Systemic Risks in the Electric Power Infrastructure?

by Carsten Orwat, ITAS

As envisaged by developers, economic actors or politicians, advanced information and communication technologies (ICT) should be utilized in electricity infrastructures to an unprecedented level, mainly to enhance the capability to handle the more volatile power supply by renewable energy sources. However, the extended use of ICT can also be a source of additional risks, due to the increased "openness" of the ICT-intensive infrastructure, increased complexities, interdependencies or system-wide failures, potential failures of ever more complex governance structures, or incoherent technical and governance developments. We raise the question whether systemic risks may emerge in the electricity sector, and which research perspectives for technology assessment may then be useful.[1]

1 Ongoing and Envisioned Developments in the Electricity Infrastructure

Recently, there is considerable political support for modernizing the electricity industry by developing and deploying advanced information and communication technologies (ICT), and to realize visions of the so-called "smart grid" or "internet of energy" (e.g., European Commission 2009; BMWi 2008; IEA 2011). One of the main goals of such strategies is to enhance the large-scale integration of the volatile power supply by renewable energy sources, especially photovoltaic- and wind energy. Additionally, it is aimed at enhancing the reliability of the electricity system in view of an ageing electricity infrastructure. To these ends, a multitude of technical and organizational measures for bettering the balance of the generation, transmission, distribution and consumption of energy at all stages of the electricity value chain are currently being proposed, developed, deployed or enhanced (Table 1).

While ICT systems have been used in the electricity sector for decades, the ongoing and envisaged developments cause a higher degree of automation, connectivity, and virtualization for the management and control of the electricity system. On the one hand, this may have many advantages, such as increased economic and energy efficiency or enhanced reliability. On the other hand, it is also widely acknowledged that new vulnerabilities and cyber security issues are introduced.

Actors of public governance have already responded to them (e.g., NIST 2010; NERC 2010). In Germany, like in many other countries, the government has initiated a Critical Infrastructure Protection (CIP) strategy (named "KRITIS" strategy) that is, among other things, realized by the recent implementation of the Cyber Security Strategy, including the establishment of a National Cyber Response Centre and a National Cyber Security Council (BMI 2011). Additionally, national multi-actor crisis-management exercises (LÜKEX) are regularly carried out, of which the exercise in 2011 is explicitly dedicated to cyber attacks. Additionally, several laws[3] require security measures, and a broad range of standards and guidelines define ICT security, in particular the ISO/IEC 27000 standard series (overview given by Wendt 2011; see also DKE 2010).

In the following, we elaborate on the interactions of technological developments with governance structures, interpreting them as ambivalent relations. Governance is necessary to mitigate risks, but governance structures can also be sources of risks or even systemic risks. The following considerations are based on the assumption that the dependability of the system is not only attained by research, development and availability of potentially reliable ICT components, but the safety of real systems depends on the actual choice and deployment of system components within the constellation of the entire system and its overall architecture. In highly regulated industries, like the electricity industry, the actual design, choice and deployment of ICT components largely depends on the incentives and constraints given by governance structures and procedures. Therefore, we assume that governance may also provide incentives and constraints that may cause ICT-related risks that may have systemic consequences. After shedding some light on the understandings of systemic risks (Section 2), we point out potential sources of systemic risks in the electricity sector. In this paper, they are subdivided for a better understanding (Section 3 and 4), but in reality, such sources are closely related.

Table 1: Fields of technological and sectoral developments of the "Smart Grid"

Fields	*Description*
Wide-area monitoring and control	Monitoring and control technologies, as well as advanced system analytics, enhance the data provision about the status of electricity systems components, behaviour and performance across interconnections and over large geographic areas. They help better to mitigate wide-area disturbances, for instance, by early warning systems, and improve transmission capacity and reliability, also better to balance volatile power supplies over long distances. Such applications necessitate cooperation across regional responsibilities for energy supply.
Transmission enhancement applications	Flexible alternating current transmission systems (FACTS) regulate the voltage and load flows in grids to handle incalculable load flows better, such as those from wind energy plants. High voltage direct current (HVDC) technologies are used to transport power across greater distances, like those from offshore wind farms.
Distribution grid management	Enhanced sensing and automation in distribution grid processes should reduce outage and repair time, for instance, by fault location or automatic network reconfigurations. It can also enable decentralized energy management, with local balancing between conventional and fluctuating energy technologies and transfers to the surrounding grid (see also the concept of "virtual power plants", "islanding" or "micro grids") (European Commission 2006, p. 27)
ICT integration	To reach the goals of the transformation to the "smart grid", it is stated that an "end-to-end" integration of all components of the energy system across different grids and across company boundaries with the help of a uniform communication infrastructure is necessary. For this integration, the metaphor of the "internet of energy" was coined (BDI 2010). One crucial step is enabling the bi-directional communication between the actors. The communication infrastructure uses private utility communication networks or public networks (cellular, cable, telephone networks, internet).
Advanced metering infrastructure	The advanced metering infrastructure includes a range of technical deployments that should provide functionalities like sending remote price signals of power consumption, ability to collect, store and report customer energy consumption data, improve energy diagnostics, improve location of outages, remote connection or disconnection, or losses or theft detection. The components at the residential customer side are the so-called "smart meters", which are the digital substitutes for the common Ferraris meters. In many European countries, it is a legal duty to install "smart meters".2 Commercial and industrial customers already use time-based measurement of their energy consumption.
Customer-side systems (building automation, "smart homes")	Such systems installed on the industrial or residential side include energy management systems, energy storage devices, "smart appliances", and distributed generation. They are used to manage energy consumption and generation in order to realize energy efficiency gains or peak demand reductions. An important part is the "demand response management" (or "demand side management") envisaged with manual control by the customer or automated response by price-sensitive appliances connected to an energy management system or remotely controlled by the utility or system operator. Dynamic pricing is the basis for "demand response management" (see below).
Charging infrastructure for electric vehicles	For the large-scale use of electric vehicles, a completely new infrastructure is necessary in order to facilitate decentralized charging, billing, or ancillary services, like peak load shaving or discharging, if electric vehicles serve as energy storages. In order to facilitate such transactions, interactions with the advanced meter infrastructure and customer-side systems become necessary.
Economic applications and new business models	With new business models it is planned that energy utility companies install and operate decentralized energy production plants, like micro gas turbines or combined heat and power (CHP) plants at the customer side ("contracting"), transmission and distribution grid operators provide information services of generation and sales data, a larger number of actors become market players at energy exchanges, or new consultancy services emerge, such as those for energy consumption optimization. For improving the shifting of power consumption by residential customers, energy companies have to provide dynamic pricing (e.g., time-differentiated pricing). All new business models require a functioning ICT infrastructure and standardized communication protocols that facilitate the automated processing of the large mass of transaction data.

Source: The non-exhaustive list is based on IEA (2011, pp. 17–20); BDI (2010, pp. 13–25), and Appelrath et al. (2011).

2 Understandings of Systemic Risks

One of the main tasks of technology assessment is to identify risks of technological developments and to develop options to cope with them, including political measures. Currently, analyses of technology assessment are also extended to systemic risks (Hellström 2009; Klinke, Renn 2006; Renn, Keil 2008; Keil et al. 2008). In the last years, analyses of systemic risks have gained considerable impetus through the financial crises, so that the majority of studies on systemic risks can be found in the field of finance and banking (e.g., Kaufman, Scott 2003; Kambhu et al. 2007) (see also Willke in this issue). Only a few studies use the approach of "systemic risks" in analyses of infrastructure risks, and they mostly point to a need for further research (Hellström 2007, 2009; Bartle, Laperrouza 2008; Laperrouza 2009; Mellstrand, Ståhl 2009). Besides the fact that there is currently no commonly accepted definition of "systemic risks", there is also a need for further research to characterize systemic risks and to develop methods for their analysis.

In the following, systemic risks are understood to be risks relating to or common to the entire system, or large parts of it, endangering its functioning, performances or attainment of societal goals. Systemic risks may emerge when the organizational and technological structures of the system would enable propagations of failures or system-wide failures (Section 3), when the sector-organizational and governance structures systematically lead to risk-generating behaviour or suboptimal risk management, or when governance structures do not develop adequately with technological or industrial developments endangering the achievement of societal goals like safety and the containment of risks, security of the energy supply, or social acceptability (Section 4). From this perspective, analyses of systemic risks in critical infrastructures have to take technical, industrial, institutional, and governance structures and the interactions among them into account.

3 Cascading or System-wide Failures

Critical infrastructure systems, especially the electricity-, telecommunication-, computation-, and transport infrastructures increasingly converge on each other (e.g., Amin 2005) leading to increased interdependencies among infrastructure systems. Such interdependencies, especially among the electricity-, IT- and communication infrastructures, are already subjects of risk analyses and simulations to consider cascading effects in particular (Rinaldi et al. 2001; IRGC 2006, 2010; Panzieri, Setola 2008; Petermann et al. 2011). The analyses demonstrate that the larger interdependencies among infrastructures, especially the increased integration of electricity networks with the internet, significantly lead to systemic risks, as exemplified by wide-area electric power outages. Internet connections are used for control and communication in the electricity sector, but the operation of the internet infrastructure itself depends on electricity, and has usually only limited energy reserves (Bartle, Laperrouza 2008; Petermann et al. 2011, pp. 70–93). However, besides such analyses, many questions are still open, such as who is responsible, with which scope, capabilities, cooperation models, or authority to monitor and govern interdependencies among infrastructures, and how several new cyber security issues and new interdependent components and actors, like internet service providers, trust services, certification services, or energy consultancy services, are included.

The realization of the "smart grid" necessitates a high level of connectivity in order to overcome "islands of automation" (NERC 2010, p. 12). To a large extent this should be based on Internet Protocol (IP) networks. On the one hand, IP networks facilitate a real-time, two-way communication that is essential for the "smart grid", are also highly cost-effective by using existing internet communication lines (especially to households facilitating demand-side management), use a flexible and widely accepted communication standard, and have some reliability advantages due to the dynamic routing capabilities (e.g., Davies 2010; Pearson 2011, p. 5214).

On the other hand, the use of IP networks brings more "openness" for accidental behaviour or malicious attacks, such as denial-of-service attacks by flooding, exploits, viruses or worms (e.g. IRGC 2006, pp. 43–48). However, the actual realization of "internet-induced" risks depends on case-specific deployments of security levels in IP communication and the specific protection measures

used such as encryption, access control, authentication, etc. What makes the use of IP networks a factor for systemic risks is their common use and widespread knowledge about their vulnerabilities. If used on a mass scale, this implies "... making any vulnerabilities they carry also exploitable on a mass scale." (Pearson 2011, p. 5214) The same holds true for the large-scale use of commercial-off-the-shelf (COTS) hard- and software (including operating systems) instead of using customized solutions. This is a common trend in the electricity sector (e.g., Ericsson 2010; Pearson 2011, p. 5214; see also Perrow in this issue). If, for example, IP-connected and standardized "smart meters" based on commodity hard- and software are deployed on a mass scale, malicious hackers can turn off "smart meters" on a mass scale, which would have negative systemic impacts at the distribution level (McDaniel, McLaughlin 2009, pp. 76–77).

In addition, the "smart grid" infrastructure will be built on existing ICT applications in the electricity sector, so-called "legacy systems", besides the newly-added "intelligent" systems. Therefore, vulnerabilities of the legacy systems could lead to compromises of the new "smart grid" technologies with systemic consequences (Flick, Morehouse 2011, pp. 54–55). The mixture of newly-added and legacy ICT systems could lead to strange and hardly predictable behaviour, especially because a large portion of ICT components stem from third parties (Mellstrand, Ståhl 2009, p. 3). This is especially relevant in cases of software updates, where the interaction of added and legacy systems is often problematic to predict, with the result that they are often the reason for IT-related incidents in critical infrastructures (Tervo, Wiander 2010).

Another source of systemic risk can be seen in the massive amount of sensitive data transferred in the "smart grid", like data from monitoring and control devices, administrative and personal data, like metering and billing information, or data of building controllers. Such data transfers have to be encrypted, necessitating a cryptographic-key management infrastructure. The high costs of maintaining such an infrastructure and the limited capabilities of such processors, that are likely to be installed in mass-uses, to conduct high-performance encryptions contradict attaining such protection goals (Khurana et al. 2010, pp. 83–84).

4 Problematic Governance Structures

In the following, we assume that systematically-created risks are caused by failures in sector-organizational and regulative structures, in other words, the governance structures. In the normal running of businesses, inappropriate incentive structures may stimulate rational actors to generate risk factors. Here, the system itself produces conditions that endanger its functions and performances. If governance structures work system-wide, the implications do also. From this perspective, an assessment of systemic risks is an analysis of social processes that create, maintain or endanger a socio-technical infrastructure system (see also Büscher in this issue). Thus, we focus on the incentives and constraints that are imposed by governance structures and that influence how risks are actually handled by individual actors and, therefore, influence the dependability of components and of the entire system.

4.1 Problematic Incentives and Regulation

In general, we assume that, if governance structures do not stimulate or demand other behaviour, actors may create risks by system applications that follow especially an economic logic that might deviate from a security-engineering logic. In general, insights from behavioural, economic and sociological research indicate that actors – in trading off external governance requirements (e.g., laws or regulations) or competitive advantages by high security reputation against profitability or capacities – do not invest in ICT security at a level that would be optimal from an security-engineering viewpoint (e.g., Croll 2010; Gordon, Loeb 2004; Dynes et al. 2008).

Governance reforms for liberalization and privatization impose economic pressures on infrastructure operators (e.g., van der Vleuten, Lagendijk 2010). That has led to decreasing redundancy or redundant back-up systems and letting electricity systems be operated closer to the margin (e.g., IRGC 2006, pp. 20–29; Cohen 2010, p. 62). Cost considerations are also relevant when actors connect control systems or Supervisory Control and Data Acquisition (SCADA) systems to IP connections or utilize the aforementioned COTS systems (e.g., Apt et al. 2006, p. 222; Nartmann et al.

2009; IRGC 2006). Furthermore, infrastructure operators are less incentivized to report and share information about reliability problems, software failures or cyber threats, thus hampering the learning important in risk prevention (Apt et al. 2006, pp. 226–229; US GAO 2011, pp. 24–25).

Another example is the certification of IT security, as one often favoured policy instrument for software security[4], that is controversially discussed (e.g., Anderson, Fuloria 2009). Many certification schemes for software dependability examine the existence of standard proof procedures and not the evidence of the actual fulfilment of dependability goals (Jackson 2009, p. 80). Additionally, a performance audit of risks governance structures conducted by the United States Government Accountability Office in 2009 to 2011 indicates that infrastructure utilities are focusing more on compliance with cyber security requirements, in particular on meeting minimum regulatory requirements, instead of designing a comprehensive approach to system security (US GAO 2011, p. 23). Furthermore, consumers are sub-optimally informed about the options and benefits of secure systems, and consequently have a low willingness to pay for secure products. Here, improvements in governance with the help of effective certification and labelling schemes are needed (US GAO 2011, p. 23).

4.2 Increased Complexity of Actor Constellations

In general, economic and behavioural research on ICT security indicates that, in systems deployed and run by many actors, system safety may also have the characteristics of a "public good", with the tendency that individual actors "free-ride" on the contributions by others, leading to an inefficient overall security level (e.g., Varian 2004). Since liberalization, unbundling of functionalities, and privatization in the 1980s and 1990s, infrastructures are already complex, due to the increased number of market and governing actors, and due to institutional fragmentation (e.g., Mayntz 2009; Finger et al. 2005; de Bruijne, van Eeten 2007). The sectoral organization and regulative structure of the energy sector become more complex through the large-scale integration of governance issues of ICT systems that may result in a higher risk of governance failures for instance, due to failures to cooperate. This can be the case in providing public goods, like commonly usable laboratories for security testing, databases for knowledge about cyber threats or solutions and best practises, or like standards for interoperability and transfer of transaction data[5]. Solutions are necessary to incentivize multiple actors with heterogeneous interests adequately to disclose and share data on system failures, and to cooperate in inter-firm governance settings to prevent systemic risks; or, if such measures are regarded as public goods, subsidizing of such measures by public funds should be considered (Assaf 2007; Dynes et al. 2008; Moore 2010; Masera 2010).

4.3 Incoherent Technological and Governance Developments

If governance structures and technologies do not develop correspondingly over the course of time, this can also cause systemic risks, in the sense that social goals like system safety, data protection, privacy, accessibility, social acceptability etc. (see also Finger et al. 2005; IRGC 2010, pp. 33–37) are not attained. For instance, this would be the case when the security-supervisory and regulative structure of critical infrastructures do not cover new risks or have inappropriate approaches in view of new risks, such as those from increased interdependencies, when security regulations would be too slow to adapt to fast-evolving cyber threats, or when the now prevailing self-organization of security measures would turn out to be ineffective.

As an example, "smart grid"-related regulatory efforts by the German Federal Office of Information Security (BSI) focus mainly on the Protection Profile for "smart meters". In contrast, security issues of IP-connected Energy Management Systems in residential premises are at the moment unregulated, and are left to the decisions of customers. With the aforementioned information lack about security issues, which customers usually have, and the resulting low willingness to pay for secure products, it is likely that the market outcome is a suboptimal security level.

Examples of further adverse governance structures in the electricity sector are unsuitable constellations of actors and the current version of the incentive regulation[6] that hinder or do not suf-

ficiently stimulate the necessary investments in the modernization of networks with "intelligent" systems (SRU 2011, pp. 477–484; Brunekreeft et al. 2011). Additionally, governmental actors involved in public-private partnerships are highly dependent on the expertise of developers and operators. This dependence is increasing ever more with the extended use of ICT in critical infrastructures. Therefore, governance structures with a changed role of governments must be adapted to changed structures of expertise and knowledge (Dunn-Cavelty, Suter 2009; Mills et al. 2008).

Furthermore, a large portion of mechanisms and rules for managing and controlling the abundance of transactions, such as system monitoring, metering, billing, etc., have to be programmed in software systems to be manageable at all ("software as an institution"). However, if software-based rules are not coherent with the existing regulative framework and with the expectations and values of users or affected actors – for instance, regarding access, affordability, treatment of personal data, or fairness of market conditions – then the acceptability of and the trust in the system are endangered, and their legitimacy questioned.[7] Advanced models of stakeholder participation in system development, standardization and use may contribute to preventing or mitigating such problems (e.g., Orwat, Raabe et al. 2010).

5 Conclusion

Risk assessments that focus only on the reliability of single components and physical interconnections are important, but seems not fully sufficient from a systemic viewpoint due to experiences with ICT-related organizational and regulative failures, increased interdependencies and complexities, and incoherence between technical and governance developments as potential sources of risks. Instead, a complementary systemic perspective that explicitly takes the interactions and co-development of technologies, social-organizational, regulative structures into account, seems more adequate to analyse reasons for dysfunctional behaviour of ICT systems, organizations or people, which may result from inappropriate incentives or controls of governance structures. From this perspective, the task of technology assessment is also to ask about the effectiveness and efficiency of risk governance structures, or whether the interplay of technology developments, sectoral-organizational and regulative governance structures causes new risks or even systemic risks.

Notes

1) This article is partly based on former publications by the author (Orwat, Büscher et al. 2010; Orwat 2011).
2) In Germany, Article 21c of the Energy Industry Act (Energiewirtschaftsgesetz – EnWG) requires the step-by-step installation of "smart meters" for buildings and plants since 2010. For a discussion of this legal duty, see Raabe et al. (2010).
3) In Germany, the most important legal security duties for energy utilities are provided by the Energy Industry Act (Energiewirtschaftsgesetz – EnWG). Other laws provide general IT security requirements, such as the Telecommunications Act (§ 109 Telekommunikationsgesetz – TKG) or the Federal Data Protection Act (§ 9 Bundesdatenschutzgesetz – BDSG) (Gaycken, Karger 2011, pp. 6–7).
4) See, for instance, the ISO/IEC 27002 information security standard, including certification, the "Common Criteria" certification scheme, or the standards for IT security management by the German Federal Office of Information Security (BSI).
5) The current problem of incompatible data formats for smart meter communication, i.e. EDIFACT versus the XML standard, is an example.
6) Compare the Incentive Regulation Ordinance (Anreizregulierungsverordnung – ARegV).
7) For example, due to consumer concerns on privacy issues the installation of "smart meters" is no longer compulsory in the Netherlands.

References

Amin, M., 2005: Infrastructure Security: Reliability and Dependability of Critical Systems. In: IEEE Security and Privacy 3/3 (2005), pp. 15–17

Anderson, R.; Fuloria, S., 2009: Certification and Evaluation: A Security Economics Perspective, ETFA 2009–2009 IEEE Conference on Emerging Technologies and Factory Automation

Appelrath, H.-J.; Behrendt, F.; Bognar, K. et al., 2011: Forschungsfragen im „Internet der Energie". In: acatech Materialien Nr. 1. acatech – Deutsche Akademie der Technikwissenschaften. Munich

Apt, J.; Morgan, M.G.; Lave, L.B., 2006: Electricity: Protecting Essential Services. In: Auerswald, P.E.;

Branscomb, L.M.; La Porte, T. et al. (eds.): Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability. New York, pp. 211–238

Assaf, D., 2007: Government Intervention in Information Infrastructure Protection. In: Goetz, E.; Shenoi, S. (eds.): Critical Infrastructure Protection. Heidelberg, pp. 29–39

Bartle, I.; Laperrouza, M., 2008: Systemic Risk in the Network Industries: Is there a Governance Gap? 5th ECPR General Conference, Potsdam University, September 10–12, 2009, Potsdam

BDI – Federation of German Industries/Bundesverband der Deutschen Industrie, 2010: Internet of Energy. ICT for Energy Markets of the Future. The Energy Industry on the Way to the Internet Age, BDI publication no. 439. Berlin

BMI – Federal Ministry of the Interior/Bundesministerium des Inneren, 2011: Cyber Security Strategy for Germany. Berlin

BMWi – Federal Ministry of Economics and Technology/Bundesministerium für Wirtschaft und Technologie, 2008: E-Energy. ICT-based Energy System of the Future. Berlin

Brunekreeft, G.; Friedrichsen, N.; Brandstätt, C. et al., 2011: Innovative Regulierung für Intelligente Netze (IRIN). Abschlussbericht (Kurzfassung). Bremer Energie Institute. Bremen

Cohen, F., 2010: The Smarter Grid. In: IEEE Security and Privacy 8/1 (2010), pp. 60–63

Croll, P.R., 2010: System and Software Assurance – Rationalizing Governance, Engineering Practice, and Engineering Economics, 2010 IEEE International Systems Conference Proceedings, SysCon 2010

Davies, S., 2010: Internet of Energy. In: Engineering and Technology 5/16 (2010), pp. 42–45

de Bruijne, M.; van Eeten, M., 2007: Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment. In: Journal of Contingencies and Crisis Management 15/1 (2007), pp. 18–29

DKE – German Commission for Electrical, Electronic & Information Technologies of DIN and VDE/ Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE, 2010: The German Roadmap E-Energy/Smart Grid. Frankfurt a. M.

Dunn-Cavelty, M.; Suter, M., 2009: Public-Private Partnerships are no Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection. In: International Journal of Critical Infrastructure Protection 2/4 (2009), pp. 179–187

Dynes, S.; Goetz, E.; Freeman, M., 2008: Cyber Security: Are Economic Incentives Adequate? In: Goetz, E.; Shenoi, S. (eds.): Critical Infrastructure Protection, New York, pp. 15–27

Ericsson, G.N., 2010: Cyber Security and Power System Communication – Essential Parts of a Smart Grid Infrastructure. In: IEEE Transactions on Power Delivery 25/3 (2010), pp. 1501–1507

European Commission, 2006: European Smart Grids Technology Platform. Vision and Strategy for Europe's Electricity Networks of the Future. Luxembourg

European Commission, 2009: ICT for a Low Carbon Economy. Smart Electricity Distribution Networks. Luxembourg

Finger, M.; Groenewegen, J.; Künneke, R., 2005: The Quest for Coherence Between Institutions and Technologies in Infrastructures. In: Journal of Network Industries 6/4 (2005), pp. 227–261

Flick, T.; Morehouse, J., 2011: Securing the Smart Grid: Next Generation Power Grid Security. Amsterdam, Boston

Gaycken, S.; Karger, M., 2011: Entnetzung statt Vernetzung – Paradigmenwechsel in der IT-Sicherheit. In: Multimedia und Recht – Zeitschrift für Informations-, Telekommunikations- und Medienrecht 14/1 (2011), pp. 3–8

Gordon, L.A.; Loeb, M.P., 2004: The Economics of Information Security Investment. In: Camp, L.J.; Lewis, S. (eds.): Economics of Information Security, Dordrecht, pp. 105–127

Hellström, T., 2007: Critical Infrastructure and Systemic Vulnerability: Towards a Planning Framework. In: Safety Science 45/3 (2007), pp. 415–430

Hellström, T., 2009: New Vistas for Technology and Risk Assessment? The OECD Programme on Emerging Systemic Risks and beyond. In: Technology in Society 31/3 (2009), pp. 325-331

IEA – International Energy Agency, 2011: Technology Roadmap Smart Grids. Paris

IRGC – International Risk Governance Council, 2006: Managing and Reducing Social Vulnerability from Coupled Critical Infrastructures. Geneva

IRGC – International Risk Governance Council, 2010: The Emergence of Risks: Contributing Factors. Geneva

Jackson, D., 2009: A Direct Path to Dependable Software. In: Communications of the ACM 52/4 (2009), pp. 78–88

Kambhu, J.; Weidman, S.; Krishnan, N. (eds.), 2007: New Directions for Understanding Systemic Risk. A Report on a Conference Cosponsored by the Federal

Reserve Bank of New York and the National Academy of Sciences. Washington, DC

Kaufman, G.G.; Scott, K.E., 2003: What is Systemic Risk, and do Bank Regulators Retard or Contribute to it? In: Independent Review 7/3 (2003), pp. 371–391

Keil, F.; Bechmann, G.; Kümmerer, K. et al., 2008: Systemic Risk Governance for Pharmaceutical Residues in Drinking Water. In: GAIA 17/4 (2008), pp. 355–361

Khurana, H.; Hadley, M.; Lu, N. et al., 2010: Smartgrid Security Issues. In: IEEE Security and Privacy 8/1 (2010), pp. 81–85

Klinke, A.; Renn, O., 2006: Systemic Risks as Challenge for Policy Making in Risk Governance. In: Forum Qualitative Sozialforschung 7/1 (2006), p. Art. 33

Laperrouza, M., 2009: Does the Liberalization of the European Railway Sector Increase Systemic Risk? In: Palmer, C.; Shenoi, S. (eds.): Critical Infrastructure Protection III. Third Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Hanover, NH, USA, March 23–25, 2009, Revised Selected Papers. Berlin, pp. 19–33

Masera, M., 2010: Governance: How to Deal with ICT Security in the Power Infrastructure? In: Lukszo, Z.; Deconinck, G.; Weijnen, M.P.C. (eds.): Securing Electricity Supply in the Cyber Age. Exploring the Risks of Information and Communication Technology in Tomorrow's Electricity Infrastructure, Dordrecht et al., pp. 111–127

Mayntz, R., 2009: The Changing Governance of Large Technical Infrastructure Systems (Vortrag auf der Tagung „Complexity and Large Technical Systems", Meersburg, Mai 2008). In: Mayntz, R. (ed.): Über Governance. Institutionen und Prozesse politischer Regelung. Frankfurt a. M., pp. 121–150

McDaniel, P.; McLaughlin, S., 2009: Security and Privacy Challenges in the Smart Grid. In: IEEE Security and Privacy 7/3 (2009), pp. 75–77

Mellstrand, P.; Ståhl, B., 2009: Analyzing Systemic Information Infrastructure Malfunction, 2009 4th International Conference on Critical Infrastructures. CRIS 2009

Mills, D.E.; Brown, K.; Waterhouse, J., 2008: Asset Management Stewardship: The Effectiveness of Public-private Mix Governance Structures, 1st International Conference on Infrastructure Systems and Services: Building Networks for a Brighter Future. INFRA 2008

Moore, T., 2010: The Economics of Cybersecurity: Principles and Policy Options. In: International Journal of Critical Infrastructure Protection 3/3-4 (2010), pp. 103–117

Nartmann, B.; Brandstetter, T.; Knorr, K., 2009: Cyber Security for Energy Automation Systems – New Challenges for Vendors. 20th International Conference on Electricity Distribution, Prague, 8-11 June 2009, Paper 0247

NERC – North American Electric Reliability Corporation, 2010: Reliability Considerations from the Integration of Smart Grid. Princeton

NIST – United States Department of Commerce, National Institute of Standards and Technology, 2010: Guidelines for Smart Grid Cyber Security. NIST Interagency Report (NISTIR) 7628. Washington, DC

Orwat, C., 2011: Technology Assessment of Software-Intensive Critical Infrastructures – A Research Perspective. In: Heiß, H.-U.; Pepper, P.; Schlingloff, H. et al. (eds.): Informatik 2011. Informatik schafft Communities. 4.–7. Oktober 2011 in Berlin. Bonn

Orwat, C.; Büscher, C.; Raabe, O., 2010: Governance of Critical Infrastructures, Systemic Risks, and Dependable Software. Technical Report. Karlsruhe Institute of Technology. Karlsruhe

Orwat, C.; Raabe, O.; Buchmann, E. et al., 2010: Software als Institution und ihre Gestaltbarkeit. In: Informatik-Spektrum 33/6 (2010), pp. 626–633

Panzieri, S.; Setola, R., 2008: Failures Propagation in Critical Interdependent Infrastructures. In: International Journal of Modelling, Identification and Control 3/1 (2008), pp. 69–78

Pearson, I.L.G., 2011: Smart Grid Cyber Security for Europe. In: Energy Policy 39/9 (2011), pp. 5211–5218

Petermann, T.; Bradke, H.; Lüllmann, A. et al., 2011: Was bei einem Blackout geschieht. Folgen eines langandauernden und großflächigen Stromausfalls. Berlin

Raabe, O.; Lorenz, M.; Schmelzer, K., 2010: Generic Legal Aspects of E-Energy. In: it – Information Technology 52/2 (2010), pp. 107–113

Renn, O.; Keil, F., 2008: Systemische Risiken: Versuch einer Charakterisierung In: GAIA 17/4 (2008), pp. 349–354

Rinaldi, S.M.; Peerenboom, J.P.; Kelly, T.K., 2001: Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. In: IEEE Control Systems Magazine 21/6 (2001), pp. 11–25

SRU – Sachverständigenrat für Umweltfragen, 2011: Wege zur 100 % erneuerbaren Stromversorgung, Sondergutachten. Berlin

Tervo, H.; Wiander, T., 2010: Sweet Dreams and Rude Awakening – Critical Infrastructure's Focal IT-related Incidents. Proceedings of the 43rd Hawaii International Conference on System Sciences 2010. Koloa, Kauai, Hawaii

US GAO – United States Government Accountability Office, 2011: Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed. Washington, DC: GAO-11-117

van der Vleuten, E.; Lagendijk, V., 2010: Interpreting Transnational Infrastructure Vulnerability: European Blackout and the Historical Dynamics of Transnational Electricity Governance. In: Energy Policy 38/4 (2010), pp. 2053–2062

Varian, H.R., 2004: System Reliability and Free Riding. In: Camp, L.J.; Lewis, S. (eds.): Economics of Information Security. Dordrecht, pp. 1–15

Wendt, M., 2011: Smart Grid – eine Herausforderung aus Sicht der Standardisierung und der IT-Sicherheit oder schon „business-as-usual". In: Datenschutz und Datensicherheit 35/1 (2011), pp. 22–26

Contact

Dr. Carsten Orwat
Karlsruhe Institute of Technology (KIT)
Institute for Technology Assessment and Systems Analysis (ITAS)
P.O. Box 36 40, 76021 Karlsruhe
Phone: +49 (0) 7 21 / 6 08 - 2 61 16
Email: orwat@kit.edu

« »

Mechanisms of Systematic Risk Production

New Perspectives for TA Research?

by Christian Büscher, ITAS

Which questions have to be posed, which scientific problems have to be addressed, and also, what kind of instruments are appropriate when tackling "Systemic Risk"? If complex systems cannot be analyzed in causalistic models, then TA and Systems Analysis have to reflect, first, on theoretical approaches, assessing the basic conditions and processes related to the reproduction of systems, and second, on innovative methods, gathering data to allow testing scientific constructions against reality. The analysis of "mechanisms" might be a direction of impact for gaining insight into self-reinforcing processes, precarious couplings between systems, or between elements of systems, and, in the end, into the systematic production of risk and danger.

1 General Considerations

Systems analysis has taken on the task of comprehensively documenting the social, economic, political, legal, as well as the technical and ecological consequences of planned action in system reproduction. In Technology Assessment, Bechmann sees, for that reason, a need for new forms of reflection and analysis. "Any action which intervenes technically and planned (purposively) in the natural environment has to watch over its impacts on the environment and their repercussions on itself" (Bechmann 2007, p. 35; Translation CB). Bechmann derives this dictum from Luhmann's suspicion that there will be not less, but more interventions into the natural environment, and that society, for that reason, should generate more knowledge about repercussions (Luhmann 1986, p. 39). With the concept of "systemic risks", system-analytical considerations with respect to risk and hazards are tackled, which do not refer to the relationship of society to its natural environment alone. It is much rather quite generally a matter of the