M-2$ analysis) are assumed to be failed; here M is the number of links / edges in the network.

Ranks were assigned to the links and the couples of links regarding the connectivity order, i.e., the loss of link $l_{1,2}$ or $l_{6,8}$ leads to a connectivity order equal to seven, thus, ranks of these links are equal to 1.5, rank of link $l_{1,6}$ is equal to 3 (connectivity order is equal to 6), and so on. Ranks of all 15 links are presented in Figure 3, ranks of couples of links (associated to the increase in connectivity order, but excluding combinations containing links $l_{1,2}$, $l_{1,6}$ and $l_{6,8}$) are presented in Figure 4.

On the other hand, effective graph resistance was calculated in each case, when one link or couple of links (all possible combinations) are assumed to be failed, as well, and compared with the nominal R_G of the initial network (Figure 1).

All links and couples of links were ranked: link (and couple of links) associated to the highest increase in effective graph resistance has rank equal to 1, and so on. Ranks (up to the increase in the effective graph resistance ΔR) of all 15 links and couples of links which belong to the set of the 2nd order critical transitions ($\overline{S^2}$) are presented in Figure 3 and Figure 4, respectively.

The correspondence of the results obtained by both approaches can be assessed by rank's correlation. Aiming at this, Spearman's rank correlation coefficients were calculated (see Table 3).

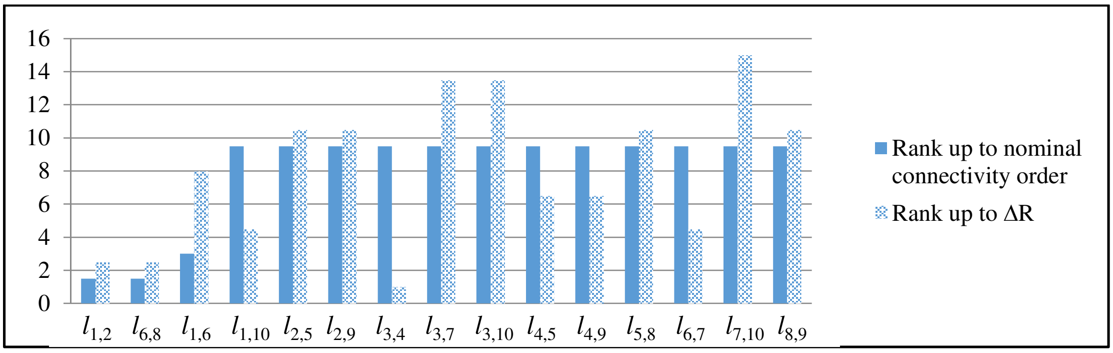


Figure 3. Ranks of all 15 links of the network.

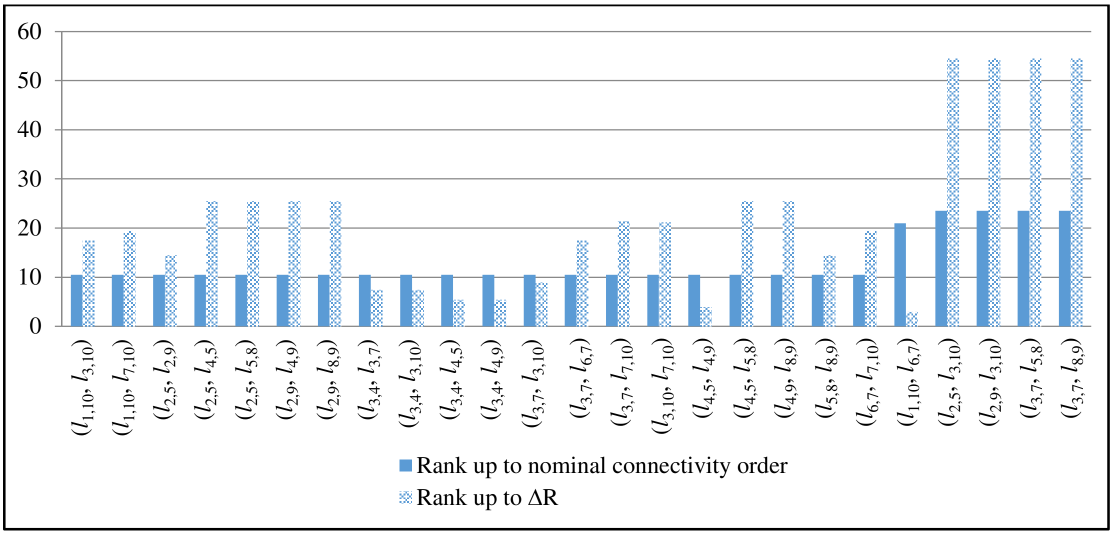


Figure 4. Ranks of couples of links, which belong to the set of the 2nd order critical transitions.

Table 3: Spearman's rank correlation coefficients (or Spearman's rho)**.**

Case of	**Spearman's rank correlation coefficient**	***p*-value**
"*M* – 1" analysis	0.456	0.047
"*M* – 2" analysis	0.521*	$7.4 \cdot 10^{-6}$

* ranks of all combinations (66, in total) were used to calculate Spearman's rank correlation coefficient.

The results (in Table 3) reveal that the correlation can be flagged as significant, since *p*-value $\leq \alpha$, if the level of significance $\leq \alpha = 0.05$. It proves that the variation in the graph resistance aligns with the results obtained by the approach based on nominal connectivity order.

8. Conclusions

A model is proposed and characterised by: the use of an algebraic metric to measure the network connectivity and the use of the critical transition notion. The model allows then to assess the network connectivity and determine the likelihood of the network nominal operability. We call it "the binary topological model".

An academic case study is used in order to illustrate the capability of the binary topological model. A comparison with the effective graph resistance approach is carried on, using the same case study.

The effective graph resistance approach was selected because it seemed to be the closest to the binary topological model, in terms of the use of an algebraic metric in measuring the network connectivity. It is also one of the most cited approaches in assessing the connectivity of networks.

The comparison between the results of both approaches proved a significant correlation according to Spearman's rank correlation analysis. However, it is worthy underlying the following differences between both models:

- the binary topological model allows dynamic calculations of the network operational nominal performance and connectivity,
- the binary topological model results seem more self-consistent.

Regarding the dynamic aspect, the effective graph resistance does not allow in its present state of progress the performance of a time-dependant connectivity modelling. Regarding the consistency of the results of each approach separately, the results of binary topological model seems self-consistent. For example, a clear clustering is observed, Figure 3, in three sets:

- $l_{1,2}$ and $l_{6,8}$; whose separate failures increase the connectivity order from 5 to 7, expressing a degradation of 2 levels in the network connectivity;
- $l_{1,6}$; whose failure increase the connectivity order from 5 to 6, expressing a degradation of 1 level in the network connectivity;
- All the others (12 edges) whose failures don't result in any critical transition.

The effective graph resistance model distinguishes significantly between the edges $l_{3,4}$ and $l_{7,10}$ while the failure of both have the same consequences on the network connectivity as shown by the binary topological model, Figure 3. That seems inconsistent.

The self-consistency of binary topological model is confirmed, as well, when assessing the ranking of cut-sets of 2nd order, Figure 4.

The binary topological model approach seems promising. Still, more formal investigations are necessary in order to explore all its potentialities and limitations. These necessary additional investigations will be the subject of separate papers.

9. Acknowledge

This work has been inspired and stimulated by the participation of the author by his collaboration in the EU projects CIPRNet (grant agreement no 312450) and PREDICT (grant agreement 607697) funded by the EU-FP7. The contents of this paper does not necessarily reflect the official opinion of the European Union or any of the projects cited above. Responsibility for the information and views expressed herein lies entirely on the author(s).

9. References

Albert, R., Barabasi, A.-L., (2002), “Statistical mechanics of complex networks,” Reviews of Modern Physics, vol. 74, 2002.

Barabasi, A.-L., Albert, R. (1999), “Emergence of scaling in random networks.” Science, vol. 286, pp. 509–512, 1999.

Eid, M., Souza de Cursi, E., El Hami, A. (2013) “A topological model to assess networks connectivity and reliability: Recent development.” J. of Polish Safety & Reliability Association, Vol.4, 2(2013)167-178, June 2013. ISNN: 2084-5316.

Eid, M., Souza de Cursi, E., El Hami, A. (2012) “Towards the development of a topological model to assess networks performance: Connectivity, robustness and reliability.” J. of Polish Safety & Reliability Association, Vol.3, 1(2012)23-37, September 2012. ISNN: 2084-5316.

Ellens, W., Spieksmaa, F.M., Van Mieghemc, P., Jamakovic, A. and Kooij R.E. (2011) Effective graph resistance. Linear Algebra and its Applications, vol. 435, pp. 2491-2506.

Guangban Bai, Zhigang Tian , Ming j. Zuo (2016), “An improved algorithm for finding ail minimal paths in a network.” Reliability Engineering and System Safety 150 (2016) 1-10.

Klein, D.J., Randic, M. (1993) “Resistance Distance.” J. of Mathematical Chemistry 12 (1993)81-95.

Koç, Y., Warnier, M., Kooij, R. and Brazier, F. (2014) Structural vulnerability assessment of electric power grids. *Proceedings of the 11th IEEE International Conference on Networking*, *Sensing and Control*, *Miami*, *FL*, pp. 386-391.

B. Mohar (1991), The Laplacian spectrum of graphs, Graph Theory, Combinatorics, and Applications: Proc. Sixth Quadrennial Int. Conf. on the Theory and Applications of Graph, vol. 2, Wiley Interscience, Kalamazoo, 1991, pp. 871–898.

Moore, E.H. (1920) On the reciprocal of the general algebraic matrix. *Bulletin of the American Mathematical Society*, vol. 26, pp. 394–395.

Van Mieghem, P., (2011), Graph Spectra for Complex Networks, Cambridge University Press, Cambridge, UK, 2011

Watts D.J., Strogatz S. H. (1998), “Collective dynamics of small-world networks.” Nature, vol. 393, pp. 440–442, 1998.

Enhancing System Preparedness by the Method of Sequence Rationale to Perform Heterogeneous Repair Works in Time

Andrey Kostogryzov, Pavel Stepanov,
Main Scientific Research Test Center (MSRTC) and Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences (FRC CSC RAS), Vavilova Street 44, bld. 2, 119333 Moscow, Russia

Andrey Nistratov,
The Russian Power Agency of Ministry for the Power Generating Industry,
Shepkina Street 40, bld. 1, 129110 Moscow, Russia

George Nistratov, Sergey Klimov,
The Research Institute of Applied Mathematics and Certification,
For correspondence: Vinnitskaja Street 15, App. 135, 119192 Moscow, Russia

Leonid Grigoriev
The Gubkin Russian State University of Oil and Gas, 65 Leninsky Prospect, 119991 Moscow, Russia

Abstract

For services supply continuity in critical system several works should be performed by one repair brigade in crossed time. And conditions for performing different repair works are characterized by uncertainties. There exists given term for each work and possible damages if the performance of works isn't well-timed. Taking into account these factors the sequence of performing heterogeneous repair work essentially influences the security and/or efficiency of system. For systems the method of sequence rationale to perform heterogeneous repair works in time are proposed. The rational sequence of works is defined by criteria of timeliness on the base of the best choice from different dispatcher technologies and the used parameters (such as distribution work calls types on priorities, distribution of calls priorities on groups, appointment of technologies inside of groups). Effects are demonstrated by example.

Keywords: criteria, efficiency, model, probability, repair, system, technology, timeliness .

1. Introduction

For critical system a necessity of performing in time a set of heterogeneous repair work to services supply continuity exists. In practice the sequence of calls performing is defined, as a rule, by the repair brigade (as it is conveniently) or under subjective chief instructions. In practice fop system preparedness there is no purposeful system coordination with background, frequency of occurrence of those or other heterogeneous calls, time of performance of repair work, the possible missed benefit, losses or damages which can follow because of delays and exceeding of repair terms.

In the present article a possibility of enhancing system preparedness is researched. Dozens years ago the queueing theory repair brigades were considered only as examples of serving systems for performing the flow of repair calls [1-4]. Here are researched the multiparameter dispatcher technology allowing to combine existing technologies, the formal requirements to timeliness of performing repair works, the criterion and the method to optimize sequence of performing heterogeneous repair work. The method is based on comparison and rational use of essentially differing properties of usual dispatcher technologies with relative and absolute priorities, technology of batch performing and the proposed multiparameter technology with a combination of the listed technologies (the two last technologies have been researched earlier by authors of this article in another applications [3, 5-6,8-23]).

2. About the criterion of timeliness

In practice an exceeding of repair terms may lead to problems with system security end efficiency, to possible losses or damages which can follow because of delays. In general cases the criteria of timeliness in conditions of uncertainties are defined formally as follows.

Definition of criterion 1. Works of i-th type are considered to be well-timed if average full performing time of calls of i-th type taking into account delays does not exceed set $T_{given.i}$, i.e. if $T_{full.i1} \leq T_{given.i.}$.

Definition of criterion 2. Works of i-th type are considered to be well-timed, if probability of well-timed performing works by calls of i-th type during the required term $T_{given\ i}$ is not below against admissible probability $P_{tim.i}=P\ (t_{full.i} \leq T_{given.i}) \geq P_{adm.i}$ where the random variable $t_{full.i}$ characterizes full time of performing works of i-th type taking into account delays.

An example of formal probability interpretation of criterion 1 and 2 in application to different types of works (types from 1 to I) is illustrated by Figure 1. The timeliness for repair works of i-th type is estimated by probability values: for criterion 1 - $T_{full.i}$ the 1st moment (average) of full performing time of calls of i-th type taking into account delays; for criterion 2 - $P_{timi}(T_{given\ i})$ – probability of well-timed performing works by calls of i-th type during the required term $T_{given\ i.}$ If $R_i(T_{given.i})$ is probability of exceeding requirements to timeliness of performing calls of i-th type, than $R_i(T_{given.i})=1-P_{tim.i}(T_{given.i})$, A risk of exceeding requirements to timeliness is estimated considering damages.

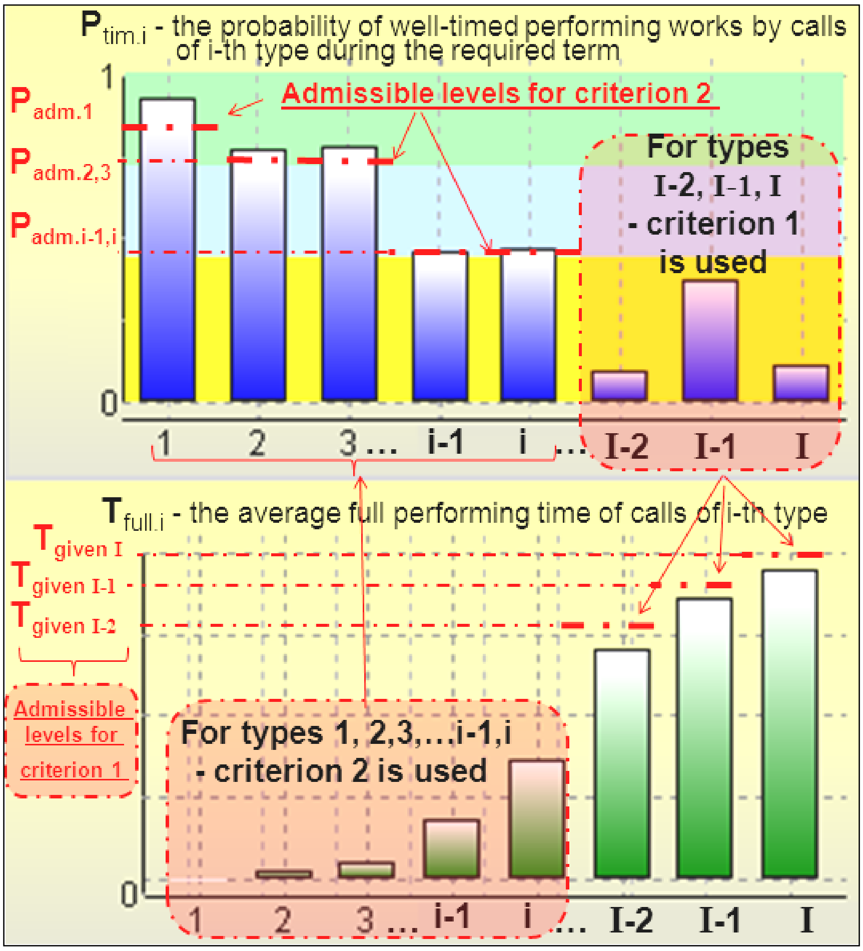


Figure 1. An example of formal illustration of criterion 1 and 2

The criterion 2 sets more hard terms (as a rule $P_{adm.i}$ ≥0.8*)* and is used when completion of calls works should be finished strictly before required time.

3. About ideas for improving repair works in time and enhancing system preparedness in conditions of uncertainty

3.1 Analysis of typical and proposed dispatcher technologies

The typical mode of repair for systems is the following. The repair brigade performs gathered calls for operating repair during a shift (or several shifts). A shift can proceed day, half-day, 8 hours or other established period of time. In a context of this approach brigades are considered as one continuously working brigade for serial performing calls for repair works. I.e. the brigade operates as one-linear system of serial service of calls flow. For large systems calls queue can be accumulated. The formal order of a choice from queue a following repair call is called dispatcher technology.

Leaving behind brackets subjective reasons and momentary preferences, we will consider 4 typical dispatcher technologies and their special properties and propose the 5-th multiparameter dispatcher technology.

According to the technology 1 (Techn.1) all calls are performed by the consecutive order “first in - first out” (FIFO) without priorities. Its main property is the average delays for all calls are identical. According to the technology 2 (Techn.2) calls are performed with relative priorities. Calls of higher priority have advantage against calls of the lowest priority, namely: among the calls waiting the beginning of performing, calls of higher priority are performed ahead of calls of the lower priority. The calls with the similar priority are performed in the order FIFO. The call of higher priority can’t interrupt the call performing with lower priority. It means, that the brigade always leads up the begun repair to the end, despite of new call with higher priority. The main valuable property of technology 2 that average delays of repair by calls of the lowest priority are in 3-5 times above (at high loading can be 10 times more), than delays of calls of the higher priority. According to the technology 3 (Techn.3) calls are performed with absolute priorities. In difference from technology 2 new calls of higher priority absolutely interrupt performing of call with a lower priority. The calls with the similar priority are performed in the order FIFO. The interrupted call will be completed from the interrupted point. It means after receiving new call with higher priority the brigade interrupts the begun repair for call with lower priority. And the brigade carries out the completion of the begun repair after the completion of all arrived calls with the higher priorities. The main valuable property of technology 3 that average delays of repair by calls of the lowest priority are in 10-20 times above (at high loading can be more), than delays of calls of the higher priority.

According to the batch technology 4 (Techn.4) calls are performed with natural formation of batches and relative priorities in a batch. The first arrived call forms the first batch. The next batch is formed of the calls which have arrived during total performing time of the previous batch. The next batch of calls starts to be served at once after complete performing all calls of the previous batch. In the batch which has arrived on service, the first call of the highest priority begin to perform. After finishing the complete performance this call another batch calls are performed in serial order FIFO. Repair by all calls which have entered into the served batch, is carried out without interruptions irrespective of new arriving calls. The main valuable property of technology 4 consists in the following. If for technologies 2 and 3 calls of the higher priority have overwhelming advantage for technology 4 this advantage is sharply reduced. As a result average delays of calls of the lowest priority considerably decrease and exceed delays of calls of the higher priority no more, than in 3 times. This valuable property can be effectively used in the technology 5 allowing to combine technologies 2, 3 and 4.

The proposed Technology 5 (Techn.5) is a combination of technologies 2, 3, 4. For Technology 5 all calls are divided on n groups. Calls of the g-th group have higher priority than calls of the e-th group if g<e (e, g = 1,…, n). In each group priorities of calls are relative. For performing calls of *g*-й groups one technology (2 or 4) is established. Between calls *e*-й and *g*-й groups are appointed relative (by technology 2) or absolute priorities (by technology 3) – see Figure 2.

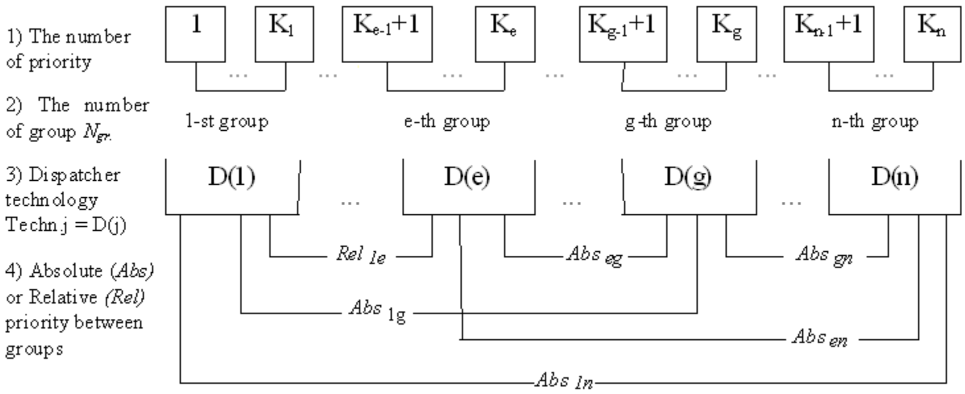


Figure 2. The structure of the proposed combined Technology 5

As a result, by optimization of parameters (such as distribution calls types on priorities, distribution of calls priorities on groups, appointment of technologies inside of groups) the combined Technology 5 is capable to possess in various degree valuable properties of technologies 2, 3, 4 to meet the given requirements for timeliness (see Figure 3).

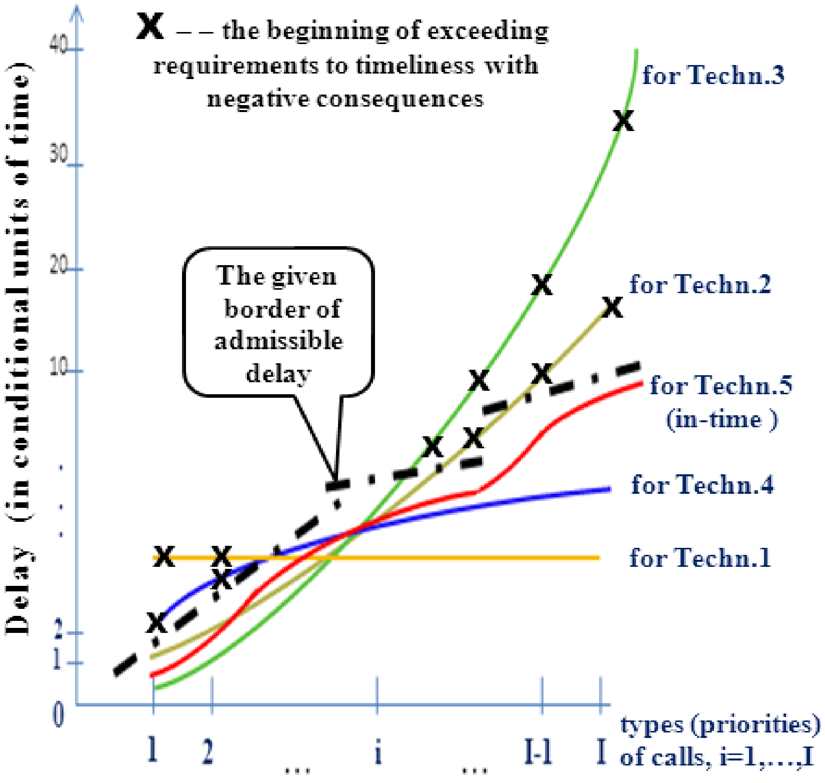


Figure 3. The properties of technologies 1-5 which affect time delays

As a result of comparison by using formal criteria for each shift the most rational technology and optimizing parameters (i.e. sequence of calls performing), on which the minimum of negative consequences is reached at limitations on admissible time for performing heterogeneous repair works, can be revealed – see Figure 4.

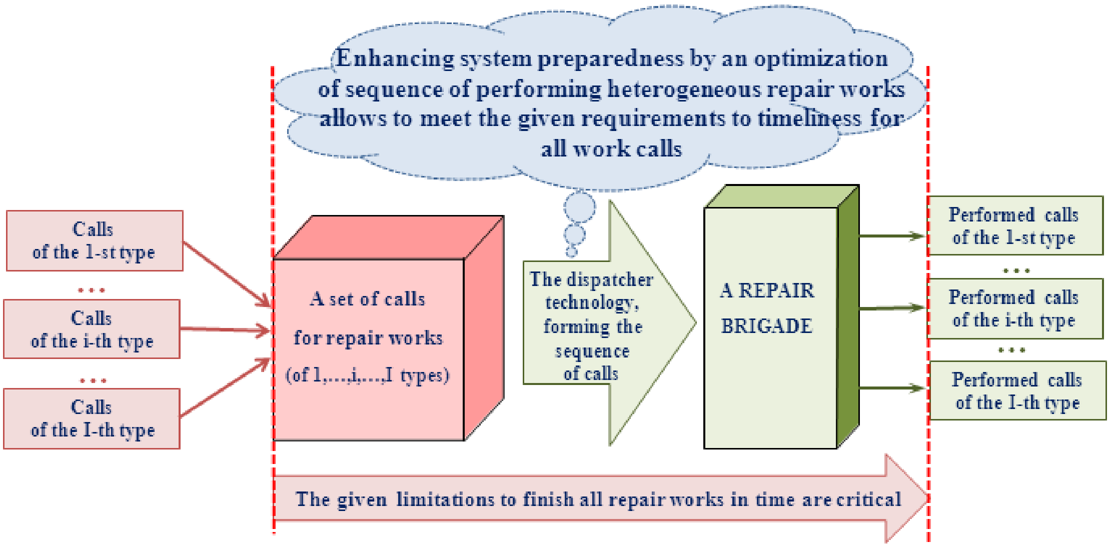

Enhancing system preparedness by an optimization of sequence of performing heterogeneous repair works allows to meet the given requirements to timeliness for all work calls
Calls of the 1-st type
...
Calls of the i-th type
...
Calls of the I-th type
A set of calls for repair works (of 1,...,i,...,I types)
The dispatcher technology, forming the sequence of calls
A REPAIR BRIGADE
Performed calls of the 1-st type
...
Performed calls of the i-th type
...
Performed calls of the I-th type
The given limitations to finish all repair works in time are critical

Figure 4. Illustration of a role and a place of dispatcher technologies in performance of repair work

For systems for which delays in performing repair works are insignificant, there may not be high practical effect from use of the proposed ideas (it should be estimated additionally).

4. Formalization for estimation of possible delays

From the point of engineering view the processes of performing repair works by one brigade are formalized as serving processes of Poisson flows of heterogeneous calls in one-linear system (*M/G/1/∞*) [1-6] with dispatcher technologies 1-5. Heterogeneity of repair work is shown in various average time of calls processing and-or in various admissible terms for calls completion considering delays.

Calls flows of the same type as a rule constitute a compound flow from different sources. In practice, each flow intensity is very low in comparison with the compound flow. In such a situation theorem of Hinchin-Grigolionis [7] is applicable, according to which the compound flow is a Poisson flow.

For investigated typical Technologies 1-5 the full delays in performing calls of i-th type are estimated by probability $P_{timi}(T_{given\ i})$ of well-timed performing during the required term $T_{given\ i}$, approximated by means of incomplete gamma function:

$$P_{tim.i} = P\left(t_{full.i} \le T_{given.i}\right) = \frac{\int_{0}^{\gamma_i^2 T_{given.i}/T_{full.i}} t^{\gamma_i - 1} e^{-t}\, dt}{\int_{0}^{\infty} t^{\gamma_i - 1} e^{-t}\, dt}, \qquad (1)$$

Where

$$\gamma_i = \frac{T_{full.i}}{\sqrt{T_{full.i\,2} - T_{full.i}^2}}.$$

Here $T_{full.i}$ and $T_{full.i2}$ are according to the 1st and 2nd moments of full performing time of calls of i-th type taking into account delays. For estimations of these metrics ($T_{full.i}$ and $T_{full.i2}$) with reference to technologies 1, 2 and 3 it is purposed to use classical models of the queueing theory [1-2, 4]. For technology 4 and 5 the formulas received earlier in the works of this paper [3, 5-6, 8-23] are applicable. Thus as input let know enough frequencies of arriving calls (λ_i) and average time of performing calls of i-th type (β_{i1}). Evaluations can be carried out with use of software tools complexes, for example, the software tools Complex for Evaluation of Information Systems Operation Quality (CEISOQ) - “know how” (registered by Rospatent N2000610272), “Mathematical modelling of system life cycle processes” – “know how” (registered by Rospatent N2004610858), “Complex for evaluating quality of production processes” (registered by Rospatent N2010614145) [8-23].

5. Formalization of a problem of optimization

The following statement of a problem to optimize a sequence of performing heterogeneous repair work is proposed.A sequence of performing heterogeneous repair work is the most rational for a repair brigade according to the technology (from technologies 1-5) and with those parameters on which the minimum of the missed benefit, losses or damages (further - a total expected damage) is reached. The next formalization is proposed: to find minimum of a total expected damage at limitations on admissible time for performing heterogeneous repair works set by criterion 1 or 2 and define the best technology and its parameters minimizing

$$\left(\sum_{i=1}^{I} \lambda i\ \mathrm{Ri(Tgiven.i)Ui}\ (\mathrm{Ind}(\alpha_1)+\mathrm{Ind}(\alpha_2))\right)/\lambda \quad \longrightarrow \quad \underset{\substack{\text{dispatcher}\\ \text{technology}}}{\min},$$

Where λi – frequency of arriving calls of i-th type, $\lambda = \sum_{i=1}^{I} \lambda i$;

$R_i(T_{given.i})$ – probability of exceeding requirements to timeliness of performing calls of i-th type, $R_i(T_{given.i}) = 1 - P_{tim.i}(T_{given.i})$, $P_{timi}(T_{given\ i})$ – probability of well-timed performing works by calls of i-th type during the required term $T_{given\ i}$;
Ui – the expected value of the missed benefit, losses or damages as a result of exceeding requirements to timeliness of performing calls of i-th type;
$Ind(\alpha_1)=1$ if the criterion of timeliness 1 is used, else $Ind(\alpha_1)=0$; $Ind(\alpha_2)=1$ if the criterion of timeliness 2 is used, else $Ind(\alpha_2)=0$.

The decision of the problem is carried out by modelling and estimation of values $R_i(T_{given.i})$ =1 - $P_{tim.i}(T_{given.i})$ with use of the formula (1) by search of all possible dispatcher technologies and variants of parameters (such as distribution calls types on priorities, distribution of calls priorities on groups, appointment of technologies inside of groups). The most rational sequence of performing heterogeneous repair work is the sequence that corresponds to dispatcher technology with the parameters for which the total expected damage is minimal.

At formation of input data for evaluation the frequency of arriving calls of i-th type is defined for the last period of time (for example, for a week or month with proper quantity of calls about repair) as the relation of quantity of calls to duration of the taken period. The decision of an optimization problem is carried out before the beginning of each shift and is valid during the shift.

6. Example of enhancing system preparedness

Researches and development of deposits of hydrocarbons on various depths of Arctic Ocean and in hard uncertainties for security and efficiency is expected. Presence of various threats generates diverse natural and techno-genic risks. Let's put, the large enterprise of oil & gas developments and searches the ways of increasing system efficiency and security at the expense of decreasing costs of operating repair. For the enterprise 8 types of repair work are peculiar. Let’s the exceeding of given terms conducts to the missed benefit equally on each type of repair, i.e. Ui = U. The repair brigade performs works consequently by Technologies 1-3 or by batch Technology 4 (forming batches of arrived calls and performing works without interruptions). It is required to do optimization of sequence of performing heterogeneous repair work and to estimate effects reached. Input for calculation $T_{full.i}$ and $P_{tim.i}(T_{given.i})$ is reflected by Table 1.

Table 1. Input for calculation

i	Type of repair work	Frequency of calls λ_i	Average time of performing calls	Admissible time $T_{given.i}$	Admissible probability for timeliness $P_{adm.i}$ ($T_{given.i}$)
1	To repair and adapt equipment for occurrence of the extreme dangerous and catastrophic phenomena at Arctic ocean and their influences on sea activity and economic objects of a coastal zone	1 day^{-1}	1 hour	8 hours	0.95
2	To repair and adapt equipment for complex control sea and coastal ecological systems	10 week^{-1}	2 hours	8 hours	0.90
3	To repair and adapt equipment for geological-geophysical investigations and exploitation of hydrocarbonic resources of Arctic ocean	3 week^{-1}	3 hours	12 hours	0.90
4	To repair and adapt equipment for	12 week^{-1}	3 hours	16 hours	0.80

	hydrometeorological and a geoinformational support of the sea activity				
5	To repair and adapt equipment for hydrometeorological and navigating-hydrographic support of sea activity	9 week^{-1}	4 hours	30 hours	0.80
6	To repair and adapt equipment for researches of influence of hydrometeorological factors on efficiency of resources development taking into account climate changes	4 month^{-1}	8 hours	33 hours	-
7	To repair equipment for protection of the sea environment against anthropogenous pollution	10 year^{-1}	10 hours	40 hours	-
8	To repair equipment for researches of efficiency of various technologies of development of hydrocarbons deposits and other minerals on the Arctic shelf	6 year^{-1}	12 hours	44 hours	-

Considering, that the expected value of the missed benefit in the conditions of an example is identical (is equal U), the total expected damage can be transformed to a form

$$(\sum_{i=1}^{I} \lambda i\ Ri(Tgiven.\, i)Ui\ (Ind(\alpha_1)+Ind(\alpha_2)))/\lambda\ = U\ (1\text{-}C),$$

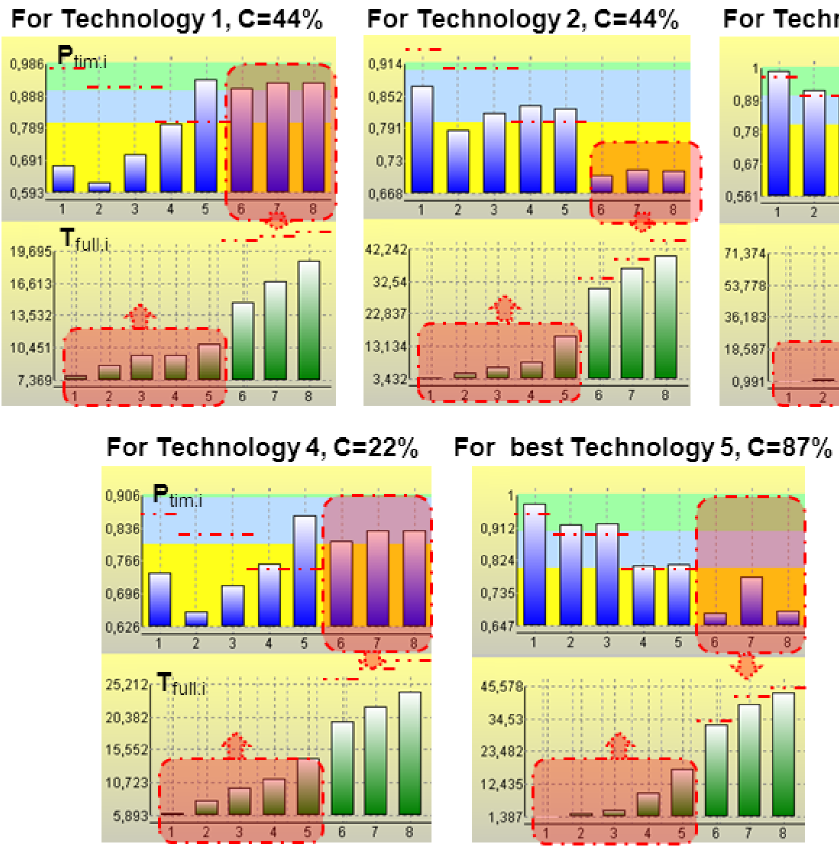
where C is a relative portion of well-timed performed calls

$$C\ =(\sum_{i=1}^{I} \lambda i\, P_{timi}(T_{given\ i})Ui\ (Ind(\alpha_1)+Ind(\alpha_2)))/\lambda\, .$$

For modelling and estimations software tools complexes CEISOQ [8-23] is used – see results on Figure 5.

Results of the analysis have shown, that at the expense of a choice of rational dispatcher Technology 5 and its optimizing parameters relative portion of well-timed performed calls in 2-4 times above in comparison with today applied Technologies 1 and 4. It may be interpret as benefit value in hard conditions of Arctic region. And all repair works will be performed in time, system preparedness is enhanced.

Certainly, in practice different interruptions in works are not always possible (i.e. real effect will be a little bit low), nevertheless this effect taking into account real limitations can be estimated and it will be essential. So, use of Technology 2 with relative priorities, i.e. without interruptions, can't raise portion of well-timed performed calls.



Optimal parameters

-1st group: 1,2,3 types, inside group the Technology 2 is used;

- 2nd group: 4,5,6 types, inside group the Technology 2 is used;

-3rd group: 7,8 types, inside group the Technology 4 is used;

- the calls of 1st group have absolute priorities against the calls of 2nd and 3rd groups;

- the calls of 2nd group have relative priorities against the calls of 3rd groups

Figure 5. Relative portion of well-timed performed calls,
Technology 5 with optimizing parameters is the best

References

[1] Gnedenko B.V. et al. (1973) Priority queueing systems, MSU, Moscow.

[2] Kleinrock L. (1976) Queueing systems, V.2: Computer applications, John Wiley & Sons, New York.

[3] Kostogryzov A.I., Nazarov L.V. (1981) Batch Processing of Calls with Relative Priorities in Queueing System, *News of Academy of Sciences of the USSR Engineering Cybernetics*, No.3, pp. 194-198.

[4] Matweev V.F. & Ushakov V.G. (1984) Queuing systems. MSU, Moscow.

[5] Kostogryzov A.I. (1987) Conditions for Efficient Batch Job Processing of Customers in Priority-Driven Computing Systems Where the Queueing Time Is Constrauned, *Avtomatika i telemehanika*, No.12, pp.158-164.

[6] Kostogryzov A.I. (1992), Study of the Efficiency of Combinations of Different Disciplines of the Priority Service of Calls in the Computer Systems, *Kibernetika i sistemny analiz*, 1992. N1. pp. 128-137.

[7] Grigolionis V. (1963) About approximating stepped processes sum to Poisson processes. *Probability theory and its applications*, V.8, 1963, No.2.

[8] Kostogryzov A.I. (2000) Software Tools Complex for Evaluation of Information Systems Operation Quality (CEISOQ). *Proceedings of the 34-th Annual Event (25-29 September 2000) of the Government Electronics and*

Information Association (GEIA), 2000 Engineering and Technical Management Symposium, USA, Dallas, 2000, pp.63-70.

[9] Kostogryzov A.I. (2001) Modelling Software Tools Complex for Evaluation of Information Systems Operation Quality (CEISOQ). *Proceedings/International Workshop - Information assurance in computer networks: methods, models and arhitectures for Network Security. MMM ACNS 2001*, St.Peterburg, Russia, May 21-23, LNCS, pp.90-101.

[10] Bezkorovainy M.M., Kostogryzov A.I. and Lvov V.M. (2001) Modelling Software Complex for Evaluation of Information Systems Operation Quality CEISOQ. 150 problems of analysis and synthesis and examples for their solutions. *Armament. Policy. Conversion*, Moscow.

[11] Kostogryzov A., Nistratov G. (2004) Standardization, mathematical modelling, rational management and certification in the field of system and software engineering" (80 standards, 100 mathematical models, 35 software tools, more than 50 practical examples). *Armament. Policy. Conversion*, Moscow.

[12] Kostogryzov A.I., Nistratov G.A. (2005) 100 Mathematical Models of System Processes According International Standards Requirements. *Transaction of the XXV International Seminar on Stability Problems for the Stochastic Models*. 2005. Maiority, University of Solerno, Italy, pp. 196-201.

[13] Kostogryzov A., Nistratov G., Kleshchev N. (2006) Mathematical Models and Software Tools to Support an Assessment of Standard System Processes. *Proceedings of the 6th International SPICE Conference on Process Assessment and Improvement*, Luxembourg, pp. 63-68

[14] Kostogryzov A., Nistratov G. (2006) Mathematical Models and Software Tools for Analyzing System Quality and Risks according to standard requirements. *Proceedings of the 6th International scientific school "Modelling and Analysis of safety and risk in complex systems" (MASR – 2006)*, Saint Petersburg, Russia, July 4 - 8, pp. 155-163.

[15] Kostogryzov A.I., Stepanov P.V. (2008) Innovative management of quality and risks in systems life cycle. *Armament. Policy. Conversion*, Moscow.

[16] Grigoriev L.I., Kershenbaum V.Ya. and Kostogryzov A.I. (2010) System foundations of the management of competitiveness in oil and gas complex. National Institute of oil and gas, Moscow.

[17] Kostogryzov A., Krylov V., Nistratov A., Nistratov G., Popov V., Stepanov P. (2011) Mathematical models and applicable technologies to forecast, analyze and optimize quality and risks for complex systems, *Proceedings of the 1st International Conference on Transportation Information and Safety (ICTIS), June 30-July 2,2011*, Wuhan, China, pp. 845-854

[18] Kostogryzov A., Nistratov A., Nistratov G. (2012) Applicable Technologies to Forecast, Analyze and Optimize Reliability and Risks for Complex Systems // *Proceedings of the 6st International Summer Safety and Reliability Seminar*, September 2012, Poland, V.3, No.1, pp. 1-14,

[19] Kostogryzov A., Nistratov G. and Nistratov A. (2012) Some Applicable Methods to Analyze and Optimize System Processes in Quality Management, Total Quality Management and Six Sigma, InTech, pp. 127-196. Available from: http://www.intechopen.com/books/total-quality-management-and-six-sigma/some-applicable-methods-to-analyze-and-optimize-system-processes-in-quality-management

[20] Kostogryzov A., Grigoriev L., Nistratov G., Nistratov A., Krylov V. (2013) Prediction and Optimization of System Quality and Risks on the Base of Modelling Processes, *American Journal of Operations Research*, Special Issue, V.3, No.1A, pp.217-244. Available from: http://www.scirp.org/journal/ajor/

[20] Kostogryzov A., Nistratov G. and Nistratov A. (2013) The Innovative Probability Models and Software Technologies of Risks Prediction for Systems Operating in Various Fields. *International Journal of Engineering and Innovative Technology (IJEIT)*, V.3, Issue 3, September 2013, pp. 146-155. Available from: http://www.ijeit.com/archive.php

[21] A.I. Kostogryzov A.I., Stepanov P.V., Nistratov G.A., Nistratov A.A., Grigoriev L.I., Atakishchev O.I. (2015) Innovative Management Based on Risks Prediction. *Information Engineering and Education Science – Zheng (Ed.). ©2015* Taylor & Francis Group, London, pp. 159-166

[22] Kostogryzov, Grigoriev L., Kershenbaum V., Guseinov Ch., Atakishchev O., Stepanov P. (2015) The probabilistic approach to solve analytical problems in a life cycle of complex systems for developing and transportation hydrocarbon deposits of Arctic regions. *The 3rd International Conference on Transportation Information and Safety, June 25 – June 28, 2015*, Wuhan, P. R. China. pp.682-688

[22] Kostogryzov A., Mahutov N., Stepanov P. at al. (2015) Security of Russia. Legal, Social&Economic and Scientific&Engineering Aspects. The Scientific Foundations of Technogenic Safety. Under the editorship of N. Mahutov N.A. – *Znanie*, Moscow.

[23] Kostogryzov A., Stepanov P., Nistratov A., Nistratov G., Atakishchev O., Kiselev V. (2016) Risks Prediction and Processes Optimization for Complex Systems on the Base of Probabilistic Modeling. *Proceedings of the 2016 International Conference on Applied Mathematics, Simulation and Modelling (AMSM2016), May 28-29, 2016*, Beijing, China, pp. 186-192.

Towards a real-time Structural Health Monitoring of railway bridges

Matteo Vagnoli, Rasa Remenyte-Prescott, John Andrews
Resilience Engineering Research Group, the University of Nottingham
Science Road, University Park,
NG7 2RD, Nottingham, United Kingdom

Abstract

More than 350,000 railway bridges are present on the European railway network, making them a key infrastructure of the whole railway network. Railway bridges are continuously exposed to changing environmental threats, such as wind, floods and traffic load, which can affect safety and reliability of the bridge. Furthermore, a problem on a bridge can affect the whole railway network by increasing the vulnerability of the geographic area, served by the railway network. In this paper a Bayesian Belief Network (BBN) method is presented in order to move from visual inspection towards a real time Structural Health Monitoring (SHM) of the bridge. It is proposed that the health state of a steel truss bridge is continuously monitored by taking account of the health state of each bridge element. In this way, levels of bridge deterioration can be identified before they become critical, the risk of direct and indirect economic losses can be reduced by defining optimal bridge maintenance works, and the reliability of the bridge can be improved by identifying possible hidden vulnerabilities among different bridge elements.

Keywords: Real-time monitoring; Structural Health Monitoring; Bayesian Belief Networks; Steel truss bridge.

1. Introduction

A continuous improvement of the reliability and robustness of the railway system is desirable in order to support the continuous expansion of the railway infrastructure within the transportation network. Indeed, the daily life of millions of people, and the economy of many industrialized countries, strongly depends on the quality of the services provided by the railway system, due to the fact that the railway has high load capacity and speed, and consequently, new passengers and freight companies are using the railways. Railway bridges are a vital element of the railway network as, on average, there is one bridge for every 700 meters of the track in the European railway network (European Commission, 2012). For these reasons, the railway system and, particularly, railway bridges are generally considered as the key system of the transportation Critical Infrastructures (CI) (Murray et al., 2007, Johansson et al., 2013).

Railway bridges are designed to operate for a long period of time, for example more than 35% of the bridges of the European railway network are over 100 years old, and as a consequence, they are exposed to continuously changing environmental threats, such as wind and floods, that can affect safety and reliability of the whole railway network (Le et al., 2013). Moreover, in order to improve railway capacity, railway bridges, especially, old bridges, are being pushed to their physical limit, due to the increased transfer speed, train frequency and length (Reyer et al., 2011; Pipinato et al., 2016).

Generally, the health state of the railway bridge is evaluated by visual inspections, which are carried out at intervals of one to six years. However, during a visual inspection the structure can be examined superficially based on expert knowledge, which can be subjective, and thus the outcomes can be significantly variable in terms of structural condition assessment (Chase, 2004). Hence, real-time Structural Health Monitoring (SHM) methods for railway bridges can significantly improve the reliability of the railway network by providing rapid and reliable information to decision makers regarding the health state of the bridge, and its elements, by considering environmental threats, such as wind, ice, flood, and deterioration mechanisms, as part of the analysis (Brownjohn et al., 2013).

Several SHM studies on railway bridges have been developed in the last years (Doebling et al., 1998) (Kim et al., 2015) (Sanayei et al., 2015) by adopting either: *i)* a model-based approach, which relies on the development of a mathematical model of the bridge (such as a Finite Element (FE) model), in order to assess the health state of the bridge by evaluating the difference between measured and simulated structural parameters; *ii)* a non-model-based method, which relies on the analysis of experimental measurements of the bridge in order to assess its health condition. Furthermore, ensemble methods, which merge together a FE model updating strategy and non-model-based method, have been recently proposed (Zhong et al., 2014; Shabbir et al., 2016). Although, computational time and influence of noisy data can be of concern in these SHM methods, followed by the main limitation that the bridge is not usually studied as a whole system, but the analysis focus is placed on the health state of a bridge element (such as abutments, slabs, joints, girder, bearings, etc.). However, railway bridges can impact the reliability of the whole transportation network, for example a bridge failure can result in the interruption of economic activities, by increasing the vulnerability of the geographic area served by the railway network (FHWA, 2011). Therefore, it is beneficial to analyse it as a system. Hence, in order to ensure safety and reliability of the bridge, and consequently of the whole transportation CI, the analysis of the bridge health state should consider the bridge as a whole system, by evaluating each bridge element and its interactions with other elements, in order to identify possible hidden vulnerabilities and to provide reliable, robust and rapid information to the decision maker (Zio, 2016).

In this paper, an SHM methodology based on a Bayesian Belief Network (BBN) (Rafiq et al., 2015) method for a truss steel railway bridge is proposed, with the aim of assessing the health state of the whole bridge continuously, by taking account of the health state of each bridge element. Indeed, an assessment of how a degradation mechanism affects the health state of the bridge over time is needed in order to prevent bridge failure. In this way, the risk of direct economic losses, such as bridge repair works, and indirect economic losses, such as network unavailability and service delays, that can affect the transportation CI after a bridge failure, can be significantly reduced by defining an optimal maintenance schedule (Lokuge et al., 2013) (Venkittaraman et al., 2014). Furthermore, variations of the bridge behaviour can be pointed out by the proposed BBN monitoring method, as soon as they occur. In this way, bridge managers can take robust and rapid decisions on whether the bridge needs to be take repaired and brought to a new safe condition, or, even if the bridge is exposed to some continuous degradation mechanism and environmental threats, the safety and reliability are still guaranteed. In the proposed method, a Finite Element (FE) model of a truss railway bridge is developed using the SAP2000 software, with the aim of calculating the displacements of the bridge elements due to a static load. The displacements are used as the evidence of the bridge behaviour and, thus, as the input of the BBN. In order to account for the environment effects on the bridge, a deterioration mechanism is introduced by modelling the formation and growth of micro-cracks at the joints, which are difficult to spot during visual inspections (Mehrjoo et al., 2008).

The paper is organized as follows: Section 2 presents the proposed methodology and describes the FE model, the degradation mechanism and the BBN method; Section 3 shows the results of a case study; the conclusions and future work are discussed in Section 4.

2. The proposed BBN methodology

A first step towards a real-time monitoring SHM is proposed by developing a BBN, in order to provide information to bridge managers about the health state of the bridge. In this way, bridge managers are able to take rapid condition-based decisions by evaluating whether the bridge needs to be maintained, or its safety and reliability are still guaranteed. The proposed method is illustrated by developing an FE model of a steel truss railway bridge. The FE model simulates the behaviour of the bridge due to external loads, such as the train load, and furthermore, the effect of the micro-cracks at the joints is analysed as degradation mechanism. A BBN of the bridge is then developed by defining one node in the BBN framework for each major element of the bridge. The behaviour of the bridge, which is obtained by using the FE model, and the information retrieved from interviews with bridge managers and structural engineers is used to define the Conditional Probabilities Tables (CPTs) of the BBN. The proposed method aims to update the health state of the bridge and of its elements automatically, as soon as sensors provide a new measurement of the bridge behaviour. As a result, using the BBN the undesired health state of the bridge can be pointed out by identifying its most degraded element(s).

2.1 The steel truss bridge model

A truss steel bridge has been chosen in this study due to the fact that the degradation mechanisms of the steel, such as corrosion and cracks, can develop rapidly after they have started, and, consequently, an early detection and management of such condition can be of great importance to bridge owners, for reducing the risk of failure and the whole-life cycle cost of the bridge (Katipamula et al., 2005).

The bridge model, which is developed by using the SAP2000 software, is 30m long, 7m wide and 8m high, as shown in Figure 1. The components of the bridge have been realized considering the S355 steel, as this is the steel commonly used in Europe to build steel railway bridges (Pipinato et al., 2016). The bridge is modelled to allow the transit of trains in two directions, and consequently two railway tracks have been modelled by following the most commonly used dimensions (Country Regional Network, 2012). The reference system, used in this paper, is as follows: the side of the bridge at y = 0m, is defined the right side of the bridge, whereas at y = 7m is defined the left side of the bridge.

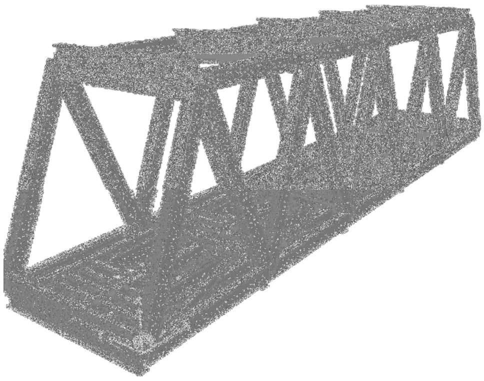


Figure 1. FE model of the steel truss railway bridge

2.2 The micro-cracks degradation mechanism

(Mehrjoo et al., 2008) claims that more than 40% of the steel truss bridges are affected by the formation of micro-cracks at the joint location, which typically can develop around the holes of the bolts or rivets during the assembling phase of the bridge. Furthermore, these micro-cracks are difficult to identify during visual inspections due to their size, and the limitations of visual inspections, which can examine the bridge structure superficially (Chase, 2004). The environmental conditions, which continuously affect the bridge elements through the cycle of loading and unloading, e.g. trains are continuously passing over the bridge, can lead to a continuously increasing size of the micro-cracks. Therefore, the bridge can suffer with fatigue unexpectedly.

The formation and growth of micro-cracks leads to a reduction of the cross sectional area at the joints, and consequently, in order to simulate this degradation mechanism, in this study, the cross sectional area of the degraded bridge elements has been reduced by as much as 30% of its initial value.

Displacements of the bridge joints are considered as the monitored parameter of the bridge behaviour due to the fact that the natural frequency and mode shape analysis have shown to be prone to measurement contamination, and besides displacements could be an interesting variable to be monitored in the near future, due to the technology improvements of sensors (Doebling et al., 1998) (Zhao et al., 2015). A static uniform load of 40 kN/m has been applied to the bridge in order to simulate a train, which has been stopped on the track, and the displacements at the joints are consequently retrieved using the FE model.

The displacements of the top chord on the right hand side of the bridge that have been retrieved using the FE model are depicted in Figure 2. The bridge healthy state is shown by the solid line in Figure 2, whereas, the degraded states, due to the reduction of the cross sectional area of the truss components by the 10% and the 30% of its initial value, are represented by the dotted and dashed lines in Figure 2, respectively. The displacements of the degraded top chord are larger than those of the healthy case, and, moreover, as the bridge degradation grows, the displacements of the top chord on the right hand side of the bridge increase consequently.

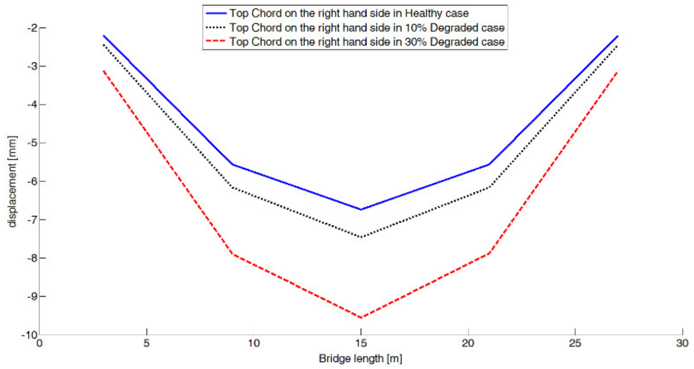


Figure 2. Displacements of the top chord on the right hand side of the bridge model

2.3 Real-time SHM method based on Bayesian Belief Network

In order to develop a SHM method for monitoring the health state of the railway bridge, a BBN is developed. The BBN can monitor the evolution of the bridge health state by considering the health state of its elements, and updating the health state of the whole system, as soon as the virtual sensor system of the FE model provides a new measurement. Hence, the health state of the bridge and its components is updated automatically every time when a new evidence of the bridge behaviour, i.e. a new displacement of each joint location (6 joints on the bottom chords and 5 joints on the top chords, in this case study), is provided by the FE model. The steel truss bridge is analysed within the BBN framework by defining a node for each major element of the bridge, and finally, with the aim of assessing the influence of each bridge element on the health state of the whole bridge, a node representing the health state of the whole bridge is introduced in the BBN.

Figure 3 shows the above mentioned idea, which can be explained following a top-down reasoning process: the FE model is perturbed by introducing the effect of environmental threats, which lead to the deterioration of the bridge materials, such as the growth of the micro-cracks at the joints. A monitoring measurement system of the displacements of the four chords is simulated by using the FE model, which mimics the sensor system on each chord. Therefore, every time that a new measurement of displacements is available, it is used in the BBN framework, where it is processed by a *virtual sensors* node, in order to assess the health state of the correspondent bridge

element. The health state of each bridge element is then evaluated at the following level of the BBN, due to the fact the health state of each bridge element is influenced also by the health state of other bridge elements. Indeed, if a bridge element degrades, other elements are subject to an increasing load. For example, the node called *Top chord left*, which represents the health state of the top chord on the left hand side of the bridge, is influenced by the health state of the other chords, and consequently each *virtual sensors* node is connected to the *Top chord left* node, as shown in Figure 3. Finally, the health state of the whole bridge, which is depicted by the *Bridge health state* node, is affected by the health state of each bridge element.

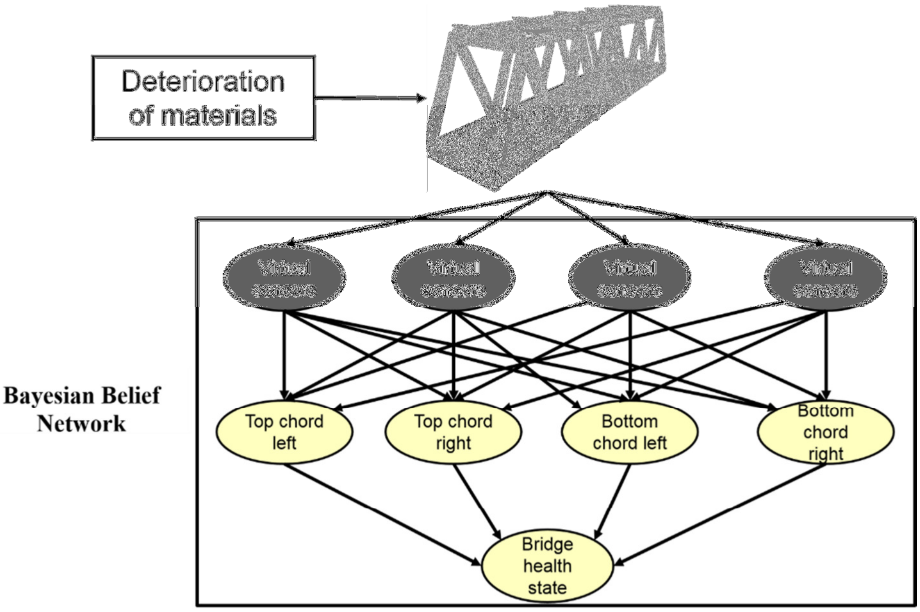


Figure 3. Bayesian Belief Network of the steel truss bridge with influence of the degradation of materials

These dependencies among different elements of the bridge are expressed by using CPTs. The CPTs are completed by merging the information from the simulation of the bridge behaviour by using the FE model and the expert elicitation process (Rafiq et al., 2015) (Andrews et al., 2017). The *virtual sensors* nodes have 6 possible states, depending on the difference between the displacement of the healthy bridge element and those of the degraded element: the healthy state is defined if the difference is less than 1%; then, the 5 degraded states are defined by arbitrarily considering a constant 5% step of the above mentioned difference (e.g. the first degraded state requires a difference between the displacement of the healthy bridge element and those of the degraded element higher than 1% and lower than 5%; the second degraded state requires a difference between 5% and 10%, etc.). Particularly, as soon as the displacements of the bridge element increase, the virtual sensors nodes assess the amount of the increment, and define the adequate health state. On the other hand, three mutually exclusive health states are defined for each bridge element and the whole bridge (i.e., for the nodes on the bottom two levels of the BBN) (Rafiq et al., 2015): *i)* a healthy state, if no corrective or repair action are required; *ii)* a partially degraded state, if some repair or prevention activities are needed, such as methods for restoring the corroded steel to shiny metal; *iii)* a severely degraded state, if strengthening or replacement of bridge elements is required, such as welding of a chord or beam, replacement of elements etc. (Ryall et al., 2000).

3. Modelling results

The proposed SHM method for railway bridges assesses the health state of the bridge element, and the health state of the whole bridge, by updating the health state of each bridge element, using the displacements provided by the FE model. In this way, the reliability of the railway network can be improved by providing rapid and reliable information to bridge managers, regarding the health state of the bridge, by considering environmental threats, such as the deterioration mechanisms. Furthermore, possible hidden vulnerabilities can be pointed out by analysing the bridge as a whole system, i.e. considering the possible influence among different bridge elements.

In this section, an example of the steel truss bridge, which is subject to the degradation of the bottom chord on the left hand side, is presented. In Section 2.2, the degradation mechanism has been presented, by explaining how the micro-cracks at the joints grow due to the effects of external factors, such as passing trains and wind, which constantly apply a load to the bridge structure. Figure 4 shows the evolution of the displacement of the bottom chord on the left hand side of the bridge: the solid dark line shows the displacement of the healthy chord, however, as soon as the material of the bridge degrades due to the environmental effect, and consequently the micro-cracks grow, the displacements become larger, as shown by the dark dotted line in Figure 4. Therefore, as the bridge structure is continuously influenced by the load-unload cycle, the micro-cracks become larger, and consequently, the cross sectional area of the bottom chord on the left hand side decreases. As a consequence, the displacement of the bottom chord on the left hand side increases as the micro-cracks growth, as shown in Figure 4.

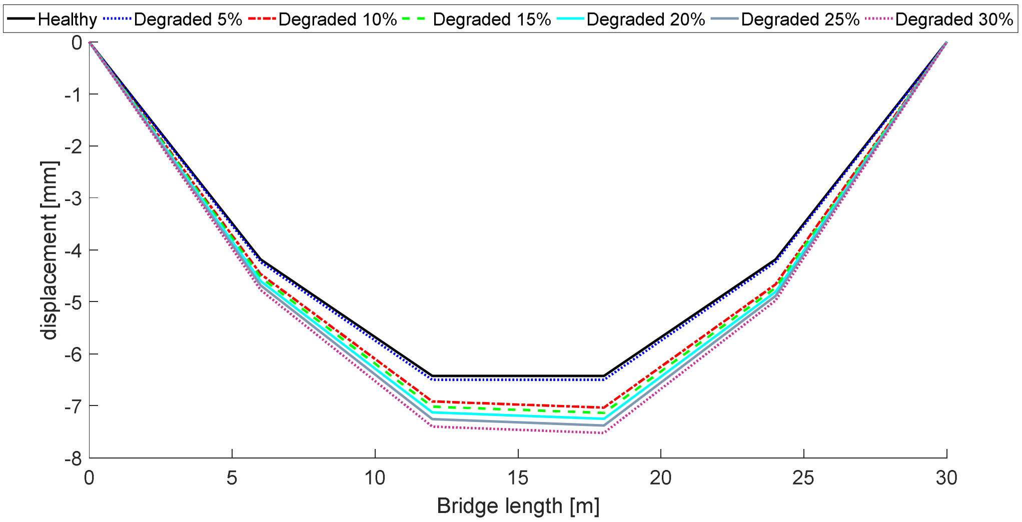


Figure 4. Displacements of the healthy and degraded bottom chord on the left hand side of the bridge model

The seven displacement patterns depicted in Figure 4, which represent the time evolution of the degradation process of the steel truss bridge, are used as the input to the BBN in order to update the health state of the whole bridge, and of its elements.

Indeed, it is worth mentioning that the simulated degradation mechanism of the materials of the bridge, which is shown in Figure 4, is a gradual process that continues over time after its initiation. Therefore, seven types of evidence of the bridge behaviour would be available over time, and as soon as a new measurement is available from the sensor system, the BBN could compute the probability of the health states of each bridge element and, thus, of the whole bridge. Figure 5 shows the real-time evolution of the posterior probability distributions of the health state of the steel truss bridge (node 5) and its components (node from 1 to 4, for the top and bottom chords on the right and left hand side, respectively): the real-time monitoring starts with the steel bridge in the healthy state, as shown by the displacement pattern depicted by the solid dark line in Figure 4 that is the first evidence (Evidence 1 in Figure 5) of the bridge behaviour provided by the measurement system of the FE model. Therefore, the probability of each health state for each bridge element, and for the whole bridge, is consequently computed, and as no degradation is present in all the components of the bridge, the probability of the healthy state is the largest (green bar in Figure 5). Then, the degradation mechanism is initiated, and therefore, the displacements of the bottom chord on the left hand side increase, as shown by the dark dotted line in Figure 4. The new measurement is immediately taken by the BBN (Evidence 2 in Figure 5), which updates the probability of each health state of each bridge element. Figure 5 shows that when Evidence 2 is used by the BBN, the probability of the partially degraded state of the bottom chord on the left hand side (yellow bar of node 4 in Figure 5) increases accordingly. It should be noted that also the probability of the degraded health states of other elements of the bridge (node from 1 to 3), and of the whole bridge health state (node 5), increases due to the influence among different bridge elements. In this way, possible hidden vulnerabilities of other bridge elements can be pointed out consequently.

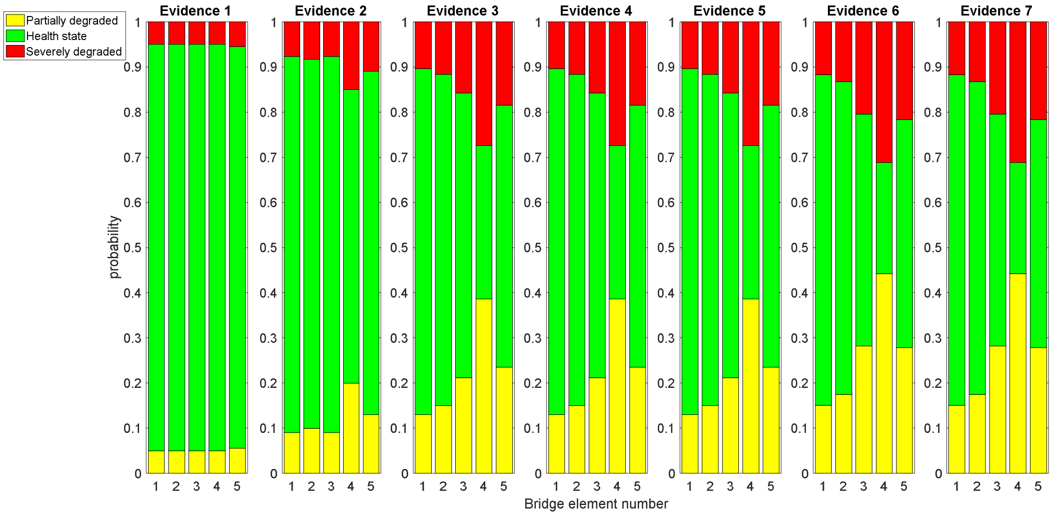


Figure 5. Evolution of the health state of the bridge using displacements as evidence of bridge behaviour

The process of monitoring continues in the same way, by providing the new available measurement of the displacement of the bridge elements to the BBN, which assesses the health state of the element of the bridge, and then of the whole bridge. Generally, Figure 5 shows that the probability of the partially degraded state of each bridge

element (node from 1 to 4) increases and, consequently, the probability of the healthy state of the whole bridge (node 5) decreases. Particularly, the probabilities of the degraded states of the bottom chord on the left hand side (node 4) show the highest increment, as the degradation mechanism directly affects this bridge element. In this way, the health state of the bridge, and of its elements, can be monitored, by identifying the most degraded elements of the bridge. Hence, optimal maintenance programme can be adequately scheduled, based on the degradation level of the bridge elements.

4. Conclusion

Railway bridges are pushed to their physical limits due to continuously changing environmental conditions, such as increasing traffic and climate change that produces extreme events in terms of strong winds and storms. Even though, recently the technology of sensors and data analysis has enhanced significantly, the railway bridges are mainly evaluated by visual inspections. However, in order to improve the reliability of the railway network by providing rapid and reliable information regarding to bridge managers the health state of the bridge, real-time SHM methods are needed. In this way, bridge manager can achieve an optimal management of the bridge, by reducing the risk of economic losses and disruption of the service.

In this paper, a truss steel bridge has been modelled by using the Finite Element software SAP2000. The effects of environmental factors on the health state of the bridge have been assessed by simulating the initiation and growth of micro-cracks of the joints, by gradually reducing the cross sectional area of the truss elements of the bridge. A BBN has been developed in order to monitor the health state of the steel truss bridge, by considering the health state of its elements. The monitoring method has demonstrated to efficiently monitor and assess the evolution of the health state of the bridge elements over time, by updating the health state of the each bridge element as soon as a new evidence of the bridge behaviour is provided by the sensor system. Therefore, bridge managers can be informed with the health condition of the bridge, and optimal maintenance schedule of the bridge can be achieved by identifying the most degraded bridge element. In this way, the reliability of the whole railway network can be consequently improved.

Real-time condition monitoring SHM methods for bridges are needed, in order to reduce the risk of possible losses, the whole life cost of the bridge and the vulnerability of the whole railway network. The proposed method is a first attempt to achieve this aim. Although, a good illustration of monitoring the evolution of the health state of the bridge has been given by the developed method, some further development are needed. For example, the relationship between joints and beams within the same chord need to be considered in the structure of the BBN, and a more robust definition of the CPTs is needed. In addition, the method needs to be tested using sensor measurements on a real bridge.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 642453.

References

Brownjohn, J., Aktan, E. (2013) *Improving resilience of infrastructure: The case of bridges,* Structures Congress 2013: Bridging Your Passion with Your Profession - Proceedings of the 2013 Structures Congress, pp. 1812-1821.

Chase, S.B. (2004) *A long term bridge performance monitoring program*, Proceedings of SPIE - The International Society for Optical Engineering, 5395, pp. 122-127.

Country Regional Network (2012)*, Sleepers and track support*, Engineering standard, track.

Doebling, S.W., Farrar, C.R., Prime, M.B., (1998) *A summary review of vibration-based fault identification methods*, the shock and vibration, Digest, 30 (2), pp. 91–105.

European Commission, (2012) *EU transport in figures*, statistical pocketbook.

Federal Highway Administration, (2011) *Framework for Improving Resilience of Bridge Design*, Publication No. FHWA-IF-11-016.

Johansson, J., Hassel, H., Zio, E. (2013) *Reliability and vulnerability analyses of critical infrastructures: Comparing two approaches in the context of power systems*, Reliability Engineering and System Safety, 120, pp. 27-38.

Katipamula, S., Brambley, M.R., (2005) *Methods for fault detection, diagnostics, and prognostics for building systems - A review, Part I*, HVAC and R Research, 11 (1), pp. 3-25.

Kim, C.-W., Morita, T., Oshima, Y., Sugiura, K., (2015) *A Bayesian approach for vibration-based long-term bridge monitoring to consider environmental and operational changes*, Smart Structures and Systems, 15 (2), pp. 395-408.

Le B., Andrews J. (2013) *Modelling railway bridge asset management*, Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, 227 (6), pp. 644-656.

Lokuge, W., Setunge, S. (2013) *Evaluating disaster resilience of bridge infrastructure when exposed to extreme natural events*, 3rd International Conference on Building Resilience: Individual, Institutional and Societal Coping Strategies to Address the Challenges Associated with Disaster Risk, 17-19 Sep 2013, Heritance Ahungalla, Sri Lanka.

Murray, A. T., Grubesic, T., (2007) Critical Infrastructure: Reliability and Vulnerability, Springer Berlin Heidelberg New York.

Mehrjoo, M., Khaji, N., et al., (2008) *Damage detection of truss bridge joints using Artificial Neural Networks*, Expert Systems with Applications, 35 (3), pp. 1122-1131.

Pipinato, A., Patton, R. (2016) *Chapter 19 - Railway bridges*, In Innovative Bridge Design Handbook, Butterworth-Heinemann, Boston, pp. 509-527.

Rafiq, M.I., Chryssanthopoulos, M.K., (2015) et al., *Bridge condition modelling and prediction using dynamic Bayesian belief networks*, Structure and Infrastructure Engineering, 11 (1), pp. 38-50.

Reyer, M., Hurlebaus, S., Mander, J., Ozbulut, O.E., (2011) *Design of a wireless sensor network for structural health monitoring of bridges*, Proceedings of the International Conference on Sensing Technology, ICST, art. no. 6137033, pp. 515-520.

Ryall, M.J., Parke, G.A.R, Hardi, J.E. (2000) *The manual of bridge engineering*, Thomas Telford, ISBN 0727727745.

Shabbir, F., Omenzetter, P., (2016) *Model updating using genetic algorithms with sequential niche technique*, Engineering Structures, 120, pp. 166-182.

Sanayei, M., Khaloo, A., Gul, M., Necati Catbas, F., (2015) *Automated finite element model updating of a scale bridge model using measured static and modal test data*, Engineering Structures, 102, pp. 66-79.

Vagnoli, M., Remenyte-Prescott, R., Andrews, J., (2017) *A fuzzy-based Bayesian Belief Network approach for railway bridge condition monitoring and fault detection*, European Safety and Reliability Conference (ESREL) 2017, accepted.

Venkittaraman, A., Banerjee, S., (2014) *Enhancing resilience of highway bridges through seismic retrofit*, Earthquake Engineering and Structural Dynamics, 43 (8), pp. 1173-1191.

Zhao, X., Liu, H., Yu, Y., Xu, X., Hu, W., Li, M., Ou, J., (2015) *Bridge displacement monitoring method based on laser projection-sensing technology*, Sensors, 15 (4), pp. 8444-8643.

Zhong, R., Zong, Z., Niu, J., Yuan, S., (2014) *A damage prognosis method of girder structures based on wavelet neural networks*, Mathematical Problems in Engineering, 2014, art. no. 130274.

Zio, E., (2016) *Challenges in the vulnerability and risk analysis of critical infrastructures,* Reliability Engineering and System Safety, 152, pp. 137-150.

List of Authors

APPENDIX:

Seminar Programme

Acknowledgements

We would like to thank many people for their support and contributions to the 52nd ESReDA Seminar. We gratefully acknowledge the members of the 52nd ESReDA Seminar Technical Programme Committee.

We also thank the 52nd ESReDA Seminar Plenary Speakers offering to share their expertise in the field.

We also thank all the contributed paper authors for their submissions and participation.

Finally we would like to thank the respective organisations for supporting the Seminar. It has been made possible by the Lithuanian Energy Institute working together with the support of Vytautas Magnus University.

Local Organization Committee

Dr. Sigitas Rimkevičius	Lithuanian Energy Institute, Lithuania
Prof. Eugenijus Ušpuras	Lithuanian Energy Institute, Lithuania
Prof. Juozas Augutis	Vytautas Magnus University, Lithuania
Dr. Rolandas Urbonas	Lithuanian Energy Institute, Lithuania
Prof. Ričardas Krikštolaitis	Vytautas Magnus University, Lithuania
Dr. Linas Martišauskas	Lithuanian Energy Institute, Lithuania
Dr. Inga Žutautaitė	Lithuanian Energy Institute, Lithuania

Technical Programme Committee

Alzbutas Robertas	Lithuanian Energy Institute, Lithuania
Andrews John	University of Nottingham, United Kingdom
Augutis Juozas	Vytautas Magnus University, Lithuania
Avizienis Algirdas A.	University of California, Los Angeles, USA
Berg Heinz-Peter	Federal Office for Radiation Protection (BfS), Germany
Chateauneuf Alaa	Polytech Clermont-Ferrand Blaise Pascal University, France
Dechy Nicolas	IRSN, France
Demichela Micaela	Politecnico di Torino, Italy
Dundulis Gintautas	Lithuanian Energy Institute, Lithuania
Eid Mohamed	CEA, France
Estel Lionel	Institut National de Sciences Appliquées - INSA, France
Ferreira Luís	Universidade do Porto, Portugal
Flourentzou Nikolas	University of Cyprus – UCY, Cyprus
Kolowrocki Krzysztof	Gdynia Maritime University, Poland
Kopustinskas Vytis	JRC Ispra, Italy
Kortner Henrik	SAFETEC, Norway
Kyriakides Elias	University of Cyprus - UCY, Cyprus
Lannoy André	Institut de Maîtrise des Risques - IMdR, France
Messias Ricardo	Electricity of Portugal - EDP, Portugal
Młyńczak Marek	Wroclow University of Technology, Poland
Nikitakos Nikitas	University of the Aegean, Greece
Nowakowski Tomasz	Wroclow University of Technology, Poland
Pestana Maria	Electricity of Portugal - EDP, Portugal
Piegdon Izabela	Rzeszow University of Technology, Poland
Pietrucha Katarzyna	Rzeszow University of Technology, Poland
Popov Perter	City University of London, United Kingdom
Raza Mohammad	GENERAL ELECTRIC (Switzerland) GmbH, Switzerland
Rosato Vittorio	ENEA, Italy
Setola Roberto	Università CAMPUS Bio-Medico di Roma, Italy
Sfetsos Thanasis	N.C.S.R. DEMOKRITOS, Greece
Skorupka Dariusz	Military Academy of Land Forces, Poland
Smal Tomasz	Military Academy of Land Forces, Poland
Sola Antonio	INGEMAN, Spain
Soszyńska-Budny Joanna	Gdynia Maritime University, Poland
Stoop John	Kindunos, Netherlands
Sýkora Miroslav	Technical University in Prague, Czech Republic
Tchórzewska-Cieślak Barbara	Rzeszow University of Technology, Poland
Theocharidou Marianthi	JRC Ispra, Italy
Urbonas Rolandas	Lithuanian Energy Institute, Lithuania
Ušpuras Eugenijus	Lithuanian Energy Institute, Lithuania
Werbińska-Wojciechowska Sylwia	Wroclaw University of Science and Technology, Poland
Zio Enrico	Politecnico di Milano, Italy
Žutautaitė Inga	Lithuanian Energy Institute, Lithuania

Organizers

European Safety, Reliability & Data Association

European Safety, Reliability & Data Association is an international non-profit association with approximately 35 member organizations comprising companies from different industries, research organizations and universities working within the safety and reliability field.

ESReDA aims to promote the development and the exchange of data, information and knowledge through the promotion of Project Groups (PG) on subjects related to Reliability, Safety and Data Analysis. In this PG's some of the best world specialists in these subjects are able to meet and, in a first time, to aggregate their knowledge and then to disseminate it for the sake of the scientific and technological communities in Europe and around the World. This dissemination can be made by organizing seminars twice per year and publishing the most important results of the Project Groups. Safety and Reliability Engineering is viewed as being an important component in the design of a system. However the discipline and its tools and methods are still evolving and expertise and knowledge dispersed throughout Europe. There is a need to pool the resources and knowledge within Europe and ESReDA provides the means to achieve this.

www.esreda.org

Lithuanian Energy Institute

The Lithuanian Energy Institute was established in 1956. LEI is a technical research centre dealing with energy related research in renewable energy (wind, biomass), smart grids, analysis of security of energy supply, energy efficiency (modelling and consulting), simulation of complex energy systems, energy planning (municipal, regional, country, international level), nuclear safety and radioactive waste management, structural integrity assessment of components and structures, thermal physics and fluid mechanics, combustion engineering, hydrogen storage, plasma research, material research (accredited laboratory), metrology (accredited and notified laboratory), hydrology studies (modelling of hydrodynamic and sediment processes).

www.lei.lt

Vytautas Magnus University

Vytautas Magnus University was established in 1922 and re-established in 1989 in Kaunas, Lithuania. It is one of the most liberal and modern universities in Lithuania and recognized worldwide – ranked among top 800 universities by QS World University Rankings and U-Multirank Ranking. At present, there are 10 faculties at VMU: Arts, Catholic Theology, Economics and Management, Humanities, Informatics, Law, Natural Sciences, Political Sciences and Diplomacy, Social Sciences, Music Academy, over 7,500 students of 50 nationalities and over 480 members of academic staff.

Vytautas Magnus University is the city's hub of academic, scientific and cultural activities, distinguished by its liberal education system (Artes Liberales), humanist spirit, cultivation of creativity and opportunities for wider, more universal enlightenment.

www.vdu.lt/en/

Programme

Vytauto Didžiojo universitetas (Vytautas Magnus University)
S. Daukanto g. 28 (Small Hall, 2nd floor), Kaunas

1st day, Tuesday May 30th, 2017

08.00 – 08.30	**Registration**
08.30 – 09.00	**Welcome to participants** *Juozas Augutis, Rector of Vytautas Magnus University* *Sigitas Rimkevičius, Director of Lithuanian Energy Institute* *Luís Andrade Ferreira, ESReDA President*
09.00 – 10.20	**PLENARY SESSION** *Chair: Eugenijus Ušpuras* **Crisis management and Critical infrastructure protection in Lithuania** *Dalius Labanauskas, Head of National Security and Crisis Management Unit, Office of the Government, Lithuania* **Critical Energy Infrastructure Protection and building resilience in NATO ENSEC COE Agenda** *Artūras Petkus, Head of Strategic Analysis Division, NATO Energy Security Centre of Excellence, Lithuania*
10.20 – 11.20	**SESSION 1: Emergency & Risk Management** *Chair: Luis Andrade Ferreira, Kaisa Simola* ***Safety and Security of Critical Infrastructures with regard to nuclear facilities*** *Heinz-Peter Berg** ***Risk assessment for interconnected Critical Infrastructures: the case of ship-port interface*** *George Leventakis, Nikitas Nikitakos*, Athanasios Sfetsos* ***Some Specifics on Using Probabilistic versus Deterministic Approaches in Emergency Zoning Evaluations*** *Dan Serbanescu**
11.20 – 11.40	**Coffee Break**
11.40 – 13.00	**SESSION 2: CIP & Safety Issues** *Chair: Heinz-Peter Berg, Athanasios Sfetsos* ***Risk informed inspection and decisions making*** Robertas Alzbutas* ***The Importance of Safety Assessment, Reliability and Maintenance for Critical Infrastructures*** Luís Andrade Ferreira* ***Exploring public expectations for aid from critical infrastructure operators*** *Laura Petersen*, Laure Fallou, Paul Reilly, Elisa Serafinelli* **Risk Assessment for Critical Infrastructure** *Inga Žutautaitė, Linas Martišauskas, Ričardas Krikštolaitis, Juozas Augutis*, Vika Juričkaitė, Roberto Setola*
13.00 – 14.00	**Lunch**
14.00 – 15.20	**SESSION 3: CIP & System Safety Engineering** *Chair: Tomasz Nowakowski, Rolandas Urbonas* ***Degradation assessment of bridge components using Structural Health Monitoring*** *Christelle Geara, Alaa Chateauneuf*, Rafic Faddoul* ***Pipe Rupture and Inspection Sensitivity Analysis*** *Gintautas Dundulis, Robertas Alzbutas* ***Energy Management Controller of a Resilient Micro-Grid for Critical Buildings*** *Lenos Hadjidemetriou, Nikolas Flourentzou*, Elias Kyriakides* ***Security of supply analysis of critical energy infrastructures by flow network approaches*** *Vytis Kopustinskas*, Pavel Praks*

15.20 – 15.40	**Coffee Break**
15.40 – 17.10	**ROUND TABLE DISCUSSION: Cyber Security for CI** *Chair: Juozas Augutis, Sigitas Rimkevičius* **The cybersecurity dimension of critical infrastructure** *Vytautas Butrimas , Subject Matter Expert, Research and Lessons Learned Department, NATO Energy Security Center of Excellence, Lithuania* **Cybersecurity of electrical grid** *Marius Celskis, Information Security Manager, the Lithuania Electricity Transmission System Operator: LITGRID AB, Lithuania* **Discussions & Synthesis**
17.30 – 19.00	**ESReDA General Assembly**
20.00	**Gala Dinner at restaurant "Senieji rūsiai" (Vilniaus g. 34, Kaunas)**

2nd day, Wednesday May 31st, 2017

09.00 – 09.40	**PLENARY SESSION** *Chair: Alaa Chateauneuf* **Investigation of seismicity in the Lithuanian territory** *Jurga Lazauskienė, Head of Division of Bedrock Geology, Lithuanian Geological Survey, under the Ministry of Environmental, Lithuania*
09.40 – 10.40	**SESSION 4: MS&A - Natural threats & CI's Resilience** *Chair: Nikitas Nikitakos, Pestana Maria-Luisa* ***Vulnerability Analysis methodology: The expected number of heavy storms and flood vulnerability prediction model of Rio de Janeiro city*** *Eduardo Calixto** ***Integrating the security in the process risk assessment*** *Micaela Demichela** ***A methodological approach for assessing the resilience of the interconnected EU critical infrastructures to climate change*** *Theodoros Katopodis, Athanasios Sfetsos*, Stelios Karozis, Georgios Karavokyros, Georgios Eftychidis, Georgios Leventakis, Ralf Hedel, Ifigenia Koutiva, Costantinos Makropoulos*
10.40 – 11.00	**Coffee Break**
11.00 – 12.20	**SESSION 5: MS&A - Preparedness, Vulnerability & Resilience** *Chair: John Andrews, Ričardas Krikštolaitis* ***Lifetime degradation and interventions for systems under random shocks*** *Dimos C. Charmpis** ***Network's Connectivity Dynamic Modelling using a Topological Binary Model: Critical Transitions Concept*** *Mohamed Eid*, Inga Žutautaitė, Dovilė Rafanavičiūtė* ***Enhancing System Preparedness by the Method of Sequence Rationale to Perform Heterogeneous Repair Works in Time*** *Andrey Kostogryzov*, Pavel Stepanov, Andrey Nistratov, George Nistratov, Sergey Klimov, Leonid Grigoriev* ***Towards a real-time Structural Health Monitoring of railway bridges*** *Matteo Vagnoli*, Rasa Remenyte-Prescott, John Andrews*
12.20 – 12.50	**Closure Session & Next Event** ESReDA General Secretary
12.50 – 14.00	**Farewell Buffet**
14.30	**Guided tour in Kaunas**

Plenary presentations

Tuesday 30th May: 09.40 – 10.20

Crisis management and Critical infrastructure protection in Lithuania
Dalius Labanauskas
Head of National Security and Crisis Management Unit, Office of the Government, Republic of Lithuania

National security is the basis for the prosperity of the State. Only a secure environment can ensure the functioning of a mature democratic constitutional order, sustainable economic growth, the protection of human rights and freedoms, and the viability of civil society. Instability in the world, natural and manmade disasters, large scale migration, humanitarian crises, terrorism, and the disruption of the vital societal functions and of the supply of strategically important resources may have negative consequences for the country. Situations which have occurred because of natural, technical, ecological or social events, the outbreaks of contagious diseases threatening to cause a major danger and threat to the health and life of the majority of the population, the environment, and to disturb public administration or the functioning of critical infrastructure. Such situations may increase in number due to negative consequences caused by the climate change. The prevention of potential threats, dangers and risks, and where it proves impossible to avoid them – the readiness to appropriately counter them using all measures and methods available to the State – steps necessary to strengthen the security of the country and its population. The priority of the Lithuanian government is to make sure that Lithuanian citizens feel safe in their homeland from all possible threats. An overview of the Lithuanian crisis management structures, responsibilities, coordination and information exchange mechanism, and the cooperation between the state and private institutions will be presented.

Dalius Labanauskas joined the Office of the Government of the Republic of Lithuania in 2009. Prior to the current position he was the Head of the Analytical Division in the Crisis Management Centre under the Ministry of National Defence. Since 2010, he has been a member of the Lithuanian Government Emergency Commission.
On an everyday basis, he is involved in risk and threat assessment, information exchange activities among national institutions and international partners, preparation and participation of national as well as international exercises such as NATO CMX. He is also involved in the European Programme for Critical Infrastructure Protection as a Lithuanian representative. In 2013, he was a chair of and is still actively involved in the Council of the European Union Friends of Presidency group, which is in charge of dealing with the EU Integrated Political Crisis Response arrangements and Solidarity Clause implementation.

Tuesday 30th May: 10.20 – 11.00

Critical Energy Infrastructure Protection and building resilience in NATO ENSEC COE Agenda
Dr. Artūras Petkus
Head of Strategic Analysis Division, NATO Energy Security Centre of Excellence,
Republic of Lithuania

Critical Energy Infrastructure has become a convenient target (especially in terms of Hybrid Threats) due to its complexity (fragility of security) and vital significance for the existence of states, effective governance and welfare of the society. Hybrid Threats meanwhile blend elements of diplomacy, clandestine action, disinformation, sabotage and irregular troops to achieve strategic objectives. In other words these are a wide spectrum of hostile acts, where the role of the military component is limited. However these methods are being succesfuly employed to impact proper function of Critical Energy Infrastructure. While hybrid war can take place over several dimensions, it appears clear that Critical Energy Infrastructure and energy industry could be and will be targeted as part of a wider campaign in order to reduce the county's ability and willingness to resist.
Since protection of Critical Energy Infrastructure is primary responsibility of nations, NATO seeks to "continue to develop NATO's capacity to support national authorities in protecting critical infrastructure, as well as enhancing their resilience against energy supply disruptions that could affect national and collective defence, including hybrid and cyber threats" (NATO Warsaw Summit Communique). Working in line with NATO's commitments, NATO ENSEC COE provides expertise in Critical Energy Infrastructure Protection. Main outcomes of Center's activities in this regard will be presented.

Dr. Artūras Petkus joined the Strategic Analysis Division of the NATO Energy Security Centre of Excellence in 2015 as a Head of division. His main areas of responsibility are: performance of energy security related analysis on strategic level; development of methodology and theoretical approach for assessment of energy security risks and threats, contribution to development of NATO ACT Strategic Foresight Analysis Report as well as Framework for Future Alliance Operations Report; contribution to research in field of Energy Security (Overview of energy security in Baltic States, study "Hybrid Conflict and Critical Energy Infrastructure: the Case of Ukraine" etc.).

Wednesday 31st May: 09.00 – 09.40

Investigation of seismicity in the Lithuanian territory
Dr. Jurga Lazauskienė
Head of Division of Bedrock Geology, Lithuanian Geological Survey, under the Ministry of Environmental, Republic of Lithuania

The territory of Lithuania and whole region of Eastern Baltic feature a low seismic activity. Earth's crust of early Precambrian consolidation and significant distances to active tectonic zones causes situation of this kind. Nevertheless, according to historical and instrumental data a few dozens of local earthquakes with intensities reaching VII points (MSK scale) took place in the Baltic countries and adjacent Belarus since 1616 to our days. Two Kaliningrad earthquakes with magnitudes 4.5 and 5.0 stroke Baltic region in 2004 which indicated seismogenic potential of this region. These seismic events indicate that earthquakes may occur in Lithuania as well. Besides manifestation of some local seismic activity in Eastern Baltic, large regional earthquakes generate earth trembling up to intensities IV or V (MSK scale) in this area. For instance, inhabitants of Lithuania have felt trembling from Oslo 1905 earthquake and from earthquakes of Vrancea area in Romania in years 1940, 1977, 1986 and 1990.

The first instrumental seismological observations in Lithuania started in 1970 as Vilnius seismic station was founded. Three analog long period (T=25 s) and three short period (T=1.5 s) seismometers were installed in the territory of Institute of Physics at outskirts of Vilnius. Seismological records were processed in Obninks (Russia) until 1992. Later on, maintenance of station and routine data processing was undertaken by stuff of Institute of Physics. 450 distant and regional seismic events were reported in the seismic bulletin of Vilnius seismic station since 1991 to 1995. No local events were registered in Vilnius seismic station. Operation of Vilnius seismic station was suspended in the beginning of 1999.

The first comprehensive study of seismic activity of Lithuania was carried out in 1988 as a part of re-examination of safety of Ignalina Nuclear Power Plant (INPP). The top twenty-two experts of the Soviet Union concluded that seismic hazard was not assessed properly when INPP has been designed despite local and international regulations. In order to improve the situation the experts proposed to install seismic network and monitor local seismicity. Seismic Alarm System (SAS) and complementary Seismic Monitoring System (SMS) were installed in the INPP in 1999. At the same time Geological Survey of Lithuania took responsibility to process, analyse and store seismological data of the SMS and project of seismological monitoring was initiated there. In 2012, Lithuanian Geological Survey established Seismological Data Center (LGS-SDC) with two broad band seismic stations PBUR (Paburgė, western Lithuania) and PABE (Paberžė, central Lithuania). In addition, data from the SMS are also received regularly. The Lithuanian Geological Survey continued seismic monitoring of Lithuania and adjacent territories. Seismic data were continuously collected from seismic stations in Lithuania and adjacent countries. Four seismic stations are located around the INPP at distances of 30 km. These INPP and Lithuanian Geological Survey two broadband stations together form the current Seismic Monitoring Network of Lithuania.

Lithuania has several important industrial facilities including the decommissioned INPP, Nemunas dam, nitrogen fertilizer factory "Achema" in Jonava, mineral fertilizer factory "Lifosa" in Kėdainiai, oil refinery "Orlen" in Mažeikiai, and liquefied natural gas floating storage and regasification unit terminal in Klaipėda. Therefore, even moderate earthquakes can cause significant damage in such objects. This shows that seismic assessment is important even in such low seismicity regions like Lithuania. Until present, assessments of seismic hazards were performed using various approaches. These assessments were, however, sporadic or they involved partly deterministic seismic hazard assessment – an approach that is no longer considered up-to-date. Until now, seismic hazard maps for entire European continent and Mediterranean region published by Jiménez et al., 2003 and later Woessneret. al., 2015, were considered the most reliable in terms of seismic hazard assessment. Yet continent- scale maps are not always appropriate for small areas like Lithuania. Naturally, it was necessary to perform a new seismic hazard assessment of the Lithuanian territory using, modern probabilistic seismic hazard assessment (PSHA). This assessment had to include all available information from historical and instrumental seismic observation sources. A new map was compiled based on revision of an existing map of seismic hazard over Lithuania. It presented Peak Ground Acceleration (PGA) that can be exceeded within 50 years with probability of 10 %.

Dr. Jurga Lazauskienė is Head of the Department of Bedrock Geology at LGT and an Associate Professor at Vilnius University where she teaches Geodynamics, Geotectonics and Petroleum Geology. She is actively involved in fields of Seismology, Petroleum and Bedrock geology, Geodynamics and sustainable development of natural resources. She is an author of more than 90 oral and poster presentations (75% internationally) and more than 15 publications in the international journals. Since year 2009 dr. Jurga Lazauskienė acts a member of Delegations of Republic of Lithuania for geological and seismo-tectonic issues related to Astravets NPP (Belarus Republic) and Kaliningrad NPP (Russian Federation) sites.

Round table discussion

Tuesday 30th May: 15.40 – 16.10

The cybersecurity dimension of critical infrastructure
Vytautas Butrimas
Subject Matter Expert, Research and Lessons Learned Department, NATO Energy Security Center of Excellence, Republic of Lithuania
Member, National Communications Regulatory Authority Council, Republic of Lithuania

As someone occupied with government information technology (IT) and national security policy for the past 27 years, I have worked in a changing cybersecurity environment that started from dealing with the first hackers invading our IT systems with viruses such as the "Michelangelo" virus of 1991 to worrying about cyber criminals, socially motivated hacktivists and possible activities of cyber "terrorists" to state sponsored cyber-attacks not limited to just IT systems. The appearance of STUXNET, the "denial of computers" attack perpetrated against energy company Saudi Aramco and cyber intrusions that took place in one of Ukraine's regional power grids in the winter of 2015 strongly indicated that critical infrastructures that support national economies and well-being of modern society were now increasingly attractive targets for cyber-attacks. Additionally, the extensive expansion of the capabilities of modern industrial control systems (ICS) made possible by the advances in information and communication technologies (ICT) and their application to the management of complex systems running critical infrastructure has introduced, together with increased efficiencies and cost savings, serious dependencies and vulnerabilities. Vulnerabilities that, due to a lack of understanding of the interrelatedness of increasingly complex systems, have given rise to unintentional incidents. Vulnerabilities, that if known by "the bad guys", may be exploited to execute intentional cyber-related attacks, attacks which are now possible due to the entry of IT in the formerly isolated and proprietary world of industrial control systems (SCADA). The new threats emanating from cyberspace have provided new and broad challenges that range beyond the national level to the international level. Critical infrastructure today has a cross-border or international dimension. Failure at a national level can affect a connected neighboring country. While some worthy and effective efforts are being made by national governments and industry in terms of laws, regulations and standards, they fall short in meeting the international dimension of today's cyber threats. SCADA and ICS environments can no longer be considered safe from today's dynamic threats emanating from cyberspace. This presentation will address implications of any changes to cyberspace environments that have taken place within the last few years that now require responses in the form of shared understanding, restraint, acceptance of responsibility, transparency and cooperation. Proposals for addressing these new threats will also be discussed.

Vytautas Butrimas has been working in information technology and security policy for over 27 years starting from his work as a computer specialist for Prince William County Government in Virginia, to his work on information society development as Vice Minister at the Ministry of Communications and Informatics, Republic of Lithuania. In 1998 he moved on to the Ministry of Defense as Policy and Planning Director where he chaired a task force which prepared Lithuania's first National Military Defense Strategy (approved in 2000). From 2001 to 2011 Mr. Butrimas worked as Deputy Director responsible for IT security at the Communications and Information System Service (CISS) under the MoND. In 2009 he chaired taskforces which prepared the first MoND Cyber Defense Strategy and Implementation Plan. In 2007 (and again in 2012) the President of the Republic of Lithuania appointed him to the National Communications Regulatory Authority Council (RRT-Council) for a 5 year term. He served as Chief Adviser for the Ministry of National Defense with a focus on cyber security policy from 2011-2016 and served on a national task force which wrote The Law on Cybersecurity passed in 2014. In November of 2016 he was posted by the Minister of National Defence to work as Cybersecurity Subject Matter Expert for the NATO Energy Security Center of Excellence in Vilnius. Mr. Butrimas has participated in NATO and National exercises that have included cyber-attacks on critical infrastructure in the scenarios. He has also contributed to various reports, written published articles and been an invited speaker at various conferences on Cyber Security and Defense policy issues.

Tuesday 30th May: 16.10 – 16.40

Cybersecurity of electrical grid
Marius Celskis
Information Security Manager, the Lithuania Electricity Transmission System Operator: LITGRID AB, Republic of Lithuania

Electricity management system. Main grid components - generation, transmission and distribution of electricity. Cybersecurity of informational and operational technology. Rise of attacks on critical infrastructure. Prevalent security threats and countermeasures. Protecting operations at Lithuania's electricity transmission system operator - Litgrid AB.

Marius Celskis is Information Security Manager at the Lithuania Electricity Transmission System Operator: LITGRID AB. Specializing in cybersecurity of industrial control systems (incl. SCADA). Mr. Celskis has a Bachelor's Degree in Electronics Engineering and Business Management from Kaunas University of Technology and holds a number of professional certificates in Industrial Control Systems Security, Information Systems Auditing and Security Incident Handling.

ESReDA events

ESReDA Project Groups Meetings

Monday, 29th May, 10.00-12.00
Lithuanian Energy Institute
Breslaujos g. 3 (Small Hall, 2nd floor, room 202)

PG CI-PR/MS&A-Data meeting will be held on May 29th, 10.00-12.00. The agenda will be circulated by the leader of PG CI-PR/MS&A-Data. The meeting is open to all the 52nd ESReDA Seminar participants. For those interested in participating, please contact PG leader Mohamed Eid (mohamed.eid@cea.fr) in advance.

ESReDA Board of Directors meeting

Monday, 29th May, 15.00-18.00
Lithuanian Energy Institute
Breslaujos g. 3 (Small Hall, 2nd floor, room 202)

The biannual meeting of the ESReDA Board of Directors will be held this afternoon. The agenda will be circulated by the ESReDA General Secretary to ESReDA Directors.

ESReDA General Assembly

Tuesday, 30th May, 17:30-19:00
The 52nd ESReDA seminar auditorium

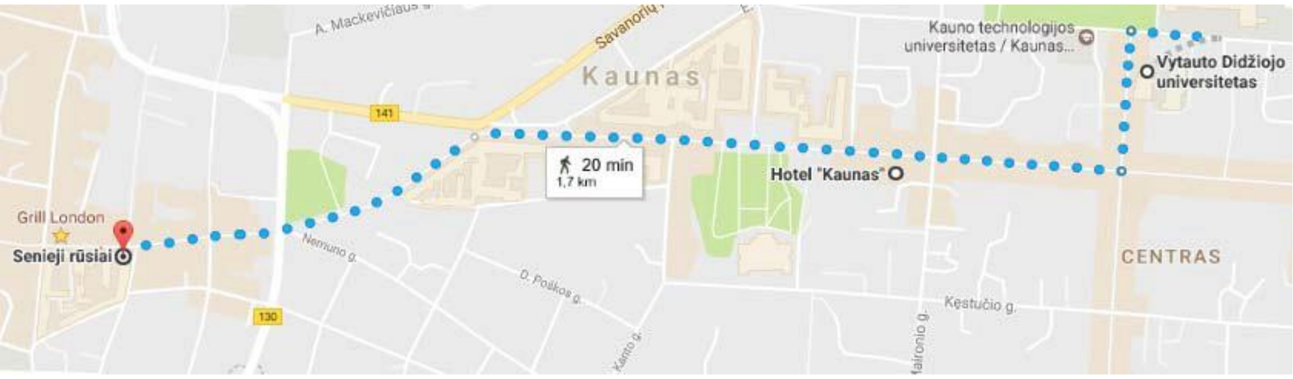
The annual meeting of the ESReDA General Assembly will be held this evening. The agenda will be circulated by the ESReDA General Secretary to Members. A Gala dinner for Members and participants of the seminar will be followed the main meeting.

Social events

Gala dinner

Tuesday, 30th May, 20:00
Restaurant "Senieji rūsiai" ("Old cellars") / Napoleon's Hall
Vilniaus g. 34, Kaunas

Gala dinner will be held in a European standard restaurant established in the17th century cellars in the heart of Kaunas old town. The restaurant with the interior in the style of middle ages attracts visitors with their Napoleon's Hall, Noblemen's Hall, and the Hall of Guns. In one of the halls, there is a fresco depicting the Middle French Army crossing the river Nemunas on 24 June 1812 according to the lithography of De C. Montte.



General information

Changes to technical and social programme

The 52nd ESReDA seminar organizers reserve the right to adjust or change the Technical and/or Social Programmes as, if and when necessary.

Seminar venue

Vytauto Didžiojo universitetas (Vytautas Magnus University)
S. Daukanto g. 28 (Small Hall, 2nd floor), goo.gl/IUk03p
Kaunas, Lithuania

Kaunas is the second-largest city in Lithuania and has historically been a leading centre of Lithuanian economic, academic, and cultural life. Kaunas was the biggest city and the centre of a county in Trakai Municipality of the Grand Duchy of Lithuania since 1413.
Kaunas is unique place since it has the oldest funiculars in the world; it is surrounded by old fortification system (now the castle are used for cultural activities, as museums); has the best example of high Baroque in Northern and Eastern Europe – "Pažaislis" Church and Monastery Ensemble; has the longest pedestrian street in Eastern Europe – "Laisvės alėja".

An old legend claims that Kaunas was established by the Romans in ancient times. These Romans were supposedly led by a patrician named Palemon, who had three sons: Barcus, Kunas and Sperus. Palemon fled from Rome because he feared the mad Emperor Nero. Palemon, his sons and other relatives travelled all the way to Lithuania. After Palemon's death, his sons divided his land. Kaunas got the land where Kaunas now stands. He built a fortress near the confluence of the Nemunas and Neris rivers, and the city that grew up there was named after him. There is also a suburban region in the vicinity named "Palemonas".

Kaunas is first mentioned in written sources in 1361 when brick Kaunas Castle was constructed. In 1362, the castle was captured and destroyed by the Teutonic Order. The Kaunas castle was rebuilt at the beginning of the 15th century.

In 1408, the town was granted Magdeburg Rights by Vytautas the Great and became a centre of Kaunas Powiat in Trakai Voivodeship in 1413. Vytautas ceded Kaunas the right to own the scales used for weighing the goods brought to the city or packed on site, wax processing, and woollen cloth trimming facilities. The power of the self-governing Kaunas was shared by three interrelated major institutions: vaitas (the Mayor), the Magistrate (12 lay judges and 4 burgomasters) and the so-called Benchers' Court (12 persons). Kaunas then began to gain prominence, since it was at an intersection of trade routes and a river port. In 1441 Kaunas joined the Hanseatic League, and Hansa merchant office Kontor was opened — the only one in the Grand Duchy of Lithuania. By the 16th century, Kaunas also had a public school and a hospital and was one of the best-formed towns in the whole country.

After the final partition of the Polish–Lithuanian state in 1795, the city was taken over by the Russian Empire and became a part of Vilna Governorate. During the French invasion of Russia in 1812, the Grand Army of Napoleon passed through Kaunas twice, devastating the city both times.
It is also the seat of the Roman Catholic Archdiocese of Kaunas.

Modern Kaunas has close links with critical infrastructures. It is an important railway hub in Lithuania and city of the crossroads of international air transport (Kaunas airport) and road transport (Via Baltic, Rail Baltic). The Kaunas Hydroelectric Power Plant, located on the Nemunas River, is producing electricity for Kaunas city.

Kaunas is often referred to as a city of students and basketball, often called as the second religion of Lithuania.

http://visit.kaunas.lt/en/

This publication is a conference proceedings by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication.

JRC Science Hub
https://ec.europa.eu/jrc

JRC108070

EUR 28803 EN

PDF ISBN 978-92-79-73870-8 ISSN 1831-9424 doi:10.2760/07157

Luxembourg: Publications Office of the European Union, 2017

How to cite this report: Zutautaite, I., Eid, M., Simola, K. and Kopustinskas, V., *Critical Infrastructures: Enhancing Preparedness & Resilience for the Security of Citizens and Services Supply Continuity: Proceedings of the 52nd ESReDA Seminar Hosted by the Lithuanian Energy Institute & Vytautas Magnus University*, EUR 28803 EN, Publications Office of the European Union, Luxembourg, 2017, ISBN 978-92-79-73870-8, doi:10.2760/07157, JRC108070..

KJ-NA-28803-EN-N

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub

Publications Office

doi:10.2760/07157

ISBN 978-92-79-73870-8