Accidents in the Energy Sector and Energy Infrastructure Attacks in the Context of Energy Security

*Peter Burgherr, Jennifer Giroux and Matteo Spada**

The risks of technological accidents in the energy sector and their potentially disastrous effects have been analyzed over the past decades, and are nowadays generally recognized to constitute a key factor in an encompassing assessment of energy security. In contrast, the issue of intentional attacks on energy infrastructures has received increased attention more recently, particularly due to growing dependence of energy imports from and transit routes through regions considered less reliable and politically stable. Both types of risks, however, illuminate different vulnerabilities. Therefore, the focus of the present analysis was on these two risk categories: accidents and intentional attacks in the energy sector. Risk assessment results were based on quantitative data from the databases ENSAD (Energy-related Severe Accident Database) and EIAD (Energy Infrastructure Attack Database). Evaluations examined similarities and differences between technological accidents and intentional attacks in terms of frequencies and consequences, considering time-series trends and regional patterns. A key difference is that accidents are typically rare and independent events, whereas intentional attacks are often multiple events and concentrated both in time and space, resulting in distinct hotspots. Concerning consequences, the severity distribution for accidents generally stretches over a broad range, with low-probability high-consequence events being an important factor of both energy chain performance and as a measure of risk aversion. On the other hand, these types of consequences are usually less important for intentional attacks because targeted energy infrastructures are often of "linear" nature (e.g. pipelines and transmission lines) that are difficult to protect and usually lead through remote areas with low population density. However, when frequently attacked substantial business and supply disruptions can occur. In summary, the joint analysis of accidents and intentional attacks provides a comprehensive and complementary approach on two types of risks that have rather different properties, but are essential in an energy security perspective.

I. Introduction

Energy is a key driver of our modern society, and it is a necessary prerequisite for most goods and services produced. Therefore, the energy sector and its infrastructures are generally considered critical[1][2]. However, there is also no energy technology that is absolutely risk free. Furthermore, risk perspectives may differ among various individuals as well as stakeholder groups, depending on their respective backgrounds, expectations and objectives. As a consequence, a comprehensive risk assessment framework of energy technologies should be transparent, understandable, and consistently applicable to different technologies to produce scientifically sound and socially accepted risk indicators.

---

* Peter Burgherr is group leader Technology Assessment at the Paul Scherrer Institut (PSI); Jennifer Giroux is an applied anthropologist specialized in research on (societal) resilience, business in conflict zones, and critical infrastructure protection; Matteo Spada is a researcher in risk assessment at the Paul Scherrer Institut (PSI).

[1] 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.

[2] Rinaldi, S. M., Peerenboom, J. P. & Kelly, T. K. (2001) Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine,* 21, 11-25.

In general, there is no agreed definition for the term risk. Aven [3] and Haimes [4] provide an encompassing overview of risk definitions, how they can be categorized, and how they are used depending on the field of application and the object under study. In engineering and natural sciences, risk is commonly defined in a quantitative way, i.e. risk (R) equals probability (p) times consequence (C). More recently, the decomposition of risk in the triplet of Threat (T) x Vulnerability (V) x Consequence (C) has received particular attention in the domain of critical infrastructure protection[5] [6]. In addition, subjective factors of risk perception and value judgment can influence a stakeholder's acceptance or aversion to a specific risk, involving trade-offs between quantitative and qualitative risk factors[7] [8] [9]. Furthermore, risk perspectives can be described based on Funtowicz and Ravetz's risk classification structure [10] [11] [12], which is built on the axes (1) decision stakes (costs, benefits) and (2) system uncertainties (imperfect knowledge).

Although different conceptual frameworks and methodological approaches exist, the discipline of risk assessment is well-established, and in the past decades a number of important advancements were achieved.[13] However, foundational issues, such as consistency, and future challenges, such as the evolutions of risks, remain a central aspects to be taken into account [14]. On the one hand risk assessment is an autonomous discipline with applications in a variety of fields, but on the other hand it is strongly connected within a broader perspective to aspects such as sustainability, energy security, critical infrastructure protection and risk governance.

Figure 1 provides a schematic overview of how energy system risk assessment can be embedded into an overarching framework, aiming to provide a safe, secure and sustainable energy supply. In the context of this paper, the focus is on accidental and intentional events, which are not attributable to normal operation conditions of energy system infrastructures. Random accidents can be caused by technical failures (e.g. explosion, fire) as well as triggered by natural hazards (e.g. earthquake, wind storm). This type of events are considered to be rare and independent, which is why their frequency is generally modeled by the Poisson Distribution [15]. In contrast, intentional attacks often show a different behavior, namely a pattern of contagion, which is known phenomenon from epidemiology [16]. Therefore, their frequency is often better modeled by the Negative Binominal (NBI) distribution [17]. Consequently, random accidents and intentional attacks can be analyzed using a common risk assessment framework, however, there is a need to take into account their respective peculiarities.

Recently, so-called extreme events have received increased attention, partially due to a number of actual occurrences with significant impacts on the en-

---

[3] Aven, T. (2012) The risk concept – historical and recent development trends. *Reliability Engineering and System Safety,* 99, 33-44.

[4] Haimes, Y. Y. (2009) On the Complex Definition of Risk: A Systems-Based Approach. *Risk Analysis,* 29, 1647-1654.

[5] Cox Jr., L. A. (2008) Some limitations of "risk = threat × vulnerability × consequence" for risk analysis of terrorist attacks. *Ibid.*28, 1749-1761.

[6] Scouras, J., Parnell, G. S., Ayyub, B. M. & Liebe, R. M. (2009) Risk analysis frameworks for counterterrorism. IN Voeller, J. G. (Ed.) *Wiley Handbook of Science and Technology for Homeland Security.* Hoboken NJ, USA, John Wiley & Sons Inc.

[7] Gregory, R. & Lichtenstein, S. (1994) A hint of risk: tradeoffs between quantitative and qualitative risk factors. *Risk Analysis,* 14, 199-206.

[8] Stirling, A. (1999) Risk at a turning point? *Journal of Environmental Medicine,* 1, 119-126.

[9] Slovic, P. (2001) The risk game. *Journal of Hazardous Materials,* 86, 17-24.

[10] Aven, T. (2013) On Funtowicz and Ravetz's "Decision Stake-System Uncertainties" Structure and Recently Developed Risk Perspectives. *Risk Analysis,* 33, 270-280.

[11] Funtowicz, S. O. & Ravetz, J. R. (1985) Three types of risk assessment. IN Whipple, C. & Covello, V. T. (Eds.) *Risk Analysis in the Private Sector.* New York (USA), Plenum Press.

[12] Funtowicz, S. O. & Ravetz, J. R. (1994) The worth of a songbird: Ecological economics as a postnormal science. *Ecological Economics,* 10, 197-207.

[13] Greenberg, M., Haas, C., Cox, J., Anthony, Lowrie, K., McComas, K. & North, W. (2012) Ten most important accomplishments in risk analysis, 1980–2010. *Risk Analysis,* 32, 771-781.

[14] Aven, T. & Zio, E. (2014) Foundational Issues in Risk Assessment and Risk Management. *Ibid.*34, 1164–1172.

[15] Eckle, P. & Burgherr, P. (2013) Bayesian data analysis of severe fatal accident risk in the oil chain. *Ibid.*33, 146-160.

[16] Giroux, J., Burgherr, P. & Melkunaite, L. (2013) Research Note on the Energy Infrastructure Attack Database (EIAD). *Perspectives on Terrorism,* 7, 113-125.

[17] Burgherr, P., Giroux, J. & Spada, M. (2015) Vulnerability of Eenergy infrastructure to intentional attacks - the interplay of resource, conflict and security. IN Nowakowski, T., Mlynczak, M., Jodejko-Pietruczuk, A. & Werbinska-Woiciechowska, S. (Eds.) *Safety and Reliability: Methodology and Applications.* London, UK, Taylor anf Francis Group.

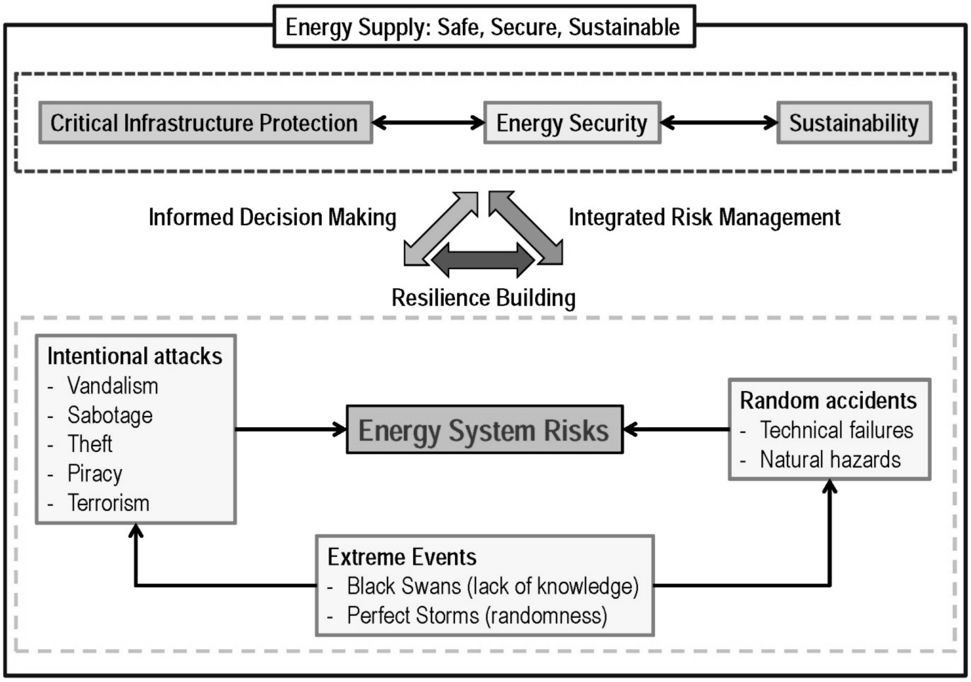


Figure 1: Energy system risk assessment in a broader context.

ergy sector. In 2005, Hurricanes Katrina and Rita initially led to the shut in of more than 91% of oil and 83% of gas production in the Gulf of Mexico [18], and 116 fixed platforms were destroyed and 163 sustained major damage [19]. Furthermore, 611 releases from offshore platforms and pipelines were reported [20], and more than 200 onshore releases that cumulatively amounted to about 75% of the Exxon Valdez release [21]. Other catastrophic events include the Three Mile Island nuclear power plant accident in 1979, the Exxon Valdez tanker spill in 1989, the Deepwater horizon platform spill in 2010, or the Fukushima nuclear accident in 2011 to name just a few [22]. In the public discussion of such disastrous, high-impact events often metaphors such as “black swans”, “perfect storms”, “unknown unknowns”, “here be dragons”, and “dragon kings” are used [23] [24] [25].

Taking a holistic perspective, risk assessment of energy systems should not remain an isolated silo activity, but rather be connected to the guiding principles and overarching concepts of sustainability [26] [27]

---

[18] RMS (2005) *Hurricane Katrina: Profile of a Super Cat. Lessons and Implications for Catastrophe Risk Management,* Newark, CA, USA, Risk Management Solutions (RMS).

[19] MMS (2007) *Assessment of fixed offshore platform performance in hurricanes Katrina and Rita. Final Report, May 2007,* Herndon, VA, USA, Mineral Management Service (MMS), U.S. Department of the Interior.

[20] Cruz, A. M. & Krausmann, E. (2009) Hazardous-materials releases from offshore oil and gas facilities and emergency response following Hurricanes Katrina and Rita. *Journal of Loss Prevention in the Process Industries,* 22, 59-65.

[21] Santella, N., Steinberg, L. J. & Sengul, H. (2010) Petroleum and Hazardous Material Releases from Industrial Facilities Associated with Hurricane Katrina. *Risk Analysis,* 30, 635-649.

[22] Sutton, I. (2012) Major events. IN Sutton, I. (Ed.) *Offshore Safety Management.* Amsterdam (The Netherlands), Elsevier, Zio, E. & Aven, T. (2013) Industrial disasters: Extreme events, extremely rare. Some reflections on the treatment of uncertainties in the assessment of the associated risks. *Process Safety and Environmental Protection 9 1,* 91, 31-45.

[23] Elahi, S. (2011) Here be dragons... exploring the‘unknown unknowns’. *Futures,* 43, 196-201.

[24] Paté-Cornell, E. (2012) On “Black Swans” and “Perfect Storms”: risk analysis and management when statistics are not enough. *Risk Analysis,* 32, 1823–1833.

[25] Sornette, D. & Ouillon, G. (2012) Dragon-kings: Mechanisms, statistical methods and empirical evidence. *The European Physical Journal Special Topics,* 205, 1-26.

[26] Gray, P. C. R. & Wiedemann, P. M. (1999) Risk management and sustainable development: mutual lessons from approaches to the use of indicators. *Journal of Risk Research,* 2, 201-218.

[27] Musango, J. K. & Brent, A. C. (2011) A conceptual framework for energy technology sustainability assessment. *Energy for Sustainable Development,* 15, 84-91.

[28], energy security [29] [30] [31] [32] [33] [34] [35] and critical infrastructure protection [36] [37] [38] [39]. Embedding classical risk assessment into integrative topics and associated approaches such as (1) resilience building including aspects of interdependencies and cascading effects [40] [41] [42] [43] [44], (2) informed decision making or risk governance [45] [46] [47], and (3) integrated risk management is crucial because it has been recognized that most technologies, services and areas are prone to multiple hazards, calling for a multi-risk approach [48] [49] [50].

This study is focused on risk assessment of random accidents in the energy sector and intentional attacks against energy infrastructures. The analytical approach for both of these energy sector risks is based on evaluation of historical experience available from two comprehensive databases, namely the Energy-related Severe Accident Database (ENSAD) [51] [52] of the Paul Scherrer Institute (PSI), and the Energy Infrastructure Attack Database (EIAD) [53] [54] jointly developed by the Center for Security Studies (CSS) at ETH Zurich and the PSI. The remainder of this paper is organized in the following way. In the method chapter the ENSAD and EIAD databases are described in detail as well as some key methods for comparative assessment of different energy technologies. The result chapter presents selected evaluations for energy-related accidents and intentional attacks. Finally, the conclusions chapter summarizes the key findings and insights, and also discusses common

---

[28] Santoyo-Castelazo, E. & Azapagic, A. (2014) Sustainability assessment of energy systems: integrating environmental, economic and social aspects. *Journal of Cleaner Production,* 80, 119-138.

[29] Cherp, A. & Jewell, J. (2014) The concept of energy security: Beyond the four As. *Energy Policy,* 75, 415-421.

[30] Chester, L. (2010) Conceptualising energy security and making explicit its polysemic nature. *Ibid.*38, 887-895.

[31] ????

[32] Winzer, C. (2012) Conceptualizing energy security. *Ibid.*46, 36-48.

[33] Ang, B. W., Choong, W. L. & Ng, T. S. (2015) Energy security: Definitions, dimensions and indexes. *Renewable and Sustainable Energy Reviews,* 42, 1077-1093.

[34] Brown, M. A., Wang, Y., Sovacool, B. K. & D'Agostino, A. L. (2014) Forty years of energy security trends: A comparative assessment of 22 industrialized countries. *Energy Research & Social Science,* 4, 64-77.

[35] Månsson, A., Johansson, B. & Nilsson, L. J. (2014) Assessing energy security: An overview of commonly used methodologies. *Energy,* 73, 1-14.

[36] DunnCavelty, M. & Suter, M. (2009) Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection,* 2, 179-187.

[37] Yustaa, J. M., Correa, G. J. & Lacal-Arántegui, R. (2011) Methodologies and applications for critical infrastructure protection: State-of-the-art. *Energy Policy,* 39, 6100-6119.

[38] Murray, A. T. & Grubesic, T. H. (2012) Critical infrastructure protection: The vulnerability conundrum. *Telematics and Informatics,* 29, 56-65.

[39] Lewis, A. M., Ward, D., Cyra, L. & Kourti, N. (2013) European Reference Network for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection,* 6, 51-60.

[40] Bruneau, M., Chang, S. E., Eguchi, R. T., Lee, G. C., O'Rourke, T. D., Reinhorn, A. M., Shinozuka, M., Tierney, K., Wallace, W. A. & von Winterfeldt, D. (2003) A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake Spectra,* 19, 733-752.

[41] Kröger, W. & Zio, E. (2011) *Vulnerable systems,* London (UK), Springer Verlag.

[42] Filippini, R. & Silva, A. (2012) Resilience analysis of networked systems-of-systems based on structural and dynamic interdependencies. *PSAM 11 & ESREL 2012.* Helsinki (Finland), pp 10.

[43] Ouyang, M. (2014) Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering and System Safety,* 121, 43-60.

[44] Roege, P. E., Collier, Z. A., Mancillas, James, McDonagh, J. A. & Linkov, I. (2014) Metrics for energy resilience. *Energy Policy,* 72, 249-256.

[45] Renn, O., Klinke, A. & van Asselt, M. (2011) Coping with complexity, uncertainty and ambiguity in risk governance: a synthesis. *Ambio,* 40, 231-246.

[46] Linkov, I., Bridges, T., Felix Creutzig, Decker, J., Fox-Lent, C., Kröger, W., Lambert, J. H., Levermann, A., Montreuil, B., Nathwani, J., Nyer, R., Renn, O., Scharte, B., Scheffler, A., Schreurs, M. & Thiel-Clemen, T. (2014) Changing the resilience paradigm. *Nature Climate Change,* 4, 407-409.

[47] Sidortsov, R. (2014) Reinventing rules for environmental risk governance in the energy sector. *Energy Research & Social Science,* 1, 171-182.

[48] Kappes, M. S., Keiler, M., von Elverfeldt, K. & Glade, T. (2012) Challenges of analyzing multi-hazard risk: a review *Natural Hazards,* 64, 1925-1958.

[49] Komendantova, N., Mrzyglocki, R., Mignan, A., Khazai, B., Wenzel, F., Patt, A. & Fleming, K. (2014) Multi-hazard and multi-risk decision-support tools as a part of participatory risk governance: Feedback from civil protection stakeholders. *International Journal of Disaster Risk Reduction,* 8, 50-67.

[50] Mignan, A., Wiemer, S. & Giardini, D. (2014) The quantification of low-probability–high-consequences events: part I. A generic multi-risk approach. *Natural Hazards,* Online First, http://dx.doi.org/10.1007/s11069-014-1178-4.

[51] Hirschberg, S., Spiekerman, G. & Dones, R. (1998) *Severe accidents in the energy sector - first edition. PSI Report No. 98-16,* Villigen PSI, Switzerland, Paul Scherrer Institut.

[52] Burgherr, P., Hirschberg, S. & Spada, M. (2013b) Comparative Assessment of Accident Risks in the Energy Sector. IN Kovacevic, R. M., Pflug, G. C. & Vespucci, M. T. (Eds.) *Handbook of Risk Management in Energy Production and Trading.* New York (USA), Springer Science+Business Media.

[53] Giroux, J., Burgherr, P. & Melkunaite, L. (2013) Research Note on the Energy Infrastructure Attack Database (EIAD). *Perspectives on Terrorism,* 7, 113-125.

[54] Burgherr, P., Giroux, J. & Spada, M. (2015) Vulnerability of Eenergy infrastructure to intentional attacks - the interplay of resource, conflict and security. IN Nowakowski, T., Mlynczak, M., Jodejko-Pietruczuk, A. & Werbinska-Woiciechowska, S. (Eds.) *Safety and Reliability: Methodology and Applications.* London, UK, Taylor anf Francis Group.

properties and differences between these two types of risks.

II. Methods

The analysis of random accidents and intentional attacks in the energy sector should take into account complete energy chains because accidents can occur at all stages, including upstream (exploration, extraction), midstream (transportation, storage) and downstream (processing and distribution) activities, the actual generation of power and/or heat, and waste treatment and disposal [55] [56]. The comparative assessment of accidents in the energy sector due to technical failures can be based on (1) statistical evaluation of historical experience, (2) probabilistic analyses, or mixed approaches combining limited availability of accident data with chain-specific modeling and expert judgment. In the case of fossil energy chains (coal, oil, natural gas) extensive historical data are available, enabling the direct use of statistical techniques to calculate risk indicators and to identify temporal and spatial patterns. For hydropower empirical data are normally sufficient to identify and assess general patterns and trends, but depending on the actual scope and objectives of an investigation should be complemented by representative case studies to account for specific dam features and location characteristics (e.g. downstream population and property assets at risk). Concerning nuclear energy, a simplified, level-3 Probabilistic Safety Assessment (PSA) has been developed by PSI to determine various offsite consequences (e.g. immediate and latent fatalities, land contamination) [57] [58]. The above-mentioned mixed approach is useful for assessing new renewable technologies for which historical experience is still often limited. While risk assessment for accidents due to technical failures is well-established since the 1990s, the analysis of intentional attacks against energy infrastructures has not been carried out using a similar systematic and rigorous approach. To improve this situation, the Center for Security Studies (CSS) and the PSI have jointly developed a new database that is uniquely dedicated to intentional attacks in the energy sector [59].

The following two sections provide a more detailed overview of the two databases used in this study for the assessment of random, energy-related accidents due to technical failures and intentional attacks on critical energy infrastructures.

1. Energy-related Severe Accident Database (ENSAD)

The importance of performing detailed risk assessment of accidents in the energy sector has been repeatedly stated in the past decades.[60] [61] [62] However, until the development of PSI' Energy-related Severe Accident Database (ENSAD) in the 1990s no information source specifically dedicated to comprehensively cover historical accidents in the energy sector was available because industry and insurance databases as well as databases with an even broader scope normally just treat energy accidents as one of many categories.[63] [64] Table 1 provides a schematic overview of the accident record structure as used in ENSAD. In general, ENSAD is a relational database implemented in MS Access, which through geo-referenc-

---

[55] Hirschberg, S., Spiekerman, G. & Dones, R. (1998) *Severe accidents in the energy sector - first edition. PSI Report No. 98-16,* Villigen PSI, Switzerland, Paul Scherrer Institut.

[56] Burgherr, P., Hirschberg, S. & Spada, M. (2013b) Comparative Assessment of Accident Risks in the Energy Sector. IN Kovacevic, R. M., Pflug, G. C. & Vespucci, M. T. (Eds.) *Handbook of Risk Management in Energy Production and Trading.* New York (USA), Springer Science+Business Media.

[57] Burgherr, P., Hirschberg, S. & Cazzoli, E. (2008) *Final report on quantification of risk indicators for sustainability assessment of future electricity supply options. NEEDS Deliverable n° D7.1 - Research Stream 2b. NEEDS project "New Energy Externalities Developments for Sustainability",* Brussels, Belgium.

[58] Burgherr, P., Eckle, P., Hirschberg, S. & Cazzoli, E. (2011) *Final Report on Severe Accident Risks including Key Indicators. SECURE Deliverable No. D5.7.2a,* Brussels, Belgium, SECURE project - Security of Energy Considering its Uncertainty, Risk and Economic implications.

[59] Giroux, J., Burgherr, P. & Melkunaite, L. (2013) Research Note on the Energy Infrastructure Attack Database (EIAD). *Perspectives on Terrorism,* 7, 113-125.

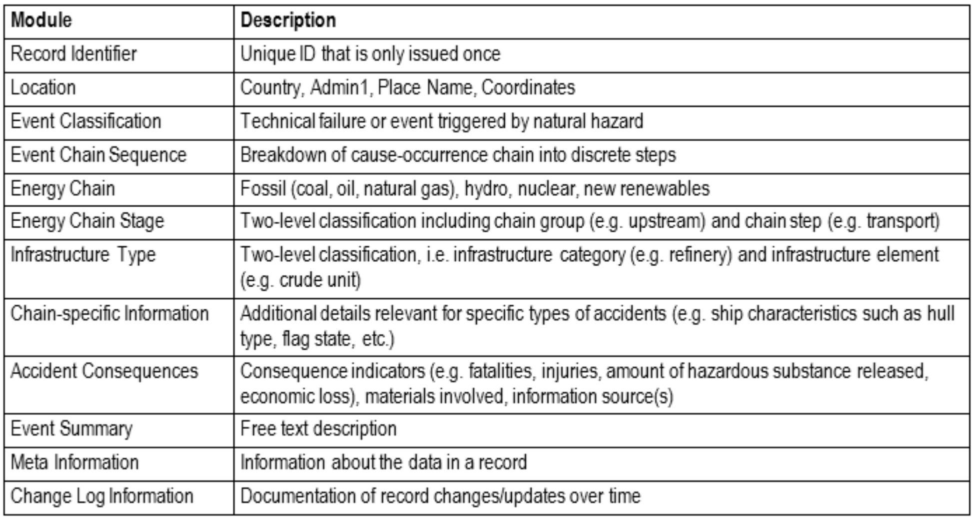
[60] Fritzsche, A. F. (1989) The health risks of energy production. *Risk Analysis,* 9, 565-577.

[61] Inhaber, H. (2004) Risk analysis applied to energy systems. IN Cleveland, C. J. (Ed.) *Encyclopedia of Energy, Volume 5.* Amsterdam, The Netherlands, Elsevier.

[62] Rasmussen, N. C. (1981) The application of probabilistic risk assessment techniques to energy technologies. *Annual Review of Energy,* 6, 123-138.

[63] Hirschberg, S., Spiekerman, G. & Dones, R. (1998) *Severe accidents in the energy sector - first edition. PSI Report No. 98-16,* Villigen PSI, Switzerland, Paul Scherrer Institut.

[64] Burgherr, P. & Hirschberg, S. (2008a) A comparative analysis of accident risks in fossil, hydro and nuclear energy chains. *Human and Ecological Risk Assessment,* 14, 947 - 973.



Module	Description
Record Identifier	Unique ID that is only issued once
Location	Country, Admin1, Place Name, Coordinates
Event Classification	Technical failure or event triggered by natural hazard
Event Chain Sequence	Breakdown of cause-occurrence chain into discrete steps
Energy Chain	Fossil (coal, oil, natural gas), hydro, nuclear, new renewables
Energy Chain Stage	Two-level classification including chain group (e.g. upstream) and chain step (e.g. transport)
Infrastructure Type	Two-level classification, i.e. infrastructure category (e.g. refinery) and infrastructure element (e.g. crude unit)
Chain-specific Information	Additional details relevant for specific types of accidents (e.g. ship characteristics such as hull type, flag state, etc.)
Accident Consequences	Consequence indicators (e.g. fatalities, injuries, amount of hazardous substance released, economic loss), materials involved, information source(s)
Event Summary	Free text description
Meta Information	Information about the data in a record
Change Log Information	Documentation of record changes/updates over time

Table 1: Overview of accident record structure in ENSAD.

ing of records can be directly coupled with Geographic Information Systems (e.g. ArcGIS) to allow map visualizations and geo-statistical analyses. [65] Despite its well-established and proven structure, ENSAD is continuously developed further to make sure ENSAD closely follows both historical developments and emerging risks; thus remaining an important resource to assess risk. Historical developments as well as scope and content extensions of ENSAD were already presented and explained in detail previously. For an up-to-date overview several recent publications and references therein can be consulted.[66] [67] [68]

2. Energy Infrastructure Attack Database (EIAD)

Compared to ENSAD, the Energy Infrastructure Attack Database (EIAD) is a rather new research activity that was jointly established in 2010 by the Center of Security Studies (CSS) at the Swiss Federal Institute of Technology (ETH) and the Technology Assessment (TA) group at the PSI. The EIAD focuses on energy infrastructure attacks that are carried out by so-called violent non-state actors (VNSA), which comprise a broad spectrum including warlords, militias, insurgencies, terrorist organizations, and criminal organizations and gangs. The motivation to develop a new database that is exclusively dedicated to intentional attacks on energy infrastructures was based on the following needs. While ENSAD comprehensively covers energy-related accidents due to technical failures, existing databases collecting intentional attacks are not suitable to provide data at a similar level of detail and completeness for the energy sector. For example the Global Terrorism Database (GTD) [69] or the Worldwide Incidents Tracking System (WITS) [70] are focused on the terrorist threat only, but include attacks from all types of sectors and activities. In contrast, EIAD considers all kinds of criminal and politically motivated attacks that are targeted at energy infrastructures. Furthermore, EIAD contains successful as well as failed and foiled attacks, and it does not code for motivation that is often difficult to accurate-

---

[65] Burgherr, P., Eckle, P. & Hirschberg, S. (2013a) Comparative risk assessment of severe accidents in the energy sector based on the ENSAD database: 20 years of experience. IN Steenbergen, R. D. J. M., Van Gelder, P. H. A. J. M., Miraglia, S. & Vrouwenvelder, A. C. W. M. (Eds.) *Safety, reliability and risk analysis: beyond the horizon.* London (UK), CRC Press, Taylor & Francis Group.

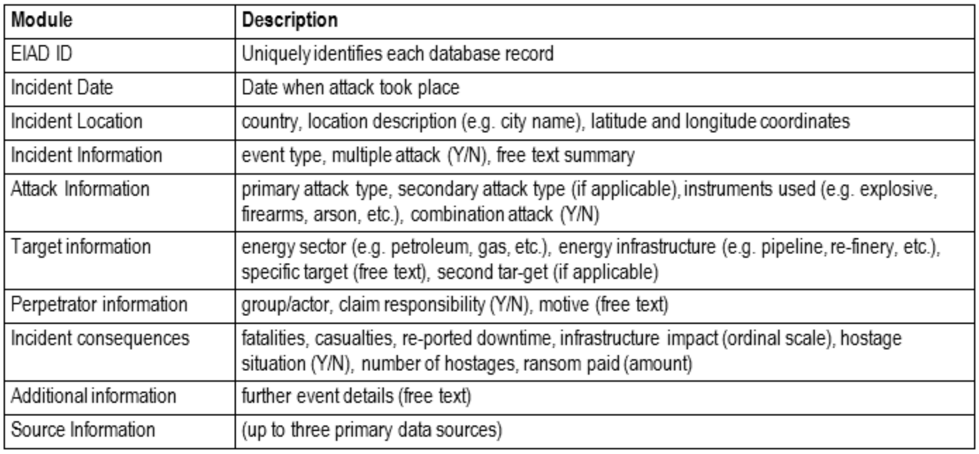
[66] Burgherr, P., Hirschberg, S. & Spada, M. (2013b) Comparative Assessment of Accident Risks in the Energy Sector. IN Kovacevic, R. M., Pflug, G. C. & Vespucci, M. T. (Eds.) *Handbook of Risk Management in Energy Production and Trading.* New York (USA), Springer Science+Business Media.

[67] Burgherr, P., Eckle, P. & Hirschberg, S. (2014) Comparative risk assessment of severe accidents in the energy sector based on the ENSAD database: 20 years of experience. IN Steenbergen, R. D. J. M., Van Gelder, P. H. A. J. M., Miraglia, S. & Vrouwenvelder, A. C. W. M. (Eds.) *Safety, Reliability and Risk Analysis: Beyond the Horizon.* London (UK), Taylor & Francis Group.

[68] Burgherr, P. & Hirschberg, S. (2014) Comparative risk assessment of severe accidents in the energy sector. *Energy Policy,* 74, S45–S56.

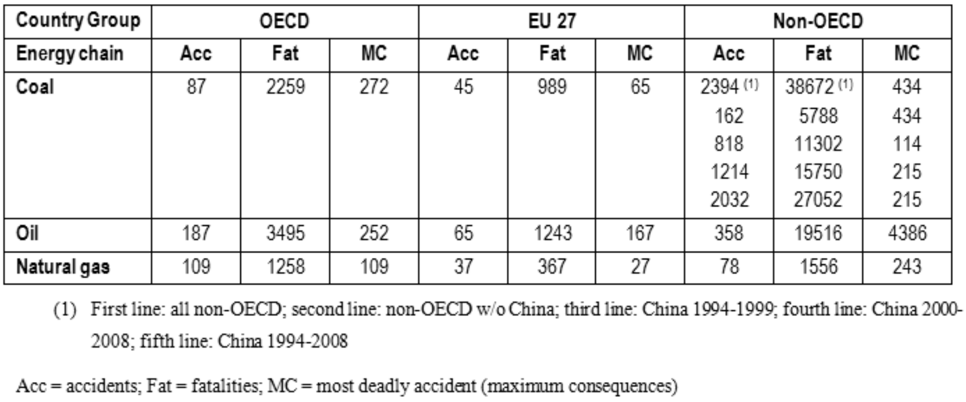
[69] LaFree, G. & Dugan, L. (2007) Introducing the Global Terrorism Database. *Terrorism and Political Violence,* 19, 181-204.

[70] Wigle, J. (2010) Introducing the Worldwide Incidents Tracking System (WITS). *Perspectives on Terrorism,* 4, 3-23.



Module	Description
EIAD ID	Uniquely identifies each database record
Incident Date	Date when attack took place
Incident Location	country, location description (e.g. city name), latitude and longitude coordinates
Incident Information	event type, multiple attack (Y/N), free text summary
Attack Information	primary attack type, secondary attack type (if applicable), instruments used (e.g. explosive, firearms, arson, etc.), combination attack (Y/N)
Target information	energy sector (e.g. petroleum, gas, etc.), energy infrastructure (e.g. pipeline, re-finery, etc.), specific target (free text), second tar-get (if applicable)
Perpetrator information	group/actor, claim responsibility (Y/N), motive (free text)
Incident consequences	fatalities, casualties, re-ported downtime, infrastructure impact (ordinal scale), hostage situation (Y/N), number of hostages, ransom paid (amount)
Additional information	further event details (free text)
Source Information	(up to three primary data sources)

Table 2: Summary of modular EIAD record structure.



Country Group	OECD			EU 27			Non-OECD		
Energy chain	Acc	Fat	MC	Acc	Fat	MC	Acc	Fat	MC
Coal	87	2259	272	45	989	65	2394 (1) 162 818 1214 2032	38672 (1) 5788 11302 15750 27052	434 434 114 215 215
Oil	187	3495	252	65	1243	167	358	19516	4386
Natural gas	109	1258	109	37	367	27	78	1556	243

(1) First line: all non-OECD; second line: non-OECD w/o China; third line: China 1994-1999; fourth line: China 2000-2008; fifth line: China 1994-2008

Acc = accidents; Fat = fatalities; MC = most deadly accident (maximum consequences)

Table 3: Summary of severe accidents (≥5 fatalities) per energy chain and country group for the period 1970–2008

ly determine, but rather for attack type (e.g. bombing, assault, hijacking, etc.). Although EIAD cannot rely on 20 years of experience like ENSAD, it is already a fully mature product in its field of application. Similar to ENSAD, EIAD has a modularized and standardized data record structure summarized in Table 2. A more extensive description of EIAD can be found in Giroux et al. [71]

III. Selected Results

1. Content of ENSAD and EIAD

Currently, ENSAD comprises a total of 32705accident records, of which 83.2% are classified as man-made, 16.3% as natural disasters, and 0.5% as conflicts. The vast majority of man-made accidents (20245) is attributable to the various energy chains, and of these 93.8% occurred in the years 1970–2008. Applying the fatality criterion of ENSAD's severe accident definition, 3367 accidents resulted in at least 5 fatalities in the previously defined observation period. Table 3 provides an overview of the numbers of severe accidents and their associated fatalities for fossil energy chains (coal, oil, natural gas) and different country groups (OECD, EU 27, non-OECD[72]). For a detailed discussion on the content of ENSAD the following recent publications can be consulted [73] [74].

---

[71] Giroux, J., Burgherr, P. & Melkunaite, L. (2013) Research Note on the Energy Infrastructure Attack Database (EIAD). *Ibid.*7, 113-125.

[72] OECD: Organisation for Economic Co-operation and Development, EU: European Union

[73] Burgherr, P., Hirschberg, S. & Spada, M. (2013b) Comparative Assessment of Accident Risks in the Energy Sector. IN Kovacevic, R. M., Pflug, G. C. & Vespucci, M. T. (Eds.) *Handbook of Risk Management in Energy Production and Trading.* New York (USA), Springer Science+Business Media.

[74] Burgherr, P. & Hirschberg, S. (2014) Comparative risk assessment of severe accidents in the energy sector. *Energy Policy,* 74, S45–S56.

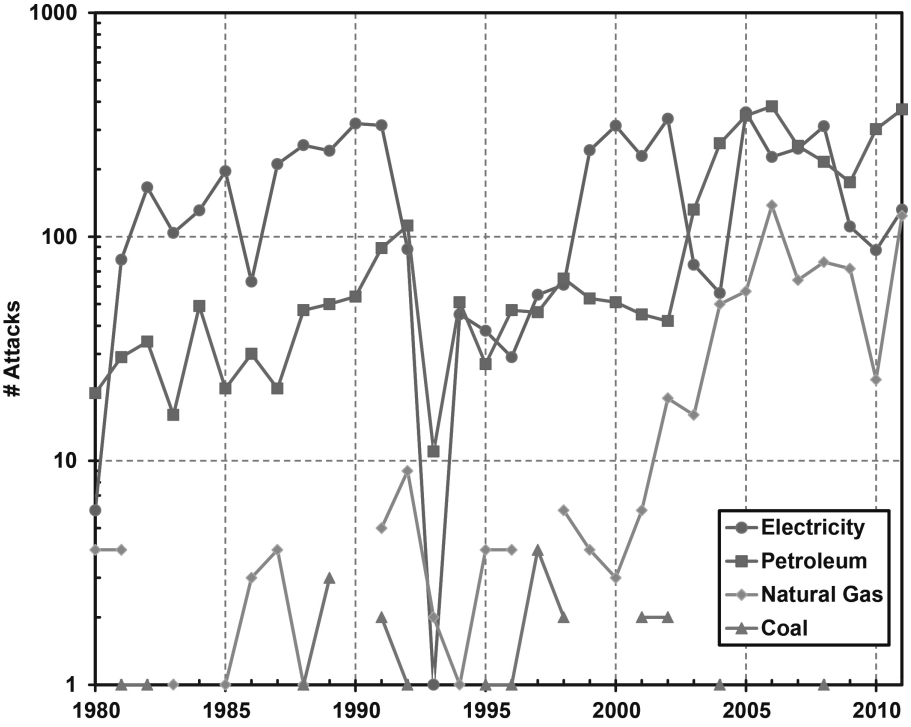


Figure 2: Annual number of EI attacks in different energy sectors during the period 1980-2011.

Overall, EIAD contains 9432 energy infrastructure attacks that took place during the period 1980–2011. The average number of attacks per year increased only slightly from 184 in the 1980s to 197 in the 1990s. In contrast, attacks more than doubled (471) in the 2000s. The two years available for the 2010s (526) indicate that this upward trend could continue, if the prevailing boundary conditions are not subject to a major change in the coming years. While accidents are normally discrete events in time, a rather large share of 43.7% of attacks was considered multiple events. The dominant attack type was bombings (82.3%), whereas other attack types such as hostage taking/kidnapping, sabotage, hijacking, assassination and looting/theft were each between 1% and 5%. Attacks most commonly affected the electricity (54.4%) and petroleum (36.6) sectors, followed distantly by the natural gas (7.4%), whereas other sectors such as coal were practically negligible (Figure 2). Finally attacks predominantly target "linear" energy infrastructures (e.g. pipelines and transmission lines, and to a lesser extent transport by trucks and ships) that are difficult to protect, and also often pass through remote areas. On the other hand, "point sources" such as power plants or refineries can be more easily controlled and secured, and thus are usually not the preferred option. A more in-depth description of EIAD and its content can be found in the following publications [75] [76].

2. Accident and Attack Patterns

Figure 3 provides an overview of the number of accidents per country and decade for fossil energy chains, i.e. coal, oil and natural gas. In the 1970s and 1980s a total of 224 and 327 severe (≥5 fatalities) accidents occurred worldwide, whereas in the 1990s and 2000 a tremendous increase to 1142 and 1520 accidents was observed. This is exclusively attributable to the substantially improved reporting and publish-

---

[75] Giroux, J., Burgherr, P. & Melkunaite, L. (2013) Research Note on the Energy Infrastructure Attack Database (EIAD). *Perspectives on Terrorism, 7*, 113-125.

[76] Burgherr, P., Giroux, J. & Spada, M. (2015) Vulnerability of Eenergy infrastructure to intentional attacks - the interplay of resource, conflict and security. IN Nowakowski, T., Mlynczak, M., Jodejko-Pietruczuk, A. & Werbinska-Woiciechowska, S. (Eds.) *Safety and Reliability: Methodology and Applications.* London, UK, Taylor anf Francis Group.

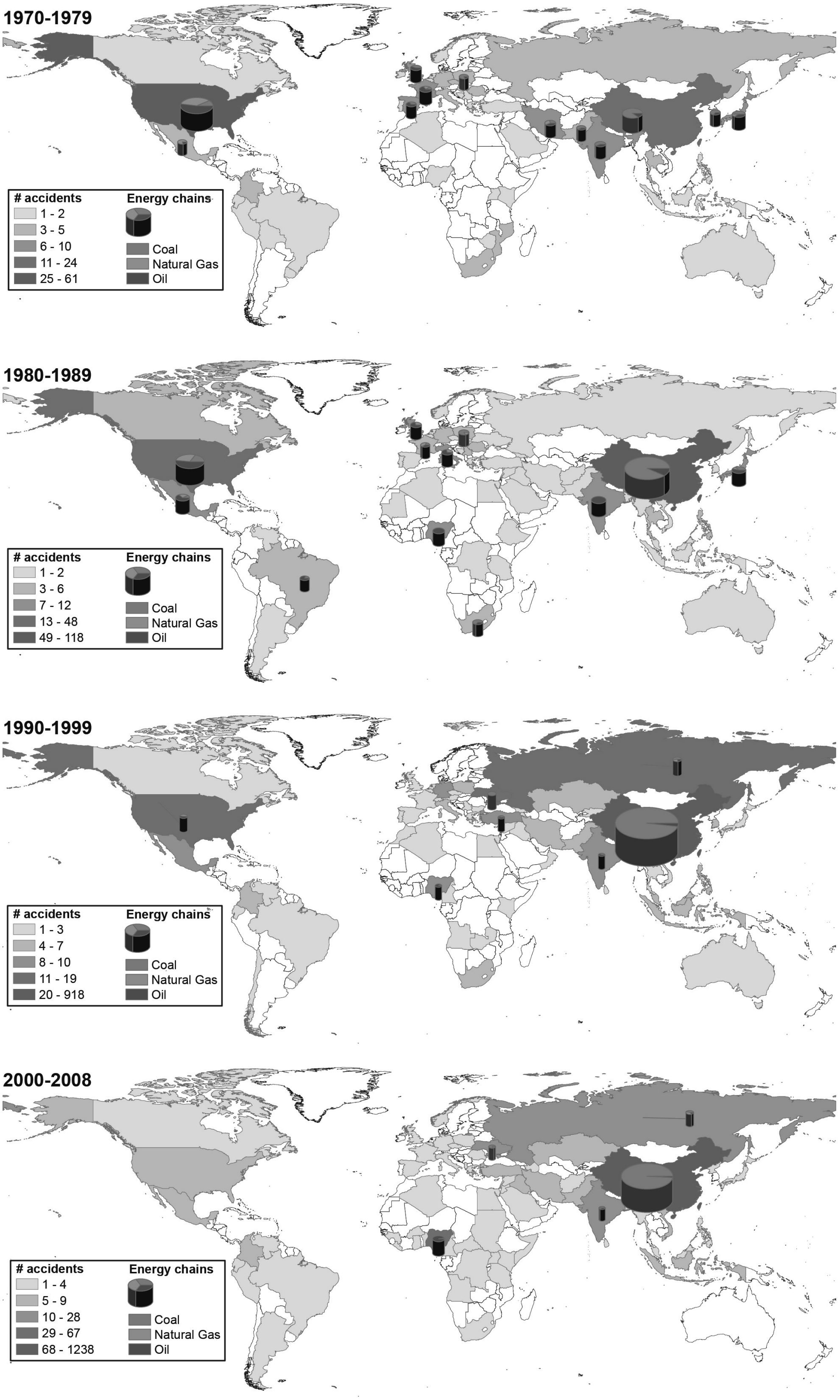


Figure 3: Number of accidents in fossil energy chains (coal, oil, natural gas) per country and decade. The pie charts show the contributions of the various energy chains to the total of all accidents in a country for a specific decade.

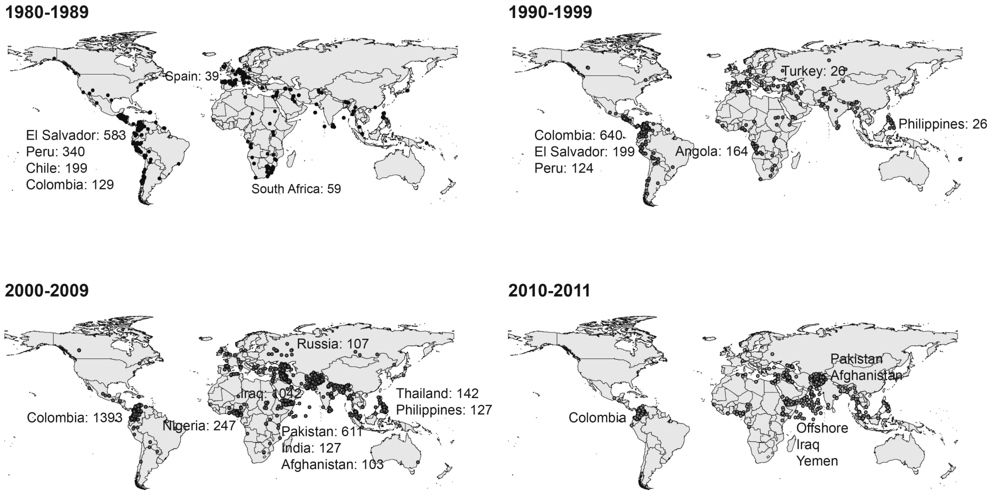


Figure 4: Spatial distribution of EI attacks by decade during the years 1980-2011 (n = 8549). For each decade, countries with highest numbers of attacks are indicated.

ing of coal mine accidents in China [77] [78]. Without the coal accidents in China the totals would be 252 and 306 accidents, which is between the 1970 and 1980 values, suggesting that the number of severe accidents without coal China remained rather stable over the whole period of observation. However, the share of accidents that took place in OECD countries clearly decreased from 59.4% in the 1970s to 36.7% in the 1980s, and then 32.5% and 15.7% in the 1990s and 2000s (without coal China).So, there is a clear shift from OECD to non-OECD countries, indicating that improved safety procedures and regulatory frameworks in the OECD are responsible for this positive trend [79], whereas a similar development in non-OECD is largely absent, and at the same time production of fossil energy carriers in non-OECD increased substantially [80].

In the 1970s, countries with most severe accidents were USA (61), China (24), Japan (10), France (9), Iran, India and UK (each 7). The pie charts in the Figure also show the share of the various energy chains in each country. For example, in USA accidents in the oil and natural gas chains are most frequent, whereas in China coal accidents dominate. In the 1980s, China (118) and USA (48) had already switched positions, followed by India (12), Mexico (11), Japan (8), Nigeria (8), UK (7) and Italy (7). In the 1990s, Russia (19) and Ukraine (17) rank second and third, distantly after China (918), whereas USA (15) is only on the fourth position, followed by India, Turkey and Nigeria (each 10). Finally in the 2000s, China (1238) still dominates due to its coal chain, but Nigeria (67) has moved up to the second with the oil chain being the dominant contributor. Russia (28) and Ukraine (21) both lost a position, followed by India (18), Iran, USA, Turkey and Pakistan (each 9).

The maps in Figure 4 depict the locations of energy infrastructure attacks by country and decade. Out of all 9432 attacks contained in EIAD, only 8549 were considered because the others could not be geo-referenced at the same level of accuracy. In the 1980s and 1990s, attacks were clearly concentrated in Central and South America, whereas events in Europe, Africa and Asia were much less frequent. However, since the 2000s a clear shift towards newly emerging hotspot countries in Africa and Asia can be observed, although Colombia remains a major area of concern.

The following patterns can be described among the top three countries in terms of numbers of attacks. In Colombia three distinct peaks of energy infrastructure attacks occurred, namely 1991-1992, 1999-2002 and 2005-2007. The first peak was predominantly attributable to attacks on the Cano Limon

---

[77] Hirschberg, S., Burgherr, P., Spiekerman, G., Cazzoli, E., Vitazek, J. & Cheng, L. (2003) Assessment of severe accident risks. IN Eliasson, B. & Lee, Y. Y. (Eds.) *Integrated assessment of sustainable energy systems in China. The China Energy Technology Program - A framework for decision support in the electric sector of Shandong province. Alliance for Global Sustainability Series Vol. 4*. Amsterdam, The Netherlands, Kluwer Academic Publishers.

[78] Burgherr, P. & Hirschberg, S. (2007) Assessment of severe accident risks in the Chinese coal chain. *International Journal of Risk Assessment and Management, 7*, 1157-1175.

[79] Burgherr, P. & Hirschberg, S. (2008b) Severe accident risks in fossil energy chains: a comparative analysis. *Energy, 33*, 538-553.

[80] IEA (2014) *World Energy Outlook 2014,* Paris (France), International Energy Agency (IEA).

pipeline, and thus the oil sector. In contrast, the second peak was targeted primarily towards transmission lines, and to a lesser extent this was also the case for the last peak. In Iraq the peak from 2004-2007 was mostly due to attacks on oil pipelines, but particularly in 2006 a higher number of attacks against energy personnel were recorded. Lastly, in Pakistan a shift from attacks on transmission lines (2004-2005) to natural gas pipelines (2006-2009), and most recently oil transport by road tanker (2010-2011) was observed.

3. Risk Indicators

Figure 5 provides a summary compilation of three risk indicators for accidents and attacks. In the case of accidents fossil energy chains were analyzed, while for attacks also electricity infrastructures were taken into account. Along the x-axis the number of accidents or attacks normalized to Gigawatt-electric-years (GWeyr) is shown, whereas the y-axis depicts the fatality rate (i.e. number of fatalities per GWeyr). Lastly, the diameter of the circles corresponds to the most deadly single accident (maximum consequences), i.e. the larger the diameter the higher the number of persons killed. Both panels for technological accidents (a) and intentional attacks (b) have the same axis scales to allow direct comparisons.

Concerning accidents, Chinese coal accidents had the highest frequencies, followed by coal non-OECD w/o China and oil non-OECD. OECD and EU 27 accident rates for all three fossil chains as well as natural gas non-OECD were about one order of magnitude smaller (see inset of Figure 5a). For fatality rates a similar pattern among the various energy chain and country groupings was found. In terms of maximum consequences, oil non-OECD had by far the worst performance. The most deadly accident involved the collision between an oil tanker and an overloaded ferry boat (1987, Philippines) resulted in 4386 fatalities. In 1982 an accident of similar severity occurred in Afghanistan (2700 fatalities), when a tank truck collided with another vehicle in a tunnel, leading to an explosion with an engulfing fire. Generally, maximum consequences for all fossil energy chains were clearly highest in non-OECD, intermediate in OECD and lowest in EU 27. Although coal China had by far the highest accident and fatality rates, maximum consequences were closer to OECD levels than the rest of non-OECD, which is likely due to the fact that local as well as township and village coal mines dominate in China, whereas the number of large state-owned mines is much smaller [81].

For intentional attacks, coal OECD, coal EU 27 and oil EU 27 are not shown in Figure 5b because no events with fatalities were registered in EIAD. In general, the oil and electricity sectors in non-OECD exhibited the worst performance with respect to all three risk indicators, followed by natural gas non-OECD. In contrast, risk indicators were substantially lower for the remaining OECD and EU 27 energy chain and country group combinations as well as coal non-OECD. The average frequencies of events for accidents and attacks were similar, but the average fatality rate of accidents was about one order of magnitude higher for accidents compared to attacks. A similar difference was found for maximum consequences. The lower proneness of attacks to severe consequences in terms of fatalities can be attributed to the preference of targeting linear infrastructures (e.g. pipelines and transmission lines) that one the one hand are less protected than point sources (e.g. refineries, power plants), and on the other hand often lead through remote and sparsely populated areas.

IV. Conclusions

- The ENSAD and EIAD databases provide a comprehensive and consistent basis of data for the objective and quantitative analysis of risks in the energy sector due to technological accidents and intentional attacks. However, it is essential that this kind of databases is regularly updated both in terms of content and scope to keep up with the growing historical experience as well as to meet newly emerging analytical needs of different stakeholders. The evaluations presented in this article are exclusively based on data from ENSAD and EIAD.
- While accidents are typically rare and independent events, intentional attacks are often multiple events and concentrated both in time and space, resulting in distinct hotspots.

---

[81] Burgherr, P. & Hirschberg, S. (2007) Assessment of severe accident risks in the Chinese coal chain. *International Journal of Risk Assessment and Management, 7*, 1157-1175.

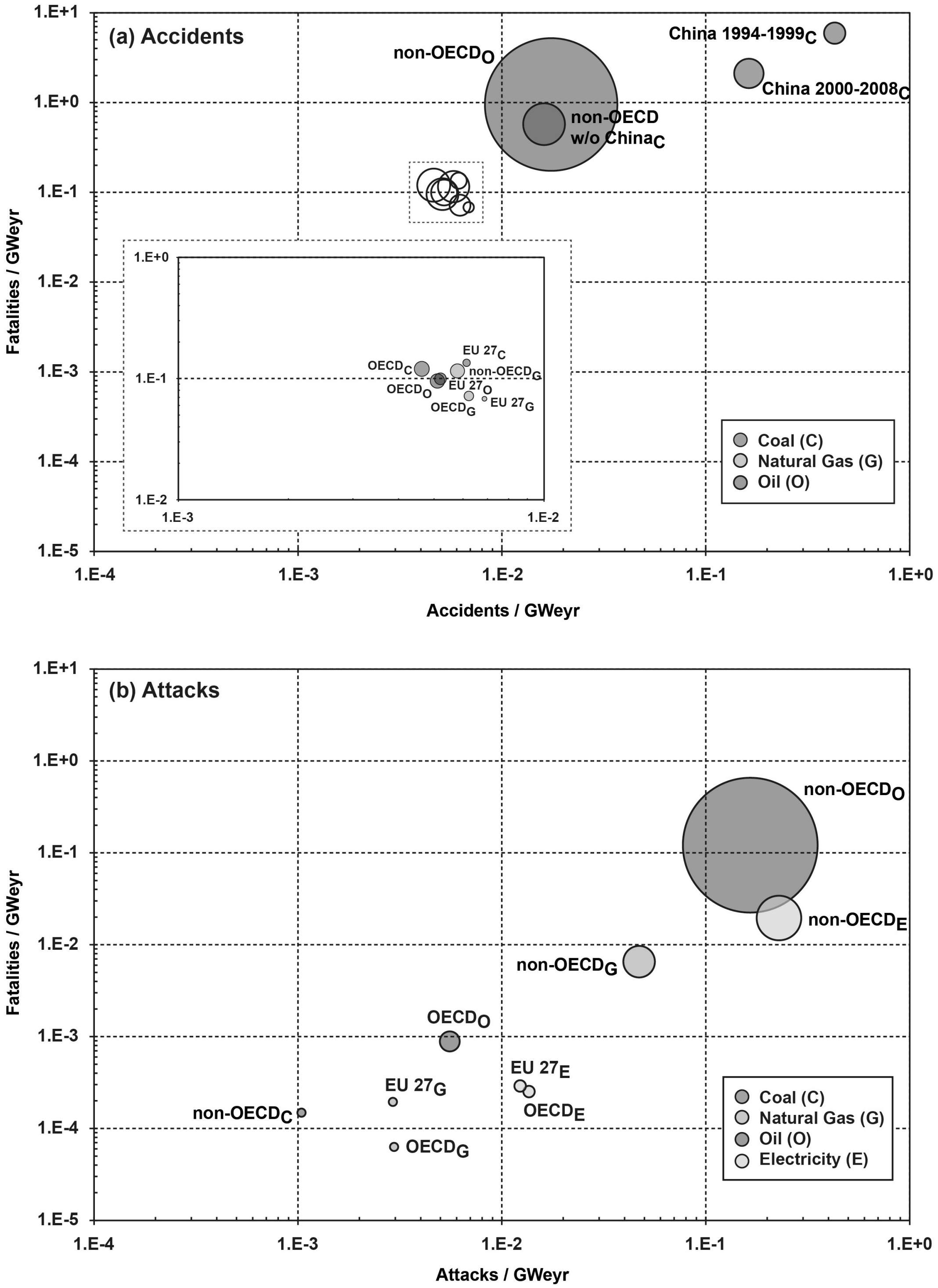


Figure 5: Comparison of technological accidents (a) and intentional attacks (b) by means of three risk indicators for different energy chains and country groups (OECD, EU 27, non-OECD). Frequencies of events (accidents or attacks) and consequences in terms of fatalities were normalized to the unit of energy production (Gigawatt-electric-year, GWeyr), whereas maximum consequences refer to the most deadly single event.

- The severity distribution for accidents generally exhibits a fat-tail, with low-probability high-consequence events being an important factor of energy chain performance as well as a proxy to provide a quantitative measure for risk aversion.
- For intentional attacks severe consequences in terms of fatalities are less an issue because "linear" infrastructures (e.g. pipelines and transmission lines) are predominantly targeted and not "point" sources such as refineries or power plant. The reason for this is that the former are more difficult to protect than the latter because they often lead trough remote areas. At the same time, population density is normally low in rural regions, which of course limits the severity potential with regard to fatal consequences However, frequent and multiple attacks against a pipeline system or electricity grid can result in substantial business and supply disruptions.
- Taking a holistic energy security perspective, it is important to take into account technological accidents and intentional attacks. Both of them have their specific characteristics, and thus address different risk aspects in a complementary manner.

V. Recommendations and Outlook

- This study provided a set of objective and quantitative risk indicators for accidental events and intentional attacks, to which various energy technologies are exposed. Such information is important for policy and decision makers to ensure that allocation of often limited resources for critical infrastructure protection takes into account actual hazard and threat levels, and is not just based on subjective risk factors (e.g. perception, aversion) or individual stakeholder preferences. Therefore, quantitative risk assessment should be an integral part of a national risk assessment (NRA) that aims to manage a country's critical infrastructures, and to prioritize and improve preparedness and contingency planning for disastrous events.
- This type of indicator-based approach to informed decision making can be used by various stakeholders to broaden the scope and depth of their analytical frameworks. Authorities, regulators and industry are commonly using performance indicators, whereas military or other security services have been somewhat more reluctant to include quantitative risk indicators in a systematic and formal manner in their assessments.
- The current study also clearly underpins the fact that the evaluation of accident risks is a well-established discipline, and has experienced a significant development since its beginning in the 1960s and early 1970s. In contrast, the analysis of the whole spectrum of intentional attacks (not just terrorist threat) is clearly lagging behind, both in terms of methodological approaches and availability of consistent and long-term data for certain countries and regions. The EIAD offers a powerful means to effectively close this gap, and to provide direct inputs for scenario analysis and predictive modeling.
- Although, the present assessment focused mostly on fossil energy chains, future studies should consider new renewable technologies in a much more detailed manner. On the one hand, new renewables are considered to reduce long-term resource availability issues and to suffer less from geographical concentration, but on the other hand new interdependencies and risk aspects may arise through large-scale imports of renewable electricity from North Africa to Europe.