Technology Assessment of Software-Intensive Critical Infrastructures – A Research Perspective

Carsten Orwat

Institute for Technology Assessment and Systems Analysis,
Karlsruhe Institute of Technology
P.O. Box 3640
76021 Karlsruhe, Germany
orwat@kit.edu

Abstract: As envisaged by developers, industry actors or politicians, software systems will be utilized in critical infrastructures to an unprecedented level in order to realise virtualization, optimize resource efficiency or provide new functionalities. However, this can also be sources of additional (systemic) risks due to increased complexities and tights couplings, potential failures of complex governance structures, or incoherent technical and governance developments. We propose a research perspective of technology assessment that focuses on the interactions between technological developments and governance structures.

1 The Analytical Perspective of Technology Assessment on Technical and Governance Structures

Since its beginning in the 1960s, technology assessment is a tool of technology policy by providing scientifically produced knowledge for advising political decision-making and informing the public about technological developments and its implications like societal benefits, unintended consequences, or risks [e.g., Be07, Gr09]. Public technology assessment mainly focuses on societal issues of new technologies which cannot be adequately solved by technology developers or market actors alone. In many cases, technology assessment, thus, also explores the necessities and options of political interventions and of necessary adjustments of governance structures. Since socio-technical systems like infrastructures are becoming increasingly complex, fast-changing, and interdependent among each other, there is also a need for technology assessment focusing on systemic risks [KR06, He09].

Recently, issues of technology policy are often discussed using the notion of 'governance'. In the public policy context, 'governance' refers to situations of collective decision-making in which not only a government actor is the sole authority. Instead, multiple actors such as civil parties, private firms, business associations, or semi-public actors such as standardisation organisations supplement or substitute governmental actors in

erschienen im Tagungsband der INFORMATIK 2011
Lecture Notes in Informatics, Band P192
ISBN 978-3-88579-286-4

self-regulating or cooperative approaches in which negotiations to balance divergent interests are prevalent [e.g., Be09, Ma09, St98]. Governance structures encompass institutional arrangements consisting of formal rules (e.g., legal rules, standards or contracts) and informal rules (e.g., conventions or norms) with their enforcement mechanisms. However, the multitude of actors involved in governance and, especially, the inclusion of non-governmental actors in public decision-making causes several problems such as a higher degree of complex interdependence among governing actors, blurring of responsibilities, or difficulties about accountabilities [e.g., St98].

Table 1: Developments, Risks Factors and Options

	Developments	**Risk factors**	**Options**
Technology:	• Ubiquitous use of software systems • Technical definition and automatic enforcement of institutions • Higher degree of interdependency between infrastructure components • More commercial off-the-shelf software (COTS)	• Software systems as additional source of risks in infrastructures • "Opening up" of infrastructure systems to malicious attacks and inadvertent errors via software systems • Technical complexity, 'self-emergent phenomena' in interconnected self-organising systems	• Technological research on dependable algorithmics, reliable security and privacy, predictable self-organisation, transparent fault tolerance, etc. • Research on software concepts for critical infrastructures (modularity, customisation vs. COTS etc.)
Social organisation of production:	• Functional unbundling in supply networks • More decentralised production • Virtualisation (coupled heterogeneous resources; real time coordination) • 'De facto' industry organisation by software systems • More use of automatic market mechanisms in management of resources and markets	• Organisational characteristics influences risk management of software uses • Inappropriate couplings of infrastructures and infrastructure elements • Complexity and non-linear behaviour of actor constellations • Autonomous decisions without human (corrective) intervention • Inappropriate self-organisation (e.g. standardisation or certification schemes	• Research for appropriate organisational structure, institutional incentives and constraints (e.g., extended certification schemes, industry-wide risk management coping with interdependencies, 'public dependability goods' such as common experimental, modelling and simulation facilities)
Regulative structure:	• Political intervention from 'liberalization' to environmental protection • Increased number of governing actors (heterogeneous players, multi-level governance) • Converging governance areas (telecommunication, electricity, transport, internet) • Software governance becomes pivotal element for infrastructure governance	• Conflicting political objectives • Complexity in governance constellations: Lack of system-wide oversight; Uncoordinated governance; Unclear responsibility • Existent software governance structures inappropriate for critical infrastructures • Governance structure incoherent with organisational and technological developments	• Balancing of divergent political goals • Governance structures spanning system-of-systems • Improved governance of software • Coherent co-evolution of technical and governance developments

For analytical purposes, we can distinguish three layers included in infrastructure systems: the production structure, which encompasses (1) the technology used in producing a given good or service and (2) the social organisation of production ('internal governance' of a production system or industry), as well as (3) the regulative structure ('external regulative governance') of infrastructure systems [Ma09, p. 122]. Each of the technological, social-organisational and regulative layers of infrastructure systems underwent considerable changes in recent years and will be subject to further changes envisaged by research, industry and policy actors (see Table 1). At all layers we can find sources of risks that are only at the beginning to be understood in the ways they work and their consequences and for which research on options to counteract is necessary. This is discussed in the following.

From the governance perspective, we focus on three recent (interrelated) developments that might be sources of risks: Governance structures influence the dependability of software systems and critical infrastructures (Section 2). Software is regarded as catalyst of the convergence of technical and governance structures. With a growing complexity and dependability also risks of system and governance failures increases (Section 3). Software increasingly becomes part of the governance structures. If regulative functions embedded in software systems do not match legal norms or societal expectations there is a risk of lacking societal acceptability (Section 4).

2 Risks Influenced by Governance Structures

The governance structure with their institutional incentives and constraints to handle risks determines to a large extend how software-related risks are actually managed by individual actors and how risks resulting from interdependencies and cooperative activities are created. Not only the availability of dependable software systems is decisive, but also their actual deployment, adoption and use. Governance structures influence indirectly through the behaviour of the involved actors the dependability of software systems and of software-intensive infrastructures. We assume that systematically created risks are caused by failures in organisational and regulative structures. In the normal running of business, inappropriate incentive structures may stimulate rational actors to accumulate risk factors until a tipping point where damage occurs. Here, the systems produce by themselves conditions that endanger the system functions. From this perspective, a systemic risk assessment is an analysis of social processes that create, maintain or endanger a socio-technical infrastructure system [Bü11, p. 9].

These hypotheses about systematically created risks are exemplified by insights from behavioural, economic and sociological research. Risks of information systems can stem from low incentives for investments in ICT security especially by for-profit entities [Ha08, TW10]. In software development and use, actors normally balance costs and benefits of investing in software security trading off external governance requirements (e.g., laws or regulations) or competitive advantages by high security reputation against profitability or capacities [e.g., Cr10, GL04, Dy08, CL04]. Also risk-relevant couplings in and between infrastructures can be influenced by economic interests such as cost savings: Risks can stem, for example, from relying control systems or Supervisory Control and Data Acquisition (SCADA) systems on internet connections and services [e.g., Na09, IR06] or from the use with insecure computer operating systems that provide more functionality or potentials of cost reductions, but also considerably more vulnerability [e.g., Go09, AF09]. Thus, we can assume that if governance structures do not stimulate or demand other behaviour, actors may create risks by system installations that follow especially an economic logic that might deviate from a security engineering logic.

In systems made up by many actors, system reliability may also have the characteristics of a public good with the tendency that individual actors 'free-ride' on the contributions by others and the overall result is inefficient [Va04]. Furthermore, damage caused by lax information security or vulnerable products of one actor also causes damages (negative externalities) to other actors that share the data or system [CL04, AM09]. Decisions about security at an individual company level can lead to neglected risk prevention or to shifting risks to other actors and result in a sub-optimal risk level from a systemic perspective.

Furthermore, with regard to infrastructure dependability, analyses of the power outages in the USA and Europe revealed governance failures accompanied by technical failures as causes [e.g., VL10]. In many cases, economic pressures, as consequence of governance reforms, cause the decrease of redundancy or redundant back-up systems and to use commercial-of-the-shelf technologies [IR06]. Examples of counteracting governance structures can be found in the electricity sector where unsuitable constellations of actors hinder the necessary investments in the modernization of networks [e.g., SR10, pp. 477-484]. Furthermore, public-private partnership, as the dominant organisation model in infrastructures of today, has implications for the treatment of risks since private actors have to calculate an economically reasonable risk optimum that may deviate from the safety optimum [DS09, Mi08].

3 Risks from Converging and Complex Systems

Critical infrastructure systems, especially the electricity, telecommunication, computation, and transport infrastructures, not only complement but increasingly converge with each other [e.g., Am05]. Already, the information infrastructure includes multiple converging ICT infrastructure systems like internet, mobile telephony, or industrial control systems. The convergence of critical infrastructures may create new chances but also new risks, in particular stemming from a much higher degree of connectivity and interdependency among infrastructures and their components, which are mostly beyond the focus of usual risk analyses and risk management. This increases the potential of low probability, high impact risks to critical infrastructures.

From this perspective, systemic risks can be understood as a phenomenon in which failure of a system component leads to the dysfunction of the entire system or large parts of it [e.g., OE03, Ka07]. This is especially relevant for socio-technical systems with complex (non-linear) interactions and tight coupling of system components that may lead to unexpected complex interactions [Pe84]. Either unanticipated interactions among previously separated system components occur (when failures interact) or failures can cascade over system components if inappropriate system structures allow this [IR10, p. 23].

In the area of critical infrastructures, the application of the systemic perspective is evermore taken into account [e.g., BL08, La09], since the problem may become more relevant by the further realization of the virtualization paradigm and its inherent tight couplings. Also the increasing convergence of infrastructures can become a potential of systemic risks. Studies reveal that especially the coupling of interdependent networks is prone to cascading of failures such as the iterative shutdowns of power stations and internet communication networks [e.g., Ri01, IR06, IR10, Ve10, see also Pe10].

Previous research also suggests that most dependability problems of ICT systems in critical infrastructures do not consist in hostile attacks or problems internal to the technical system, but rather stem from socio-economic and technical conditions in complex system-of-systems developments that lack, for example, large-scale, holistic risk analysis and collaboration [TW10]. Furthermore, as illustrated by computer trading of securities without human control, a potential of uncontrolled chain-reactions and non-linear processes emerges from automated decision-making [e.g., GV10]. In the field of organic computing [e.g., MS10], similar phenomena have been recently analysed under the term of ‘emergent phenomena’ or ‘emergent behaviour’ that may show up as unanticipated behaviour in self-organising interactive ICT systems, which are also intended to use in future critical infrastructures.

Future infrastructures will have a plethora of tightly interconnected heterogeneous systems run by a multitude of public or private actors with heterogeneous interests in security. This has the effect of increased governance complexity at the socio-organisational and regulative layer with a higher risk of governance failures, for instance, due to a lack of motivation to cooperate. Since liberalization, unbundling of functionalities and privatization in the 1980s and 1990s, infrastructures are already complex due to the increased number of market actors and governing actors and due to institutional fragmentation [e.g., Ma09, Fi05, BE07]. Infrastructure governance becomes even more complex by the penetration of governance issues of software. However, it is an open question how governance structures have to be readjusted with regard to the more converging and interdependent infrastructures and to the new core elements of ICT in general and software systems in particular [Ma10].

4 Risks from Lacking Societal Acceptability and Incoherence

In order to realise the ‘real-time’, ‘self-organisation’ and ‘virtualization’ paradigms of critical infrastructures a large portion of institutional elements of the governance structures has to be programmed into software systems. In other words, institutional arrangements for enabling, steering, and controlling of the millions of decentralised transactions in future infrastructures have to be automated by software systems in order to be successfully handled or manageable at all. Economic and social transactions, which would otherwise be impeded by the difficulties encountered when erecting a conventional institutional framework, become now possible, efficient, and effective. Automation also helps to exclude occasional human error.

However, if software development, implementation, and the software-technical realisation of rules are not coherent with the expectations of users or affected actors (e.g. regarding access, affordability or fairness of market conditions) as well as with the existent institutional framework, the individual acceptance and the societal acceptability of the software systems are endangered and their legitimacy questioned. For instance, technical realisations of privacy protections may not be successful if they do not fulfil legal requirements or are in conflict with user expectations. Advanced models of stakeholder participation in software development, standardisation and use may contribute to prevent or solve such problems [e.g., Or10]. In addition, difficulties of policy measures in the software sector can be spread to infrastructure sectors such as the problems of software standardisation, for instance, which is plagued with problems of the dominance of some proprietary standards and ‘standard wars’ [e.g., SV99] or hurdles for participation [e.g., Or10].

Furthermore, research on interactions and co-evolutionary developments of technologies and governance structures become crucial, since the coherence is decisive for obtaining reliability, price efficiency, innovation capacity, data protection, accessibility, affordability etc. [see also Fi05, IR10, pp. 33-37]. For instance, the envisaged decentralisation with intelligent software-intensive control systems is hampered by the existent network governance structure organised as a centralised integrated system [e.g., Fi05, SR10]. Furthermore, corresponding to converging technological developments, adaptations of governance structures are necessary to incentivize actors across sectors to adequately disclose and share data on system failures or to cooperate in inter-firm risk governance to prevent systemic risks [As07, Dy08]. Also certification schemes have to be adapted to new forms of risks that stem from the interactions within and between infrastructures and their technical, organisational and human components [e.g., Ja07].

Conclusion

Risk assessment that focuses only on the reliability of system components and physical interconnections seems inadequate due to experiences with software-related organisational failures, increased interdependencies and complexities, and incoherence between technical and governance developments as potential source of risks. Instead, we propose a systemic perspective for technology assessment that explicitly takes the interactions and co-evolution of technologies, social-organisational and regulative structures into account to investigate reasons for dysfunctional behaviour of software systems or humans, which may result from inappropriate incentives or controls of governance structures.

References

[Am05] Amin, M.: Infrastructure security: Reliability and dependability of critical systems. IEEE Security and Privacy, 3(2005)3; pp. 15-17.

[AF09] Anderson, R.; Fuloria, S.: Security Economics and Critical National Infrastructure. The Eighth Workshop on the Economics of Information Security (WEIS 2009), University College London, England, 24-25 June, 2009

[AM09] Anderson, R.; Moore, T.: Information security: where computer science, economics and psychology meet. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 367(2009)1898; pp. 2717-2727.

[As07] Assaf, D.: Government Intervention in Information Infrastructure Protection. In (Goetz, E., Shenoi, S. eds.): Critical Infrastructure Protection. Springer, Heidelberg et al., 2007; pp. 29-39.

[BL08] Bartle, I.; Laperrouza, M.: Systemic risk in the network industries: is there a governance gap? 5th ECPR general conference, Potsdam University, September 10th -12th, 2009, Potsdam, 2008. Centre for the Study of Regulated Industries, School of Management, University of Bath, Bath

[Be07] Bechmann, G.; Decker, M. et al.: Technology assessment in a complex world. International Journal of Foresight and Innovation Policy, 3(2007)1; pp. 6-27.

[Be09] Benz, A.: Governance in Connected Arenas – Political Science Analysis of Coordination and Control in Complex Rule Systems. In (Jansen, D. ed.): New Forms of Governance in Research Organizations. Disciplinary Approaches, Interfaces and Integration. Springer, Dordrecht, 2007; pp. 3-22.

[Bü11] Büscher, C.: Systemische Risiken oder Mechanismen der systemischen Risikoproduktion? (Draft manuscript). Karlsruhe Institute of Technology, Karlsruhe, 2011.

[CL04] Camp, L.J.; Lewis, S. (eds.): Economics of Information Security, Advances in Information Security, Vol. 12. Springer, Heidelberg et al., 2004.

[Cr10] Croll, P.R.: System and software assurance - Rationalizing governance, engineering practice, and engineering economics. 2010 IEEE International Systems Conference Proceedings, SysCon 2010, 2010; pp. 604-609.

[BE07] de Bruijne, M.; van Eeten, M.: Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment. Journal of Contingencies and Crisis Management, 15(2007)1; pp. 18-29.

[DS09] Dunn-Cavelty, M.; Suter, M.: Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. International Journal of Critical Infrastructure Protection, 2(2009)4; pp. 179-187.

[Dy08] Dynes, S.; Goetz, E. et al.: Cyber Security: Are Economic Incentives Adequate? In (Goetz, E., Shenoi, S. eds.): Critical Infrastructure Protection, IFIP International Federation of Information Processing, Vol. 253. Springer, New York, 2008; pp. 15-27.

[Fi05] Finger, M.; Groenewegen, J. et al.: The Quest for Coherence Between Institutions and Technologies in Infrastructures. Journal of Network Industries, 6(2005)4; pp. 227-261.

[Go09] Gold, S.: The SCADA challenge: securing critical infrastructure. Network Security, 2009(2009)8; pp. 18-20.

[GV10] Goldin, I.; Vogel, T.: Global Governance and Systemic Risk in the 21st Century: Lessons from the Financial Crisis. Global Policy, 1(2010)1; pp. 4-15.

[GL04] Gordon, L.A.; Loeb, M.P.: The Economics of Information Security Investment. In (Camp, L.J., Lewis, S. eds.): Economics of Information Security. Kluwer, Dordrecht, 2004; pp. 105-127.

[Gr09] Grunwald, A.: Technology Assessment: Concepts and Methods. In (Meijers, A. ed.): Handbook of the Philosophy of Science, Volume 9: Philosophy of Technology and Engineering Sciences. Elsevier/North Holland, Amsterdam et al., 2009; pp. 1103-1146.

[Ha08] Haimes, Y.; Santos, J. et al.: Risk Analysis in Interdependent Infrastructures. In (Goetz, E., Shenoi, S. eds.): Critical Infrastructure Protection, IFIP International Federation of Information Processing, Vol. 253. Springer, New York, 2008; pp. 297-310.

[He09] Hellström, T.: New vistas for technology and risk assessment? The OECD Programme on Emerging Systemic Risks and beyond. Technology in Society, 31(2009)3; pp. 325-331.

[IR06] IRGC: Managing and Reducing Social Vulnerability from Coupled Critical Infrastructures. International Risk Governance Council (IRGC), Geneva, 2006.

[IR10] IRGC: The Emergence of Risks: Contributing Factors. International Risk Governance Council (IRGC), Geneva, 2010.

[Ja07] Jackson, D.; Thomas, M. et al. (eds.): Software for Dependable Systems: Sufficient Evidence?, National Research Council - Committee on Certifiably Dependable Software Systems. National Academies Press, Washington, D.C., 2007.

[Ka07] Kambhu, J.; Weidman, S. et al. (eds.): 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, Federal Reserve Bank of New York, National Research Council. National Academies Press, Washington, 2007.

[KR06] Klinke, A.; Renn, O.: Systemic Risks as Challenge for Policy Making in Risk Governance. Forum Qualitative Sozialforschung, 7(2006)1; p. Art. 33.

[La09] Laperrouza, M.: 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, New Hampshire, USA, March 23-25, 2009, Revised Selected Papers. Springer, Berlin, Heidelberg, 2009; pp. 19-33.

[Ma10] Masera, M.: Governance: How to Deal with ICT Security in the Power Infrastructure? In (Lukszo, Z., Deconinck, G. et al. eds.): Securing Electricity Supply in the Cyber Age. Exploring the Risks of Information and Communication Technology in Tomorrow's Electricity Infrastructure. Springer, Dordrecht et al., 2010; pp. 111-127.

[Ma09] Mayntz, R.: 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, Schriften aus dem Max-Planck-Institut für Gesellschaftsforschung, Band 62. Campus, Frankfurt am Main, New York, 2009; pp. 121-150.

[Mi08] Mills, D.E.; Brown, K. et al.: 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, 2008. IEEE

[MS10] Müller-Schloer, C.; Schmeck, H.: Organic Computing: A Grand Challenge for Mastering Complex Systems. it - Information Technology, 52(2010)3; pp. 135-141.

[Na09] Nartmann, B.; Brandstetter, T. et al.: Cyber security for energy automation systems - new challenges for vendors. 20th International Conference on Electricity Distribution, Prague, 8-11 June 2009, Paper 0247, 2009

[OE03] OECD: Emerging Risks in the 21st Century - An Agenda for Action. Organisation for Economic Co-operation and Development, Paris, 2003.

[Or10] Orwat, C.; Raabe, O. et al.: Software als Institution und ihre Gestaltbarkeit. Informatik-Spektrum, 33(2010)6; pp. 626-633.

[Pe84] Perrow, C.B.: Normal Accidents: Living with High-Risk Technologies. Basic Books, New York, 1984.

[Pe10] Petermann, T.; Bradke, H. et al.: Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung. Endbericht zum TA-Projekt, Arbeitsbericht Nr. 141. Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, Berlin, 2010.

[Ri01] Rinaldi, S.M.; Peerenboom, J.P. et al.: Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine, 21(2001)6; pp. 11-25.

[SV99] Shapiro, C.; Varian, H.R.: The Art of Standard Wars. California Management Review, 41(1999)2; pp. 8–32.

[SR10] SRU: Wege zur 100 % erneuerbaren Stromversorgung, Sondergutachten. Sachverständigenrat für Umweltfragen (SRU), Berlin, 2011.

[St98] Stoker, G.: Governance as theory: five propositions. International Social Science Journal, 50(1998)155; pp. 17-28.

[TW10] Tervo, H.; Wiander, T.: Sweet dreams and rude awakening - Critical infrastructure's focal IT-related incidents. Proceedings of the 43rd Hawaii International Conference on System Sciences - 2010, HICSS-43, Koloa, Kauai, Hawaii, 2010. IEEE; pp. 1-8.

[VL10] van der Vleuten, E.; Lagendijk, V.: Interpreting transnational infrastructure vulnerability: European blackout and the historical dynamics of transnational electricity governance. Energy Policy, 38(2010)4; pp. 2053-2062.

[Va04] Varian, H.R.: System Reliability and Free Riding. In (Camp, L.J., Lewis, S. eds.): Economics of Information Security. Kluwer, Dordrecht, 2004; pp. 1-15.

[Ve10] Vespignani, A.: The fragility of interdependency. Nature, 464(2010)7291; pp. 984-985.

erschienen im Tagungsband der INFORMATIK 2011
Lecture Notes in Informatics, Band P192
ISBN 978-3-88579-286-4