Addressing the Importance of Data Veracity During Data Acquisition for Risk Assessment Processes

Michael Pacevicius, Norwegian University of Science and Technology
Nicola Paltrinieri, PhD, Norwegian University of Science and Technology
Christoph Alexander Thieme, PhD, Norwegian University of Science and Technology
Pierluigi Salvo Rossi, PhD, Norwegian University of Science and Technology

Key Words: Data veracity, Dynamic risk management, Confirmation factor, Power grids.

2021 Annual Reliability and Maintainability Symposium (RAMS) | 978-1-7281-8017-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/RAMS48097.2021.9605737

SUMMARY & CONCLUSIONS

The veracity of information (i.e., its quality of being and remaining true, accurate, and complete) is a pillar of efficient risk management. The informative capacity of the data on which the risk management process relies needs to be fully kept across the entire information pipeline in order to ensure that risk can be properly understood and managed. Unfortunately, research shows that the informative capacity of data may - partially or entirely - be lost between the generation and the final use of a piece of information. This problem starts with the capture of information, where inconsistencies may already be observed between the reality of a phenomenon and the data supposedly reporting its measurement. As a consequence, this can lead to inadequate decision making when answering a risky event and, thus to a critical escalation of the situation. Such circumstances have been reported as contributing factors in several well-known large-impact accidents (e.g., *Three Mile Island*, 1979; *BP Texas City Refinery*, 2005; *Deepwater Horizon*, 2010) and continue to be faced in high-risk infrastructures nowadays.

The multiplication of information sources made available through advances in the Internet of Things (IoT) and digital fields offers an opportunity to address this issue, as more and more data sources can be used to confirm a single fact. That way, decision-makers can better detect inconsistencies in the data used for risk analyses and apply appropriate corrective actions. However, this comes with several challenges. Firstly, conventional risk management approaches need to be rethought and restructured to enabling a dynamic updating of the risk picture as new information is made available. Secondly, they need to enable a characterization of the information quality by providing details on the level of uncertainties related to the generated risk picture. Thirdly, the data capture process needs to be properly understood in order to ensure that possible data corruption modes are correctly identified.

This paper discusses the points above by focusing on the veracity of information during the capture of data for risk assessment purposes. We discuss how multiple data sources may be managed to reduce uncertainties in this phase. A case study on the presence of vegetation close to power lines illustrates the related implications.

1 INTRODUCTION

Common risk assessments remain mostly focused on the processes themselves, assuming the existence of a reliable supporting infrastructure [1]. However, the information pipeline responsible for transmitting a piece of data from phenomenon observation to decision making (data capture, data transmission, data pre-processing, information processing, results transmission) represents a complex system of systems, which all can be a source of data corruption eventually leading to an inadequate decision making. Corruption is here understood as the possibility for a piece of information to lose its veracity, i.e., its quality of being and remaining true, accurate, and complete. Different major accidents can be used to illustrate the important consequences of a degraded information management process. In the *Three Mile Island* accident (1979), decision-makers have built their reasoning and took action in an emergency situation based on inaccurate information, being informed that automatic safety procedure had been successfully executed, while they were not [2]. Misreading of pressure information and ignoring of warnings about cement weaknesses were also some of the root causes responsible for the *Deepwater Horizon* catastrophe (2010), the biggest offshore oil spill in US history [3]. Additional events happening in between the *Three Mile Island* accident and the *Deepwater Horizon* catastrophe (e.g., the *BP Texas City Refinery* accident in 2005 [4]) are other illustrations of accidents showing that a piece of information may:

- not have been generated (e.g., sensors not working), and/or
- have been generated in an inappropriate way (e.g., sensors generating false information), and/or
- have been wrongly transported and distributed (i.e., telecommunication network failure), and/or
- have been treated by inappropriate analysis methods (e.g., outdated algorithm utilization), and/or
- have been wrongly interpreted by operators (e.g., human errors: making wrong decisions despite receiving the correct information in the right format).

978-1-7281-8017-5/21/$31.00 ©2021 IEEE

There is thus a need to increase attention on the gathering, transmission, and processing of information to ensure higher reliability of risk management processes. This topic becomes even more relevant in today's era of big data, where more and more digital information is made available and considered for risk management. Although the veracity of data is discussed in the literature for different applications, implications from the perspective of risk assessment have not yet been thoroughly examined. The present paper addresses thus this topic during the first step of the information chain used for risk assessment - data acquisition - through:

(1) the understanding of the implications and adaptation requirements for conventional risk approaches to fully integrate the veracity dimension in the risk assessment process; and
(2) discussing a framework for enabling the management of existing data sources so that a more reliable risk assessment can be executed.

This paper first revisits risk fundamentals in Section 2, clarifying the concept of Dynamic Risk Management (DRM), and highlighting the importance of reliable data acquisition for this purpose. It then builds on approaches typically used for data validation to integrate the veracity of information into conventional risk assessment approaches in Section 3. Finally, Section 4 presents a case study on vegetation management for power grids risk assessment. The presence of vegetation in the surrounding of power lines significantly impacts the probability of outage in power grids, and power grid outages can have on serious impact on modern societies.

2 FUNDAMENTALS

2.1 Risk Definition

One of the most renowned definitions of risk was given by Kaplan and Garrick [5]. It states that risk (R) can be expressed by what can go wrong (scenario s), what likelihood it will have (probability p), and how severe consequences will be (consequence c):

$$R = f(s, p, c) \tag{1}$$

On the other hand, several review articles [6–8] collect parallel risk definitions from the scientific literature to demonstrate the multiplicity of perspectives on the understanding of the concept of risk. In [9], the risk is defined as an uncertain consequence of an event or an activity with respect to something that humans value. For [10], Risk equals the expected loss. And for [11], the risk is the potential for realization of unwanted, negative consequences of an event.

There is thus not one single approach, but several paths leading to relatively different results, which may be all beneficial but intrinsically incomplete. This is demonstrated by the occurrence of major accidents whose scenarios were disregarded by safety reports because being deemed improbable [12]. As an attempt to provide a more comprehensive risk definition, Aven and Krohn (2014) suggest including knowledge (k) as a new dimension in the original definition (1):

$$R = f(s, p, c, k) \tag{2}$$

Here, this definition is retained due to the strong overlap existing between the concepts of *knowledge* and *veracity*. Its use is further detailed in Section (3).

2.2 Risk Management

Several examples of frameworks addressing risk management or governance may be found in standards and related contributions in literature [14]: i) "Risk management: guideline for decision makers" by the Canadian Standard Association (standard CSA Q850-97) [15]; ii) "Risk management: principles and guidelines" by the International Organization for Standardization (standard ISO 31000:2018) [16]; iii) "Risk governance framework" by the International Risk Governance Council [9]; and "Risk and emergency preparedness assessment" by the Norwegian petroleum industry (standard NORSOK Z-013) [17].

The mentioned risk management frameworks unanimously address the following steps: pre-assessment, risk assessment, tolerability/ acceptability judgment, risk management, and risk communication. Treatment of uncertainties is also emphasized, and different related practices are suggested. ISO 31000 defines risk as uncertainty to achieve an objective [16]. The IRGC framework [9] distinguishes between uncertainty and ambiguity. Uncertainty refers to a lack of clarity over the scientific or technical basis for decision making, whereas ambiguity gives rise to several meaningful and legitimate interpretations of accepted risk assessment results. Ambiguity may refer to potential different values leading to a variety of interpretations.

Uncertainties can arise at different levels and moments of the risk management process, and they may be related to data, models, or the decision-making phase. Most of the risk management frameworks invite to consider and acknowledge all forms of uncertainties, not only technical but also social. Decision making under uncertainty usually relies on the consideration and comparison of multiple scenarios, therefore requiring continuous improvement to maximize the likelihood of appropriate judgments. For instance, in the presence of emerging risks, differences among actual and expected results are likely, due to limits in experience and knowledge. The introduction of continuous improvement is thus fundamental in order to proceed towards effective and efficient risk management.

Constant monitoring supports continuous improvement, which is already a recurrent step in the risk management frameworks presented. However, there are very few references on what and how to monitor or measure. The monitoring process is often related to the level of achievement of objectives or to the adequacy of assumptions with observed consequences. While on the contrary, the IRGC framework insists on the monitoring of [9]: equity in the repartition of risks and benefits among different categories of populations; and transparency and availability of information for various stakeholders.

2.3 Dynamic Risk Management

DRM has an evident focus on the concept of risk. However, one should not be misled into thinking that this

domain aims at managing "dynamic risk." Analogously to dynamic risk analysis [18], it refers to the management process that is designed to dynamically handle the risk of a system. One important role of DRM is the conversion of the traditionally static process of risk analysis into a dynamic technique with the capacity to be regularly updated. This should include a common understanding of tolerability and acceptability of risk levels and a clear operational scope [19]. Despite its relevance, the frequency of updates of the process falls outside the purely methodological scope of this research [18]. DRM refers to the risk management frameworks (DRMF) designed to be dynamic, which optimally enables restructuration, updates, and iterations when needed. Whether a DRMF updates instantaneously, yearly, or every decade, it will always keep its dynamic characteristic as it is independent of the actual use. On the contrary, non-DRM still has the possibility to be updated but with considerable inertia leading it to require substantial efforts, time, and energy by appointed teams of experts and managers.

An illustrative example can be made by means of computer software coding. When a software code is meant to be updated based on the inputs provided while running, its structure and characteristics should be defined and designed accordingly. One can say that this software code is dynamic. When, instead, a software code does not accept any input for the sake of updates while running, the only option is modifying the lines of code that we want to be changed. We can define the latter code as static. Its update is still possible, but it requires increased effort and knowledge as it was not designed for it.

Thus, if we need to understand whether risk management can be considered dynamic, we should ask ourselves whether it was intended and designed to be dynamic, as this characteristic must be taken into account in the scope definition, i.e., the very first phases of its development.

2.4 Role of data acquisition in Dynamic Risk Management

Modern data acquisition refers to the process of sampling measurements of a physical phenomenon and converting this into a digital value exploitable by a software. This is usually done using sensors, converters, transmitters, and/or other transmission devices, forwarding the data to an analytical or archiving unit for post-acquisition data processing and/or storing. Manual reporting of information and information extraction from existing databases are usually not considered to be part of the data acquisition process. However, this is generally done in the field of risk management, considering the limited amount of information that can be met when dealing with rare events, as well as the importance of human operators in the management of high-risk infrastructures.

Here, the process of data acquisition can thus be defined as requiring:

- The acknowledgment of the parameter to analyze,
- The identification of the data sources to be considered (measuring device, database, personnel, etc.),
- The capture of the raw data and the initialization of the information transmission.

Although data acquisition may have been considered as part of the risk influencing factor (RIF) "design" in the ORIM [20] or "System feedback" in the BORA [21], it is, to the best of the authors' knowledge, never considered individually as a RIF, and thus never addressed in detail. This is particularly problematic, as the data acquisition process can be failing in different ways. For example:

- data may not be generated (e.g., inactive hardware or hardware failure),
- data may be corrupted (e.g., sensors with false indications),
- considered databases may be outdated,
- data may be available, but not correctly transmitted (e.g., data directed to the wrong endpoint, lack of authority hindering communication in the control team),
- data may be available, but face compatibility issues between devices (e.g., different protocols, language, hardware).

Detecting and acknowledging the occurrence of such issues in real-time is critical to maximizing the probability of good decision making in risk management. Traditional risk management approaches need thus also to be reshaped regarding the possibility of data corruption in order to integrate detection and acknowledgment by design, which is another dimension aimed to be covered by DRM.

3 CONFIRMATION FACTOR FOR VERACITY ASSESSMENT

Expressing the level of knowledge (k) used for risk assessment, as suggested in Formula (2), is an intrinsic feature of the calculated value of risk. We can tolerate having relatively little knowledge of scenarios with both low probability and low consequence. On the other hand, knowledge is critical when the probability and consequences of an event have their highest values. Formula (2) gives important insight into how we should manage risk while continuously improving. As mentioned by several risk management frameworks [14], it should be acknowledged that uncertainty is always a companion [22]. Calibration and correction based on new evidence will possibly allow for decreasing this uncertainty and accounting for evolving system conditions.

Current trends in the IoT and digital fields allow for the assumption that the average number of data sources per parameter observed is likely to increase in the future. Three generic situations may then be encountered when assessing how much the data sources agree on the forwarded information:

1) Absence of alternatives: only one data source is available to inform about a specific parameter. In such a situation, there is no better option than to fully rely on the only existing data source.
2) Confirmation of information: all data sources agree on the information to forward, and the value of the knowledge is increased as the number of data sources increases.
3) Conflicting answers: at least two data sources provide conflicting information. In that situation, further recommendations need to be provided to decide how to handle available information in the risk analysis.

As a consequence, we thus suggest to further characterizing the "strength of knowledge" as reported by Aven and Krohn by splitting the knowledge dimension into two indicators (Formula

(3)) to qualify the veracity of information. The first one simply indicates the number (N) of sources available to inform a specific observed parameter. The second indicator corresponds to a veracity indicator (v), capturing the agreement level across the considered data sources, a common approach for data validation and reconciliation [23].

$$k = g(N, v) \tag{3}$$

The number of data sources (N) is reported, as a higher value of (N) would generally imply a higher likelihood that the real status of the observed phenomenon can be captured, especially in the case where the information originates from independent data sources of different nature. The nature of the veracity indicator (v) is based on the nature of the objective function (i.e., categorical, discrete, continuous, etc.), which needs to be clarified in the first phases of the risk analysis. One needs then to define the trust level to assign to each data source, based on a priori knowledge indicating the reliability level of the source. In the absence of relevant side information, an identical trust level will be given by default to the different data sources. Finally, a combination rule needs to be chosen to calculate the value of the veracity indicator.

A simple illustration can be the use of (N) binary data sources (a_i), characterizing the same specific situation (e.g., presence or absence of a hazard in a specified area). Assuming the similar level of trust for all data sources and independence across their acquisition modes (i.e., no common source of corruption), one may choose a simple averaged value to define how likely reported information is to be true:

$$v = \frac{\sum_{i=1}^{N} a_i}{N}, a_i \in \{0,1\} \tag{4}$$

In this situation, the class maximizing the value of (v) may logically be chosen to report the status of the observed phenomenon [24]. Additionally, the value of (v) will enable to better characterize the level of uncertainty existing around the probability dimension reported in Formula (2). However, other situations may be more complex [25] and require a different decision rule, such as counting rules (where at least (M) out of (N) sources need to agree) or linear combinations of the individual data sources, useable when additional information on the reliability of the sources is available. Linear combinations of individual data sources usually outperform simple rules (like the counting rule), while simple rules do not require anything more than monitored information. Finally, discrete scenarios with more than 2 choices and/or fuzzy scenarios where situation evolution may be continuous instead of discrete would also impact the final choice for the decision rule. This decision needs thus to be appreciated on a case-by-case reasoning in the first steps of any risk analysis.

4 CASE-STUDY: VEGETATION MANAGEMENT IN POWER GRIDS

4.1 Context & Data

Overhead power lines are broadly used to transport power from production sites (e.g., dams, nuclear power plants or coal power plants) to consumers (e.g., industrial, commercial, and residential customers). Vegetation represents a main source of hazards worldwide in the management of those power lines [26]. Two principal unwanted scenarios (s) can indeed be identified with this regard: either (1) tree/branch falls on power lines, or (2) vegetation growth under the infrastructures. In both cases, the probability (p) of outages escalates when the distance from vegetation to the power lines decreases, as shortcuts due to connections between different phases are more likely. The consequences (c) can then be particularly important, as this can lead to wildfires and even large blackouts [27]. Distribution System Operators (DSOs) and Transmission System Operators (TSOs) – in charge of the power grid management – require, therefore, to be informed about the presence of vegetation in the surrounding of their grids in order to take adequate maintenance decisions.

Information relative to the assessment of vegetation presence close to power lines is traditionally obtained during visual inspections, which can be executed via foot patrols, helicopters, and the use of drones. Light Detection And Ranging (LiDAR)-based point clouds are also commonly used to obtain 3D insights, allowing for precise distance measurements between power lines and other elements, such as trees. Furthermore, photogrammetry-based point clouds are getting more and more attention in recent years as a more economical alternative to LiDAR point clouds. Finally, the use of orthophotos (geometrically corrected satellite images or large scale aerial images) for efficient large-scale inspections is currently intensively explored [28], mostly pushed by the progress made in computer vision and the continuously increasing availability of satellite imaging technologies with higher resolution and more frequent coverage [29].

These sources of information can all be used to assess the threatening level of vegetation in the surrounding of power grids. Figure 1 (a to d) illustrates how the presence of four small trees growing under a power line can be seen on a drone image (a), in a LiDAR point cloud (b), in a photogrammetry point cloud (c), and on an orthophoto (d).

4.2 Application

The current application principally focuses on the *probability* dimension of the risk definition. We consider the binary case of presence/absence of threatening vegetation between subsections of the power grid (here, a section between 2 consecutive power poles) as a simplified version of the original objective function focusing on exact distance measurement between trees and the infrastructure. In the present situation, the different data sources agree on the presence of four trees growing under the lines, leading the veracity indicator (v) to equal 1. Furthermore, considering the number (4) and the nature of data sources involved, we can confidently assume the information to be accurate. The suggested formulation of the *knowledge* dimension enables thus to dynamically assess the pertinence of the provided probability that threatening trees are present under the lines. It also enables to evaluate the impact of adding/removing data sources in the risk calculation by increasing/decreasing confidence in the provided results depending on the forwarded information.

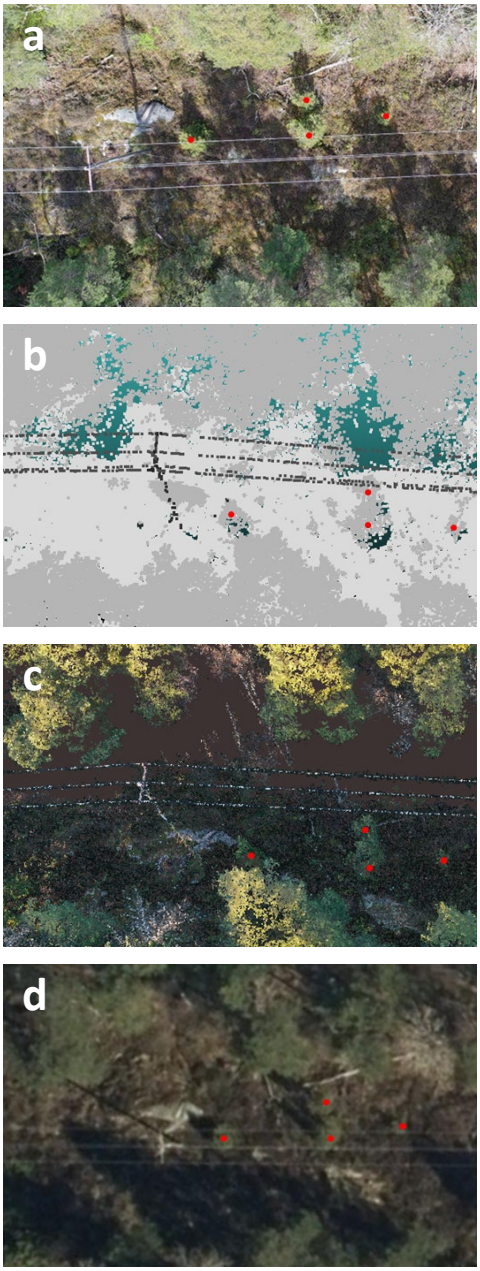

Figure 1 (a to d) - Detection of four small trees (marked via red points) growing under a power line and reported via a drone image (a), a LiDAR point cloud (b), a photogrammetry point cloud (c), and on an orthophoto (d).

5 DISCUSSION

The choice and management of data sources to be considered for risk management remain challenging activities. First, because the pertinence of a choice of data sources may change over time, e.g., due to a variation of the situation circumstances or to a variation in the quality of the acquired data. Second, because the merging of heterogeneous data sources remains a complicated task [30]. For instance, source-specific weaknesses imply that not all data sources can be used for the same purposes. The clarification of the objective function is thus critical to ensure that the chosen data sources properly support the resolution of the problem under review. Furthermore, regular revisions are required to ensure that the choice of data sources is continuously justified. This is, however, hindered by the fact that the definition of the data acquisition process (and more generally, the entire information pipeline construction) is usually seen as a "once and for all" process. This leads it to be often excluded from any serious system improvement plan, even though it has been recognized as a main contributing factor in major accidents. Tracking the variations of the veracity indicator (v) can thus also be used in that sense as a lagging alerting indicator. Once sources of disagreement have been identified, it can potentially reveal the need for removing initially chosen data sources that became irrelevant over time.

The concept of independence across data sources also requires proper attention. Data acquired from independent data sources but in a short period of time may all be outdated when considered in risk analysis, thus all confirming inaccurate information, potentially leading to inadequate decision making. This highlights the critical need for a proper definition of the reliability criteria of the data sources, for which levels need to be tracked over time. Some factors influencing the reliability level of the sources (and thus the pertinence of the executed risk analysis) are, in addition to the choice of the sources, the environmental conditions during data capture, the data collection modes, the choices of technologies, the maintainability of the physical equipment, the exposition of the physical equipment to environmental hazards, the maintenance of the physical equipment and the communication network design. Finally, the choice of the decision rule defining which values will eventually be reported in the risk analyses is a critical task that needs to be adequately executed by a panel of experts in the first phases of the studies and regularly reassessed to ensure its pertinence over time.

6 CONCLUSIVE REMARKS

Ensuring the veracity of information during the entire lifetime of risk management processes is of critical importance to guarantee the pertinence of the reported results. Conventional risk management approaches suffer from a lack of tools ensuring and controlling that data veracity can be kept over time. DRM provides solutions to fill this gap by enabling the establishment of continuity in the risk management processes, facilitating their updates and reiterations when required. This is supported by the rapid development of newly accessible data sources, made, for example, available via numerous IoT-based development strategies. In the present paper, we suggested an approach to formalize the benefit that increased access to a plurality of diverse data sources can provide. For this, we suggested extending the knowledge dimension of a relatively recent risk formulation, based on the number of data sources available and on veracity, indicator capturing the level of agreement across those sources. We applied this approach in a case-study focusing on vegetation close to power lines, which is a common source of outages in power grid management. We concluded that the approach was useful to confirm the presence of potentially problematic

vegetation in the analyzed case, but also pointed out that it is, in general, strongly dependent on both the formalization of the problem in initial phases and the quality of the data sources management over the entire life-cycle of the risk management processes.

ACKNOWLEDGMENTS

This work is part of the project "*Dynamic risk management for Smart Grids in large-scale interconnected power systems.*" funded by eSmart Systems and the Norwegian Research Council (NæringsPhD program - Project No.: 276404), which the authors would like to thank for their support.

REFERENCES

1. Thieme CA, Mosleh A, Utne IB, *et al.* Incorporating software failure in risk analysis – Part 1: Software functional failure mode classification. *Reliab. Eng. Syst. Saf.* 2020 ; 197 : 106803.
2. Jacquemain D. *Les accidents de fusion du cœur des réacteurs nucléaires de puissance État des connaissances*. EDP Scienc. 2013 : 464 p.
3. Anderson J, Burkeen AD, Clark D, *et al. Deep Water: The Gulf Oil Disaster And The Future Of Offshore Drilling - Report to the President (BP Oil Spill Commission Report)*. 2011 : 398 p.
4. Ramos MA, Droguett EL, Mosleh A, *et al.* Revisiting past refinery accidents from a human reliability analysis perspective: The BP Texas City and the Chevron Richmond accidents. *Can. J. Chem. Eng.* 2017 ;.
5. Kaplan S, Garrick BJ. On The Quantitative Definition of Risk. *Risk Anal.* 1981 ; 1 : 11–27.
6. Aven T, Renn O. On risk defined as an event where the outcome is uncertain. *J. Risk Res.* 2009 ; 12 : 1–11.
7. Aven T, Renn O. Response to Professor Eugene Rosa's viewpoint to our paper. *J. Risk Res.* 2010 ; 13 : 255–259.
8. Aven T. The risk concept—historical and recent development trends. *Reliab. Eng. Syst. Saf.* 2012 ; 99 : 33–44.
9. IRGC - International Risk Governance Council. *Risk Governance Deficits. An analysis and illustration of the most common deficits in risk governance*. Geneva, 2009 : p.
10. Willis HH. Guiding Resource Allocations Based on Terrorism Risk. *Risk Anal.* 2007 ; 27 : 597–606.
11. Rowe WD. *An Anatomy of Risk*. New York : John Wiley & Sons, 1977 : 24 p.
12. Paltrinieri N, Dechy N, Salzano E, *et al.* Lessons Learned from Toulouse and Buncefield Disasters: From Risk Analysis Failures to the Identification of Atypical Scenarios Through a Better Knowledge Management. *Risk Anal.* 2012 ; 32 .
13. Aven T, Krohn BS. A new perspective on how to understand, assess and manage risk and the unforeseen. *Reliab. Eng. Syst. Saf.* 2014 ; 121 : 1–10.
14. Paltrinieri N, Hauge S, Albrechtsen E. Risk management models in an integrated operations context. *Transactions of the American Nuclear Society*. 2013 : 1854–1857.
15. Canadian Standard Association. *CSA Q850 Risk Management: Guideline for Decision-Makers*. Toronto, Canada, 2009 : p.
16. ISO. Risk Management. ISO 31000:2018. 2018 ;.
17. NORSOK. *Risk and emergency preparedness assessment. Z-013*. Oslo, norway, Norway, 2010 : p.
18. Paltrinieri N, Khan FI. Dynamic risk analysis—Fundamentals. In : Khan FI, Amyotte PRBT-M in CPS, editors. *Advanced Methods of Risk Assessment and Management*. Elsevier, 2020 : 35–60.
19. Yang X, Haugen S, Paltrinieri N. Clarifying the concept of operational risk assessment in the oil and gas industry. *Saf. Sci.* 2017 ;.
20. Øien K. A framework for the establishment of organizational risk indicators. *Reliab. Eng. Syst. Saf.* 2001 ; 74 : 147–167.
21. Aven T, Sklet S, Vinnem JE. Barrier and operational risk analysis of hydrocarbon releases (BORA-Release). Part I. Method description. *J. Hazard. Mater.* 2006 ; 137 : 681–91.
22. Marchi B De, Ravetz JR. Risk management and governance:: a post-normal science approach. *Futures* 1999 ; 31 : 743–757.
23. Narasimhan S, Jordache C. *Data Reconciliation and Gross Error Detection. An Intelligent Use of Process Data*. Houston, Texas: Gulf Publishing Company, 2000 : 411 p.
24. Ciuonzo D, Salvo Rossi P. Distributed detection of a non-cooperative target via generalized locally-optimum approaches. *Inf. Fusion* 2017 ;.
25. Cheng X, Ciuonzo D, Rossi PS, *et al.* Multi-bit Decentralized Detection of a Non-cooperative Moving Target Through a Generalized Rao Test. 2020 ; 1–5.
26. Pacevicius M, A. Ramos M, Paltrinieri N. Optimizing Technology-based Decision-support for management of Infrastructures under risk: The Case of Power Grids. *Proceedings of the 30th ESREL-15th PSAM*. Research Publishing, Singapore, 2020 : 8.
27. Alhelou HH, Hamedani-golshan ME, Njenda TC, *et al.* A Survey on Power System Blackout and Cascading Events Research: Motivations and Challenges. *Energies* 2019 ; 12 : 1–28.
28. European Space Agency (ESA). Space-based Services for Distributed Energy Networks (Smart-Grids). *ESA Bus. Appl.* 2019 ;.
29. Space Industry Bulletin. Market Analysis and Business Intelligence for the Space Community. *Sp. Ind. Bull.* 2019 ; 2 : 24.
30. Pacevicius M, Roverso D, Salvo Rossi P, *et al.* Smart Grids : Challenges of Processing Heterogeneous Data for Risk Assessment. *Probabilistic Safety Assesment and Management - PSAM 14*. Los Angeles, 2018 : 11.

BIOGRAPHIES

Michael Pacevicius
Department of Mechanical and Industrial Engineering
Norwegian University of Science and Technology NTNU
Richard Birkelands vei 2B

7034 Trondheim, Norway

e-mail: michael.f.pacevicius@ntnu.no

Michael Pacevicius is an industrial PhD candidate in the RAMS group at NTNU, Norway and works as a researcher in eSmart Systems, a company delivering high-tech IT solutions for power grid related companies. His research activities focus on the development and implementation of dynamic risk analysis methods for large-scale interconnected power systems. He has a MSc. in Operational safety, Risks and Environment from the Université de Technologie de Troyes (UTT) in France and a MSc. in Economics and Business Administration from the Technische Universität Braunschweig (TUBS) in Germany. He worked as a project coordinator and analyst in the Big Data business development department of SAP in Munich, Germany, before joining eSmart Systems back in 2017.

Nicola Paltrinieri, PhD CEng CSci MIChemE
Department of Mechanical and Industrial Engineering
Norwegian University of Science and Technology NTNU
Richard Birkelands vei 2B
7034 Trondheim, Norway
e-mail: nicola.paltrinieri@ntnu.no

Nicola Paltrinieri is associate professor of risk analysis at NTNU (Norway) and adjunct professor in offshore HSE management at the university of Bologna (Italy). He has earned a PhD in Environmental, Safety and Chemical Engineering from the University of Bologna. From 2012 to 2016 he was research scientist at the department of Safety Research, SINTEF Technology and Society (Norway) and in 2012 he held a postdoctoral position at the university of Bologna. He is chartered engineer in the British Engineering Council register and charted scientist in the British Science Council register. He serves as associate editor of the journal “Safety Science”. He is member of the editorial boards of the “Journal of Marine Science and Engineering”, “Journal of Risk Research” and “Safety in Extreme Environments”. He is member of the board of the NTNU Team Hydrogen. He is member of the board and treasurer of the Society of Risk Analysis – Europe. He serves as Norwegian delegate of the Working Party on Loss Prevention and Safety Promotion within the European Federation of Chemical Engineering. He is co-chair on Accident and Incident modelling, European Safety and Reliability Association Technical Committee. He serves as member of the of the scientific committees for the ESREL, Loss Prevention and CISAP conferences.

Christoph A. Thieme, PhD, MSc, BSc
Department of Marine Technology
Norwegian University of Science and Technology NTNU
Otto Nielsenvei 10
7052 Trondheim, Norway

e-mail: christoph.thieme@ntnu.no

Dr. Christoph Thieme obtained his PhD in Marine Technology from NTNU. He has experience with risk analysis and modelling of autonomous marine systems. Currently, he is a postdoctoral research fellow at NTNU in the UNLOCK project, working on risk assessment methods development and applications on autonomous control systems. His main research interests are the contribution of software and control system aspects to the risk level of autonomous systems.

Pierluigi Salvo Rossi, PhD
Department of Electronic Systems
Norwegian University of Science and Technology NTNU
O.S. Bragstads Plass 2B,
7491 Trondheim, Norway

e-mail: salvorossi@ieee.org

Pierluigi Salvo Rossi received the Dr.Eng. degree (summa cum laude) in telecommunications engineering and the Ph.D. degree in computer engineering from the University of Naples ``Federico II", Italy, in 2002 and 2005, respectively. Currently, he is a full professor of statistical machine learning with the Dept. Electronic Systems, NTNU, Norway, and also the director of IoT@NTNU. He is an IEEE Senior Member since 2011 and serves as an executive editor for the IEEE Communications Letters, an area editor for the IEEE Open Journal of the Communications Society, an associate editor for the IEEE Transactions on Signal and Information Processing over Networks, and an associate editor for the IEEE Transactions on Wireless Communications since 2015. His research interests fall within the areas of communication theory, data fusion, machine learning, and signal processing.