

Systemic risk in the network industries: is there a governance gap?

Paper presented at the 5th ECPR general conference, Potsdam University,
September 10th -12th, 2009.

Section: Regulation of Networks and Networks of Regulation.

Panel: Networks of Regulation and the Management of Transnational Risk

Ian Bartle and Marc Laperrouza
EPFL, Lausanne

Abstract

Systemic risks and hazards have become increasingly significant features of modern industrial society of which the network industries form a vital element. The idea of systemic risk, however, is much less prominent in the network industries compared to banking and finance. This paper addresses why there is such a difference between these sectors. It then addresses how complexity and systemic risk in the network industries should be managed and governed. Does it above all require more and better scientific and technical analysis to understand the risks and reduce uncertainty? Or does it require qualitatively different forms of governance that draw on many different types of knowledge, and involve a wider range of stakeholders? We argue in this paper that systemic risk is very important in the network industries and it needs to be considered more explicitly than hitherto in the governance and regulation of risk in the network industries. Traditional technocratic forms of risk management and governance while necessary are not sufficient, particularly due because of heightened uncertainty and interdependence. Unless and until the problems of uncertainty are overcome, means of governing risk and uncertainty beyond the technocratic are required. In particular, judgements by different experts and stakeholders are required about the nature of the uncertainty, about the potential hazards and their consequences, and about the level of caution required. This requires a more participative and open form of risk governance, a form which draws on socio-political forms of governance as well as technocratic. This is recognised in part in the recent literature on risk governance of critical infrastructures but the literature says little about the participative governance structures which might be appropriate nor how they may be developed in the patchwork that is the European regulatory environment for the network industries.

Key words: regulation, governance, European Union.

1. Introduction

The network industries – gas, electricity, transport, communications, water supply – are commonly seen as ‘critical’ infrastructures: they provide services without which modern society could not function and modern life would not be tenable. They are also examples of ‘systems’ or ‘systems of systems’ which, by their nature, are subject to whole system risks – often referred to as ‘systemic’ risks. Broadly, ‘systemic risk refers to the risk or probability of breakdowns in an entire system, as opposed to breakdowns in individual parts or components, and is evidenced by comovements (correlation) among all or most parts’ (Kaufman and Scott, 2003: 371). Systemic risk is often also used to refer to risk of failure of vitally important systems. For example, in a major report on systemic risk, the OECD refers to it as ‘one that affects the systems on which society depends - health, transport, environment, telecommunications etc’ (OECD, 2003: 30).

One reason for the concern about systemic risk is that it has become ever more prevalent and important in the modern world: there are significant ‘emerging systemic risks’ (OECD, 2003). Reasons are multiple (OECD, 2003: 30-31). They include firstly demographic trends with global population expected to rise by about 50%, particularly in urban areas in developing countries becoming increasingly dependent on modern systems. Secondly, environmental pressures and problems, notably related to global warming are expected to increase and to enhance the vulnerability of critical systems. Thirdly, technological changes are expected to continue apace leading to more and more complexity and interconnectedness of critical systems. Fourthly, socio-economic changes brought on by increased competition and economic growth, notably social and geographic inequalities in development, are likely to increase risks.

Increasing technological, social and economical interconnectedness brings with it many advantages but it is also accompanied by increasing vulnerabilities. More and more people become dependent on and affected by technological systems. Emergent systemic phenomena or ‘surprises’ are also likely. Analysis of the modern systems is often done on a component parts basis and systems are designed on the premise of bounded use and connection. However, their use evolves and becomes more integrated with other systems potentially leading the emergence of unforeseen systemic characteristics which might have negative consequences.

These trends of interconnectedness, interdependence and systemic risk have become inherent features of the network industries. A number of observations and questions about systemic risk in the network industries can be made. Firstly, there is a notable difference in the prominence of the concept of systemic risk in the academic literature (and practice) of banking and finance, where it is highly prominent, compared to the literature on risk in the network industries and ‘critical infrastructure’ risk where it is much less prominent. In the extensive academic and practitioner literature on risk in banking and finance, systemic risk is frequently and explicitly addressed and analysed and is one of the most important concepts in the sector (see e.g. Kaufman and Scott, 2003; Kambhu, Weidman et al., 2007; Milne, 2007). In contrast, while safety and reliability in the network industries and critical infrastructures is extensively analysed, systemic risk is only referenced briefly in the literature and not subject to extended and explicit analysis (IRGC, 2006; Zimmerman and Restrepo, 2006; Gheorghe, Masera et al., 2007). The associated term, ‘cascading’, is referred to more frequently but still not subject to intensive analysis.

A second observation of the network industries is that there are arguments and some evidence that these industries are increasingly vulnerable to systemic failures. Technological change can be disruptive to established steady states, ‘innovation trajectories ... can cascade in unforeseen ways’, particularly when technological systems rapidly expand into other systems and areas or life (Hellström, 2007: 417). The development of IT and the internet is a highly prominent example of this trend. Similar developments have occurred in other apparently more stable and established infrastructure industries such as electricity supply. It has been argued, for example, that electricity supply networks are becoming more integrated with the internet. This integration is occurring both ways: internet systems are used more and more for control and communications of the power transmission system while the latter is used as part of the communications system for the internet. Also due to liberalisation and internationalisation, particularly in Europe, they are being operated well outside their original design parameters (Gheorghe, 2006; IRGC, 2006; Kröger, 2008).

There have also been some significant systemic failures in the electricity supply system across Europe, for example, in 2003 transmission system fault in Switzerland led to a loss of supply across the whole of Italy for almost a day (Gheorghe et al, 2006). While it is not fully clear that there has been an increase in failures in Europe in the last decade or two, there is statistical data from the US and Canada which suggests a gradual increase in system failures since the 1980s (Zimmerman and Restrepo, 2006: 219-220).

These observations raise questions such as: why is there such a difference between the banking and the network industries in the prominence of the concept of systemic risk? Does it reflect big cross-sectoral differences in its significance? Or does it just reflect cross-disciplinary differences in terminology? Also how should complexity and systemic risk in the network industries, which has been especially compounded by market liberalisation, be managed and governed? Does it above all require more and better scientific and technical analysis to understand the risks and reduce uncertainty? Or does it require qualitatively different forms of governance that draw on many different types of knowledge, and involve a wider range of stakeholders? The latter might involve a shift from ‘risk management’ to ‘risk governance’ (Sajeva and Masera, 2006; Kröger, 2008) involving more deliberation and participation (Klinke and Renn, 2006).

2. What is systemic risk?

Before considering systemic risk in relation to the network industries it is useful to consider what the concept of systemic risk refers to. The concept of risk itself is not easy to delineate and in modern usage is closely associated with the notion of hazard. While the latter is the capacity or potential to do harm, risk is more to do with ‘possibilities, chances or likelihoods of events, often as consequences of some activity or policy’ (Taylor-Gooby and Zinn, 2006: 1). Nevertheless in most risk analysis and debate risk is associated with harmful outcomes and is thought of as the likelihood of a harm occurring combined in some way with the extent of the harm. Risk therefore involves two elements: (i) the likelihood or probability of a particular event occurring and (ii) the extent of the harmful consequences of the event.

A standard technical definition involves quantification and is the statistical probability of the occurrence of the unwanted event multiplied by its severity (Hansson, 2007). However, there are

extended debates on risk and uncertainty in the literature, particularly between a scientific view which sees risk as a statistical probability of harm and uncertainty when probabilities cannot be quantified and a social science view which sees risk and uncertainty in most practical situations as difficult to separate and is sceptical about the quantification of outcome probabilities.¹

As noted above, the concept of systemic risk refers to breakdowns of whole systems rather than their component parts. Systemic risk therefore appears to be distinguishable from other kinds of risk primarily in terms of the widespread and potentially damaging consequences. Nevertheless, definitions of systemic risk often focus on the cause of the harm, processes involved and the uncertainties in assessing the likely outcomes.

Systemic risk in banking: macro and micro causes

The literature on systemic risk in banking and finance is extensive and is an obvious starting point when considering the nature of systemic risk. The nature of systemic risk can be distinguished by focusing on the cause of harm. Kaufman and Scott distinguish between macro and micro causes (summary in table 1) (Kaufman and Scott, 2003). A macro systemic risk is a ‘a big shock or macro-shock that produces nearly simultaneous, large, adverse effects on most or all of the domestic economy or system’ (Kaufman and Scott, 2003: 372). There is a single (and often sudden) common cause that affects all or most parts of the system directly.

A micro systemic risk is when the initial cause or shock is only on one component of the system. The systemic risk is caused by the ‘transmission of the shock and potential spillover from one unit to others’. The transmission of the shock can occur directly or indirectly. In direct causation ‘systemic risk is the risk of a chain reaction of falling interconnected dominos’ and implies direct physical causation between the interconnected elements.

Indirect causations are ‘when one unit experiences adverse effects from a shock ... uncertainty is created about the values of other units potentially also subject to the adverse effects from the same shock’. Causation is thus connected to human perceptions and understandings, which are limited and uncertain, and human interactions with elements of the system, possibly exaggerated with risk averse responses, and herding behaviour and contagion. Human responses in the chain of events can therefore be self-reinforcing and systemic harm becomes a ‘self-fulfilling-prophecy’ (Kambhu, Weidman et al., 2007: 5).

Table 1. Types of systemic risk (Kaufman and Scott, 2003)

Macro	A single big shock which impacts on all or most of the parts of a system – a common cause
Micro (i) direct	A single shock which impacts on only one or a small number of system parts. The systemic effect is a result of a chain reaction between physically interconnected elements – a ‘domino effect’
Micro (ii) indirect	A single shock which impacts on only one or a small number of system parts. The systemic effect is a result of human interaction with other elements, in particular the result of loss of confidence and herding or contagious behaviour

These different categories of the causes of systemic risk relate closely to common understandings, particularly the notions of chain reaction and contagion, and provide a useful

¹ For more detail on these debate see Bartle (2008) and Bartle and Vass (2008).

starting point. Nevertheless it should be noted that there is no easy consensus amongst academics and practitioners on the nature and significance of systemic risks in banking (Kambhu, Weidman et al., 2007: 8).

While the concept of systemic risk has a high profile in banking and finance, it has been argued that the most common cause of banking failures is not systemic risk as commonly understood, ie chain reactions and contagion. 'The evidence indicates that problems at one bank or at a group of banks do spill over to other banks in general, but almost exclusively to banks with the same or similar portfolio-risk exposures and subject to the same shock (Kaufman and Scott, 2003: 376-377). In the US, 'clustered bank failures' are 'almost always triggered by adverse conditions in the regional and national macro-economies or by the bursting of asset price bubbles, especially in real estate' together with poorly performing or insolvent banks (Kaufman and Scott, 2003: 379). Healthy units are much less vulnerable to systemic shocks: 'at the height of the banking crisis and bank runs in Chicago in 1932, liquidity problems and depositor runs rarely, if ever, drove economically solvent independent banks into insolvency' (Kaufman and Scott, 2003: 379).

Systemic risk in banking therefore appears to be less chain reaction and contagion than often thought to be, and more a result of common cause external circumstances. It also raises a question about systemic risk. Is it a systemic risk when the chain reaction or spillover is just a trigger for the failure of unhealthy units? Or is systemic risk something more – when the trigger from the chain reaction is sufficient shock in itself to cause the failure of healthy units?

Complexity and systemic change

Moving beyond causation towards process, there are some other important distinguishing features of systemic risk associated with the inherent complexity of systems. 'Complexity' is a widely used term to describe the difficulties of analysing large systems with many components. Complexity is more than just 'complicated' (Sajeve and Masera, 2006: 381); it is qualitatively more than the difficulty involved in analysing systems with many sub components with complicated behavioural functions. It refers to systems which have features which make the prediction of system behaviour extremely difficult even if the properties of the component parts are well understood.

The features of complexity include 'nonlinearities, multiple stable states, hysteresis, contagion, and synchrony' which 'are features common to all complex adaptive systems' (Kambhu, Weidman et al., 2007: 6). Complex systems also manifest the characteristics of 'chaos', one reading of which is high sensitivity to initial conditions meaning outcomes can be practically impossible to predict. Abrupt regime shifts can occur which in the economy, for example, can lead to a 'transition to an inferior but stable equilibrium' (Kambhu, Weidman et al., 2007: 2).

Complexity has become a significant feature of the whole modern science and technological infrastructures. Science and technological developments progress in an incremental manner and not in a systemic or holistic way. Products and processes are added incrementally to a complex whole of science, technology, life, environment, society, politics and the economy. However, as is well known in systems analysis, there can be unexpected and unforeseen 'emergent' phenomena:

Created for specific functions and without cognisance of the networked interconnectivity of life, technological products enter the living world as 'foreign bodies'. Once inserted

into the ecology of life, they begin to interact with their networked environments and from that point onwards scientists and engineers have inescapably lost control over the effects of their creations (Adam and Loon, 2000: 6).

Undoubtedly many risks and hazards have been reduced by science and technology, however, the important argument is that new qualitatively different systemic risks have arisen out of technological change.

Perhaps most importantly, systems with a high degree of complexity apparently cannot be understood fully by scientific methods which means uncertainty becomes a distinctive feature. Uncertainty 'reduces the strength of confidence in the estimated cause and effect chain' (Klinke and Renn, 2006: 3). Systemic risk therefore appears to be replete with uncertainty; it appears to limit the effectiveness of statistical probabilistic analytical techniques and raises questions about how risk should be managed. It has been noted that 'many quantitative risk management approaches rely too heavily on data from relatively benign periods and thus allow history to grant a false sense of security' (Kambhu, Weidman et al., 2007: 18).

3. Is systemic risk in the network industries important?

Systemic risk is clearly a high profile issue in finance and banking and its frequent media reference in the current financial crisis indicates it is much more than an arcane theoretical concept.² However, is systemic risk in the network industries, a special category of risk which warrants special attention? One way of addressing this question is to consider what is problematic about systemic risk in general, though with particular reference to banking and the network industries.

One important feature of systemic risk as noted above is that there is a high level of uncertainty in risk due to complexity, interconnectedness and interdependence. It is not only difficult to know precisely what the risks are, but in ever more complex systems it can be difficult to know what the potential hazards are. There is therefore an unknown vulnerability to potentially high and possibly catastrophic hazards.

Perhaps the most obvious feature of systemic risk is the potential magnitude of economic damage and its geographic extent; they are wide ranging in scope and scale and transcend national borders (Klinke and Renn, 2006). The implication therefore is that other forms of risk are less in scope, bounded and contained. The speed of transmission of shocks is another inherent feature of systemic risk which can make it very difficult to respond in a focused way on the component parts affected (Kaufman and Scott, 2003: 375).

Is systemic risk important in the network industries? What is clear that systemic risk is an explicit and central concept within much of the literature and practice on finance and banking.³ This contrasts with systemic risk in the critical infrastructure literature, particularly that associated

² For example, 'Now is the witching hour when we find out if we are in for systemic meltdown', The Guardian, October 13, p28.

³ See for example, CRMPG III, 2008, Bühler and Prokopczuk, 2007, Elsinger, Lehar et al., 2006.

with the network industries.⁴ In the network industries literature the concept ‘systemic risk’ is only used occasionally and often only in passing.

One reason may be that many important risks and hazards in critical infrastructures do not appear to be systemic, eg train, plane and car crashes. Indeed in a special issue of the *Journal of Risk Research* on risk in critical infrastructures, one paper covered, airport risks, air travel risks, road safety, the transport of hazardous wastes and safety of a high speed train (Vrijling, van Gelder et al., 2004). Another paper considered the reliability of hydraulic structures for the seawall protection against flooding in the east coast of England and cliff stabilisation in the Isle of Wight (Schoustra, Mockett et al., 2004). It is possible to think of systemic consequences of some of these risks, e.g. an air crash causing widespread disruption to international flights, or the flooding of large areas (e.g. in the Netherlands) which impacts on other infrastructures. Nevertheless, these papers do not address the issue of systemic risk and the kinds of risks addressed are normally considered to be localised and bounded, albeit with severe consequences.

However, infrastructures are ‘complex systems-of-systems’ thus subject to systemic risks and failures (Sajeva and Masera, 2006: 381). One analysis of critical infrastructure risk focuses both on the severe consequences of failures of critical infrastructure and on the systemic aspects (Hellström, 2007). Drawing on the US national strategy for critical infrastructure, Hellström, notes a ‘clear understanding of critical infrastructures as grounded in “critical nodes”, “cascading effects” or multiplier effects, and the possibilities of “acting at a distance” which the interlinked nature of such systems offer’ (Hellström, 2007: 419). The ‘criticality’ of critical infrastructures is ‘not because they are important in general, but because they are strategically connected in such a way that they focus society’s total vulnerability to a few particular points in the system’ (Hellström, 2007: 427). This is indicative both of a general systemic quality, i.e. shocks or failures to component parts can have systemic effects but also that some component parts are much more significant and vulnerable than others.

One infrastructure industry in which risks do appear to have a systemic component is electricity supply, although the concept of systemic risk is not as central and explicit as in finance and banking. Terms such as ‘cascading’ and ‘chain reaction’ are used more often and much of the description of infrastructure risks in the network industries appears to have at least some systemic component. In arguing for the need for ‘international risk governance’ (Gheorghe, 2006; Gheorghe, Masera et al., 2007) focus on electricity supply and particularly the systemic risks that arise from the interconnected European electricity supply infrastructure.⁵ They note that although the system is decentralised, i.e. it derives from the interconnection of national systems, ‘disturbances can propagate all through it’ (Gheorghe, Masera et al., 2007, p9). However, although the term ‘systemic’ is occasionally used (Gheorghe, 2006, pxix), it is not systematic or explicit. The term ‘cascading’ is explicitly used to describe potential failures in electricity supply when one disruption can cause a second and so on (Zimmerman and Restrepo, 2006: 218) but they eschew the word ‘systemic’. For instance the SFOE (2003) report on the September 2003 blackout in Italy makes no reference to the systemic nature of the incident. Instead, it uses several

⁴ See for example, *Journal of Risk Research* (7:6, September, 2004) Special Issue on Risk and vulnerability of critical infrastructures in which systemic risks are not considered.

⁵ Arguments for international risk governance in electricity supply are also made in Kröger, 2008, IRGC, 2006, Sajeva and Masera 2006.

times the concept of cascade (cascade-style failure, cascading effect). Similarly, the UCTE (2006) report on the November 2006 pan-European disturbance refers many times to cascade tripping but not once to the systemic cause or effect.

Electricity supply might be much more vulnerable to systemic failures than other network industries such as water (IRGC, 2006: 17) the variety of ‘criticality’ within electricity and water supply after varying types of disturbance. While disruptions to electricity supply can have severe repercussions in other sectors such as water or transport, major disruptions to water are unlikely to have effects on other infrastructures.

Of the network industries in addition to electricity supply, information and communication technologies (ICT), particularly those associated with the internet, are seen as vulnerable to systemic risks. The threat of ‘cyber terrorism and computer virology’ is drawn on to describe the increasing systemic pressures in critical infrastructures (Hellström, 2007: 422). While many attacks on computer systems are aimed at individuals rather than infrastructure systems, attacks can have severe consequences on infrastructures and there are intentional ‘cascade-based attacks on important internet nodes’ (IRGC, 2006: 45). ICT and internet based systems are now highly integrated into the control of other major infrastructures such as electricity supply and transport and create another area of systemic vulnerability (IRGC, 2006: 28).

There are therefore clearly some important systemic risks in the network industries even if they are not frequently described as such. This raises the question, why is systemic risk a central concept in banking and finance but not in the network industries. One reason might simply be cross-disciplinary differences in terminology. Language such as ‘cascading’, is more frequently used in electricity supply than systemic and the latter is used with other terms such as ‘interdependency’, ‘interconnectedness’ and ‘propagation of disturbances’. However, even accounting for differences of terminology, the literature on systemic banking risk is much larger than similar literature in the network industries.

A second argument is that systemic risk (and similar terminology) is much more established in banking and finance and more widely recognised as a problem. The history of systemic risk in finance and banking goes back a long way: runs on banks were common in the 19th century and some important early regulation of banking (e.g. in the 1930s) was to reduce systemic risk. Complexity and interconnectedness in banking and finance have also increased apace since the liberalisation and rapid globalisation of the sector in the late 20th century. By contrast, in the 19th and early 20th century the network industries were either not developed (electricity) or in their infancy (telecommunications, railways). Electricity infrastructure developed in the mid 20th century, with some limited international interconnection developed since the 1950s, particularly in Europe. Digitalisation and computer based communication was in its infancy in the 1960s and 1970s and the internet and associated systems and technologies only become established in the 1990s. It appears there that it is only in recent years with the development of greater complexity and interconnectedness of network industries (systems of systems) that systemic risk (and complexity phenomena) have become more distinct.

There are other possible arguments based on differences between the sectors. Some aspects of finance are argued to be special and warrant special attention. For example, ‘financial market trading and post-trade processing have several distinctive features that distinguish them from

other network industries and make it difficult to directly apply standard analyses' (Milne, 2007: 2947). One of those features is that the network operates as both a one way and two way network. However, while there are undoubtedly special features of the sector, it is difficult to see this as a reason that systemic risk is especially important to this sector. There are many important network differences between network industries, such as ICT and electricity supply (in the former the network carries discrete and identifiable data packages while the latter network operates as a synchronized whole in which individual inputs and outputs cannot be identified once in the system), but this in itself does not mean that systemic risk is more important in one rather than the other.

Speed of transmission is noted above to be a feature of systemic risk, the speed is such that failures or disruptions in individual units cannot be dealt with quick enough to prevent propagation to other parts of the system. It has been noted, for example, that 'adverse shocks in the financial sector appear to be transmitted more rapidly than similar shocks in other sectors' (Kaufman and Scott, 2003: 375). However, this argument seems untenable. In electricity supply faults can cascade to whole systems within minutes, sometimes seconds (Schlöpfer and Glavitsch, 2006).

A more credible argument is that the damages and costs are much worse in banking and finance than the network industries; they can last longer and are more uncertain. Major disruptions to electricity supply can be very costly, for example, the major loss of supply in north east US and Canada in August 2003 affected about 50 million people and was estimated to have cost between 2 and 10 billion dollars (Kröger, 2008). However, the current financial crisis seems to be much more costly: many governments have paid out tens of billions and in some cases hundreds of billions to aid failing banks.

However, perhaps most distinct difference between banking and electricity is uncertainty of the effects. All of the major disruptions in electricity supply between 2003 and 2006 lasted less than a day, while financial costs were undoubtedly high, disruptions to normal life were limited to a few hours. This will cause a lot of disruption to some people, it may involve many millions in costs, but generally experience indicates that its effects will be relatively limited, certain and bounded. Clearly if loss of supplies became more frequent with more widespread effects then confidence and trust may fall and this could involve much bigger costs.

By contrast there is great uncertainty of effects crises in finance and banking in particular the extent to which they will impact on the real economy. The financial crisis of the early 1930s had a huge effect on the wider economy with a depression that lasted for most of the decade while the financial crises of 1987 and 1998 had a much smaller impact on the wider economy (Kambhu, Weidman et al., 2007: 12). The current crisis is clearly affecting millions of people and costing billions but there is huge uncertainty about how long it will last and how severe the effects will be. Will 'normal service' be resumed in a few months or a year or two, or are we entering a prolonged downturn and economic turmoil?

Is systemic risk important in the network industries? a comparison of the network industries with banking and finance

Issue	Banking and finance	Network industries
Use of the terminology 'systemic'	Systemic risk established as a central problem and analytical concept for many decades	Systemic risk not an established concept; it is only occasionally used - other terms such as 'cascading' or 'chain reaction' more frequently used
Are risks and hazards systemic?	Have been recognised for over a century (notably bank runs), though some dispute just how systemic the risks are	Many significant risks are not systemic, eg transport crashes, explosions at major industry facilities. But increasingly in the last two decades there are emerging significant systemic risks, particularly in electricity supply and ICT
Are there special features which make systemic risk especially important?	Some special features are claimed, eg speed of transmission, but difficult to see them as unique to the sector	There are some special features of electricity supply and ICT, notably their interconnectedness, which make them vulnerable to systemic risk
Are the consequences significant?	Consequences on the whole economy and society are potentially very high. High level of uncertainty about the effects	Consequences are potentially high, but the effects are normally bounded and constrained and more certain than in finance and banking

4. Systemic risk: a comparison of banking and electricity.

Table 1 compares systemic risk in the banking and electricity sectors. Whereas systemic risks are well-documented in the banking sector (Kaufman and Scott, 2003), this is less the case for network industries in general. In the electricity sector, there is an abundant technical literature on blackouts (Andersson, Donalek et al., 2005; Ilic, Allen et al., 2005; Makarov, Reshetov et al., 2005; Pourbeik, Kundur et al., 2006) but, relatively little specifically devoted to the systemic nature of risk. While mentioned, the concept of systemic risk is seldom unpacked. For example, most of the existing work on critical infrastructure deals with the concept of risk through “shaping factors”. Such factors include societal (public risk acceptance and awareness, urbanization, demography), system-related (degree of complexity, interconnectedness), technological (technology-related or infrastructure-related), natural (availability of resources, natural conditions) and institutional (market organization, government policy-making, legislation, regulation) factors (IRGC, 2006; Kröger, 2008).

In less than 20 years, cross-border flows have increased from less than 100TWh to more than 320 TWh in Europe alone. One can not conclude that higher levels of electricity exchange and increased demand automatically leads to increased risk/failure. For example, in the United States, the total number of operating reliability events has decreased 33% from 2002 to 2006⁶. However, the number of high severity Category-4 events went up in 2005 and 2007⁷. It appears that “large disturbances often stem from a sequence of interrelated events that would otherwise be manageable if they appeared alone. The cascading often results from equipment failure or poor coordination. Thus, the improvement of existing substations and other equipment through refurbishing, constant inspection, and maintenance, and replacement of critical components is vital to the prevention of cascading events” (Andersson, Donalek et al., 2005).

In addition, increased competition and open access to the transmission systems present new challenges to the reliable operation of the interconnected electric systems. As noted by (Kröger, 2008), the increase of systemic risk is compounded by the development towards a highly integrated system of interdependent systems. That said, (Kendall, 2001) explored the possible relationship between electric power outages and market de-regulation and concluded that, at the time, deregulation itself had not resulted in a lasting increase in the incidence of power outages in the UK and United States⁸.

⁶ Of the 29 events in 2006, 15 (52%) occurred due to equipment failures, while system protection mis-operations accounted for 31% and human errors accounted for 14%.

⁷ **Category 4:** An event results in any or combination of the following actions: a) system separation or islanding of more than 1,000 MW of load b) the loss of load (1,000 to 9,999 MW) ; **Category 5:** An event results in any or combination of the following actions: a) the occurrence of an uncontrolled or cascading blackout, b) the loss of load (10,000 MW or more)

⁸ Electricity transmission is not dependent on a single route, so failure due to a single component problem is reduced. However, an inherent risk of interconnected networks is the ‘domino effect’ – that is a system failure in one part of the network can quickly spread. Therefore, the active network needs appropriate design standards, fast-acting protection mechanisms and automatic reconfiguration equipment to address potentially higher fault levels.

Table 1: Cross-sectoral comparison of systemic risks

	Banking crisis	Electricity crisis
Triggering (crisis) event	Insolvency, runs	Natural event (lightening, strike) or device failure (loss of nuclear unit, tripping of a major tie-line, voltage collapse, protection system failure ⁽¹⁾ , relay system mis-operation), inadequate right-of-way maintenance
Sector vulnerability ⁽²⁾	Low cash to assets, low capital, high demand	Growth in demand, rise in cross-border trade, inadequate reinforcement of the power grid, poor coordination among neighbouring transmission system operators (TSOs) ⁽³⁾ , frequency and voltage collapse, hidden failures ⁽⁴⁾ , lack of investment in transmission infrastructure (within and between countries), failure to provide sufficient backup reserves
Potential dangers	Clustering of bank runs, credit availability, money supply efficiency, increased uncertainty, spillover beyond banks	Integration of smaller systems into larger systems (facilitated by modern ICT thereby increasing complexity and enabling trans-boundary propagation of disturbances); growing system oscillations; spillover to other network industries; uncoordinated generation supply response
Type of SR	Big shock, direct causation contagion, common shock contagion	Big shock, direct causation contagion, common shock contagion
Transmission channels	Interconnectedness, similar markets, high leverage	Interconnectedness, similar system, high level of cross-border exchange
Requirements for contagious SR	Interdependence, opaqueness	Interdependence, coordination failure between operators
Recent changes in SR	Increased interconnection, technology advances	Increased interconnection, next-generation networks (remote access arrangements), operating at the limit, market liberalization (unbundling of network elements and price)
Historical evidence of contagious SR	Direct causation (little), common shock (yes)	Direct causation (yes), common shock (little)
Corrective policies	Private, public, rollback de-regulation	Private, public (domestic and international), Re-regulation

Source: Based on Kaufmann (2000) and adapted by authors. Note: (1) There are two major failure modes in protection system: “failure to operate” and “undesired tripping”. (2) The vulnerability of power systems has been traditionally considered mainly from the physical perspective; however attackers can provoke or amplify negative impacts of physical attacks to power systems by attacking information system or exploiting inappropriate decisions of (SOs). (3) In Europe, the TSOs are national entities subject to different regulatory regimes, ownership structures and operating conditions. Protective relays are involved in about 75% of major disturbances. (4) A hidden failure is defined to be a permanent defect that will cause a relay or a relay system to incorrectly and inappropriately remove a circuit element(s) as a direct consequence of another switching event.

Potential solutions

Power grids have traditionally been designed to withstand without resulting in cascading events transmission outage contingencies of the N-1 or N-2 kind.⁹ However, in actual operation, power grids are potentially vulnerable to cascading outages. Reliable operations therefore require a risk-based-approach to monitoring and managing the probability an impact of potential cascading outages (Lee, 2008). Andersson, Donalek et al. (2005) argue that the introduction of reliability standards and regulatory clarification towards system reliability would reduce the risk of blackouts in the future.

According to UCTE (2007) the risk and propagation of the disturbance can be limited by the creation of common emergency procedures by neighbouring transmission system operators (TSOs). For the most probable disturbed situations, remedial actions to bring the system back to the security limits have to be jointly coordinated, prepared, agreed and trained both at inter-TSO and at national level. One should not forget the relationship between grid reliability and investment. It is often indicated that trends in transmission investment in North America generally have not kept pace with the growth in electricity demand, which has led to stressing the transmission system and, in some cases, compromising electric reliability.

Governance

On governance, there is also the need to have an independent source of reliability performance information. For example, in the USA, NERC commenced operations as the Electric Reliability Organization (ERO) in 2007 (assuming the responsibilities for electric reliability from its predecessor, the North American Electric Reliability Council). Perhaps the most significant feature of the US institutional framework is that it depends entirely on self-regulation and peer review, without external enforcement powers. NERC develops both operating and planning guidance for the regional reliability councils. Operating policies flow down through standards to requirements and guides to system operators. Planning policies flow down through procedures, principles, and guides to system planners. NERC and the regional councils follow this process to establish and maintain adherence to the planning and operational guidance. The Department of Energy (DOE) has limited but significant authority with regard to electric reliability.

Extending to other sectors

The electricity sector was chosen because of its high degree of interconnectedness - the centrality of electricity in infrastructure interdependence (Rinaldi, Peerenboom et al., 2001)¹⁰. But other network industries, by their *de facto* systemic nature, should also be taken into account. Such industries would include ICT, railways.

5. Systemic risk: the need for ‘risk governance’?

There are therefore some important aspects of risk in the network industries, particularly electricity supply and ICT, which have a systemic quality. There are clearly some important cross-sectoral differences in systemic risk between banking in which it is a central concept and the network industries in which it is less clearly central. Nevertheless some general aspects of systemic risk apply in all sectors: the widespread and severe impact,

⁹ N-1 criterion asks whether the system operating with N devices still operate after the loss of any single one of them. The assumption is that the system will move from the N component steady-state condition and settle into steady-state at the N-1 configuration.

¹⁰ There are numerous types of interdependencies, including physical, cyber, geographic and logical.

interdependence, complexity and uncertainty of outcome. The question arises, is there a need for any special forms of governance to address systemic risk?

Clearly the most fundamental aspect of systemic risk is its system nature and this suggests a the need for a system wide or centralised approach to governance. The two network industries of particular concern regarding systemic risk are electricity and ICT. Electricity has become internationalised on a continental basis (notably in Europe) while ICT has become globalised. Prima facie this suggests the need for centralised systemic risk governance at European level for electricity and global level for ICT. However, this centralised depiction of systemic risk does not fully capture its essence. As discussed above perhaps the most important systemic risks have micro causes, e.g. trees falling on power lines, which are then propagated through the whole system. This suggests that some aspects of systemic risk need to be managed on a decentralised basis. It particularly suggests that there needs to be a balance between centralised and decentralised governance depending on the type of risk.

The previous sections concluded that although there are some key features of systemic risk common to all sectors, there are some important cross-sectoral differences in detail. This suggests the necessity of alignment of institutions of governance with the technologies. In a comparison of the railway and electricity sectors in the context of the significant regulatory reforms of the past two decades it has been suggested that there needs to be a coherence between the ‘critical institutional arrangements that support the technical functioning of the systems’ (Künneke and Finger, 2007: 332).

From risk management to risk governance

In relation to the network industries the increasing difficulties associated with systemic risk have led some authors to suggest the need to move from ‘risk management’ towards ‘risk governance’ (Sajeva and Masera, 2006; Kröger, 2008; Gheorghe et al, 2007; IRGC, 2006). The complexity and interconnectedness of the network industries, particularly electricity, mean that established forms of risk management are insufficient. Conventional forms of risk management focus on the strategies and techniques adopted by one or a small number of similar and closely connected organisations. While they may be appropriate for bounded non-systemic risks, they are of limited effectiveness for systemic risks. Processes of risk governance are proposed which extend, though not wholly replace, risk management strategies where there are many and varied actors and institutions involved. ‘Risk governance admits the existence of multiple stakeholders, with their individual interests and viewpoints, in parallel with overall objectives (related to society as a whole).’ (Gheorghe et al, 2007, p16)

These ideas of risk management and governance imply different approaches to risk and appear to reflect two fundamentally differing approaches which pervade the literature on risk (Royal Society, 1983, 1992; Baldwin and Cave, 1999: 142-148; Bartle, 2008). They are deeply embedded to the extent that they are often referred to as ‘two cultures’ (Hood and Jones, 1996: 11; Kemshall, 2002: xi-xiii). These might be able to assist in conceptualising the kind sort of governance is appropriate for systemic risk in the network industries.

Scientific-technocratic and socio-political approaches to risk

One model can be labelled variously as ‘scientific-rationalist’, ‘realist-absolutist’, ‘modernist’ or ‘scientific-technocratic’. Risk is an objective concept, separate from subjective perceptions and is normally understood as the statistical probability of the occurrence of the unwanted event multiplied by its severity (Hansson, 2007). Risk can be understood and analysed by mathematical, scientific and technological analysis, particularly statistical probabilistic

techniques and reliability engineering. Uncertainty is a separate concept from risk and applies to situations when there is insufficient data to reliably and meaningfully quantify outcome probabilities. Rational responses to risk can be developed based on the level of risk that society deems to be tolerable and regulatory remedies proposed on the basis on economic cost-benefit analysis. Risk policy-making and regulation therefore is primarily a technocratic process led by experts.

A second model is variously labelled as ‘social-constructivist’, ‘relativist’, ‘political-democratic’, ‘post-modernist’ (Adam and van Loon, 2000, p8) or ‘socio-political’. Risk cannot be easily technically conceived and quantified. Risk merges with uncertainty and subjective perceptions of risk merge with the objective. In particular, there is scepticism about the idea that quantifiable risks can be identified. There can also be different understandings and interpretations of risk between different types of experts and between experts and non-experts. Leaving risk analysis to one body of experts is therefore insufficient and systems of risk governance and management have to be established to reflect this. Failures of risk management are often due to excessive faith in quantitative techniques and a futile aspiration towards more and more numerical accuracy at the cost of effective and more subtle understandings and analysis of the qualitative aspects of risk. Risk governance, regulation and management should therefore be a more democratic process with dialogue and input from a wide range of affected social and political actors.

While two models can aid analysis and understanding, it should be noted that understandings of risk and risk governance are more subtle than this. There are some commonalities between the approaches and many subtle differences within each. Analysts often strive to move beyond rather rigid bipolar oppositions towards a more complete analysis (Adam and van Loon, 2000, p8). Also some analysts identify more than two approaches to risk governance. For example, (Hermansson, 2005) distinguishes three models: a ‘standard model’ close to the ‘scientific-technocratic’ notion of risk, a ‘model of inviolable rights’ and a ‘model of procedural justice’.

Prima facie the best way of handling risk in highly complex industries understood only by small communities of experts such as the network industries and finance and banking appears to be the technocratic approach. However, this appears to be close to ‘the tradition methods of risk management (applied for instance by electric power companies) [which] do not suffice for coping with the new challenges faced by the electricity structure in its entirety’ (Gheorghe et al, 2007, p16). Despite this and despite the recognition of the increased uncertainties involved in complex systems, the approach of some analyses is predominantly scientific-technocratic. Two analyses of critical infrastructures such as energy and telecommunications (Zimmerman and Restrepo, 2006; Zio, 2007) both recognise the difficulties of scientific methods of risk analysis in the face of complex and interdependency: ‘the current quantitative methods of risk analysis seem not to be fully equipped to deal with the level of complexity inherent in such systems’ (Zio, 2007: 505). However, their approach to overcoming these problems is better scientific analysis, for example, with ‘better quantitative measures of the degree of interdependency and the cascading effects’ (Zimmerman and Restrepo, 2006: 228) or with ‘study of the topological properties of network systems [which] may give rise to new possibilities for exploring the vulnerabilities and the criticalities of critical infrastructures’ (Zio, 2007: 505). In essence, these approaches involve addressing the problem by more and better scientific analysis to understand systemic risk better, to reduce the uncertainties and better manage risk and uncertainty.

However, while attempts to gain greater understandings of systemic risk are necessary and welcome, it is not clear that they can overcome the problems of uncertainty due to complexity, interdependence and interconnectedness. While not denying the need to attempt to reduce uncertainty by scientific methods, it seems that decision making needs to go beyond this and incorporate processes which recognise that uncertainty is very likely to be always there.

This suggests the need for a more socio-political oriented approach to risk. In this vein Klinke and Renn (2006) argue that a 'deliberative approach' to risk management and decision making is required. A first level of deliberation is between different types of experts with a 'goal to achieve a homogenous and consistent definition and explanation of the phenomenon in question as well as a clarification of dissenting views'. A second level requires moving beyond scientific input with information about the uncertainties brought into a deliberative arena which includes a wide range of stakeholders and public interest groups. This is primarily to decide on the level of precaution in decision making.

Risk governance in the network industries

A number of analyses are moving towards a more socio-political approach, for example, those authors referred to above who suggest the need to move towards 'risk governance' from 'risk management' (IRGC, 2006; Sajeve and Masera, 2006; Gheorghe, Masera et al., 2007; Kröger, 2008). Another study suggests that complex infrastructure systems should be analysed as 'socio-technical systems' in which technical systems themselves are not only complex but also involve the 'variegated and penetrating involvement of human action, which, in all its forms, is able to affect, even critically to affect, the functioning of the system' (Ottens, Franssen et al., 2006). Understanding and interpreting systems thus requires analysis of the relations between human actors and organisations and physical elements and systems.

In relation to risk governance of critical infrastructures, Sajeve and Masera (2006, p391) suggest developing the principles of good governance recommended by the European Commission's 2001 white paper on governance. Principles include openness, participation, accountability, effectiveness and coherence. In relation to risk governance, openness, for example, means 'access to relevant information for the understanding of the risks ... organisations involved are able to communicate potential risks' and participation means 'active participation of experts, stakeholders, citizens and different viewpoints is crucial for a comprehensive consideration of the risk situations and the relevance of risk countermeasures'.

Some institutional and policy suggestions have also been made for risk governance in the network industries, notably the governance of risk in electricity supply (Kröger, 2008, IRGC, 2006). Institutional recommendations have been made in electricity at the European level to focus on risk and supply security. A modest suggestion is a 'modification of the mission statements for the current organisations in Europe (such as the Florence Forum)' (and possibly the EU regulatory networks which are to be institutionalised into the Agency for the Cooperation of Energy Regulators) and a more radical suggestion is the 'institution of a European Council for the Security of Electric Power' (Gheorghe et al, 2007, p18). Policy recommendations include inter alia strengthening the level of network security required in regulations, promoting technical research and analysis of infrastructure risks, promotion of best practices by all participants, and ensuring adequate dialogue with all key stakeholders in decision and rule making (IRGC, 2006, p54; Kröger, 2008, p1786).

However, while these are all useful and important suggestions, they suggest little in detail about the governance and institutional structures, nor do they focus explicitly on systemic risk and how it should be governed in the network industries. In particular, while more detail is indicated on technical methods, eg system analysis based on ‘an object-orientated, hybrid approach combining Monte Carlo and agent-based modelling techniques’ (Kröger, 2008, p1786), little detail is suggested on governance structures.

Many important questions about governance structures and the governance of systemic risk and uncertainty need to be addressed. It might involve more analysis of potential failure scenarios and more engagement with variety of stakeholders about the scenarios and the level of caution required in addressing the risks.

There are also difficult questions about the involvement of stakeholders. Given that systemic risk requires decentralised as well as centralised risk governance there are questions of vertical structure, ie which national, subnational, international stakeholders to involve and how. Horizontal questions of participation by stakeholders such as industrial users and individual consumers, trade unions, public interests such as environmental interests are also pertinent. As noted above, interconnectedness suggests at least more and closer working between TSOs in electricity supply. Interdependency and interconnectedness also means that participation might include a range of stakeholders from interconnected sectors, such as industry, technical experts, consumers and public interests.

In addition to questions about who is involved there are questions about how they are involved and what their place is in the process. ‘Dialogue’ is frequently referred to in the above references but is this enough to address the uncertainties associated with systemic risk governance? There are wide range of ways of involvement, from information transparency, close consultation to co-decision making.

Finally there are questions about how appropriate are current regulatory institutions in Europe such as the Florence forum, the regulatory networks and the new Agency for the Cooperation of Energy Regulators. A primary issue here is that these institutions developed specifically in response to the liberalised single European market in energy and particularly the need to manage new forms of competition across Europe. Is it appropriate for institutions which were developed primarily to manage competition to be modified to manage systemic risk? Or should systemic risk be managed entirely separately?

6. Conclusion

Systemic risks and hazards are becoming increasingly important features of modern industrial society of which the network industries form a vital and central element. Nevertheless a comparison of the literature indicates that the idea of systemic risk is much less prominent in the network industries compared to banking and finance. This could perhaps indicate that systemic risk is somehow less important in the network industries. We argue in this paper, however, that systemic risk is very important in the network industries and it needs to be a considered more explicitly than hitherto in the governance of risk in the network industries.

While comparison of banking and finance with the network industries reveals many differences, they are not enough to conclude that systemic risk is not important in the network industries. Two key reasons point to why systemic risk is much more high profile in banking than the network industries. First, it has a long and established history, at least a century and a

half in banking. Second, the potential consequences of systemic hazards are very high in banking and finance; they can affect the whole economy and society for many months and possibly years during which there is a high degree of uncertainty about their effects. While these features are clearly different to the network industries, this does not mean that systemic risk is not important in the latter. Systemic risk has only become significant in the past two decades in the network industries yet there are many uncertainties about just what the risks are. Although the consequences of systemic risks are likely to be much more bounded in the network industries than in banking, their consequences in terms of financial costs and disruptions to modern routines are likely to be very high and to be avoided as much as possible.

This paper has also highlighted a number of technical differences between banking and one of the key network industries, electricity supply. Again, however, while these differences can impact on risk governance strategies, they are insufficient to argue that systemic risk is not important in the network industries. Some of the differences in systemic risk are due to the emerging nature of risk in the network industries compared to the established risks in banking. Thus, the key sectoral vulnerabilities in electricity are the rise in cross border trade, integration of different systems and operation outside of their original design parameters have become much more significant in the last two decades while the key vulnerabilities in finance and banking such as low capital, have been important in the last two centuries of banking.

Systemic risk in the network industries is therefore very important and we argue that systemic risk and its governance need to be addressed more explicitly in the network industries. This is because of the potential severe and widespread consequences, the heightened uncertainty about the risks and potential for surprises, interdependence and interconnectedness, and the emerging nature of systemic risk in the network industries.

We also argue that traditional technocratic forms of risk management and governance are not sufficient, particularly due because of heightened uncertainty and interdependence. Undoubtedly more and better scientific and technical analysis of systemic risk is necessary and important. However, unless and until the problems of uncertainty are overcome, which seems highly unlikely, other means of governing risk and uncertainty are required. In particular, judgements by different experts and different stakeholders are required about the nature of the uncertainty, about the potential hazards and their consequences and about the level of caution required. This requires a more participative and open form of risk governance, a form which draws as much on socio-political forms of governance as technocratic.

This is recognised in part in the recent literature on risk governance of critical infrastructures but the literature says little about the participative governance structures which might be appropriate nor how they may be developed in practical terms in the patchwork that is the European regulatory environment for the network industries (Kröger, 2008; IRGC, 2006; Gheorghe et al, 2007; Sajeve and Masera, 2006). The patchwork, which includes the Florence forum and the new Agency for the Cooperation of Energy Regulators, has been developed primarily to manage competition across Europe. It is however not clear that they would be appropriate for the management of systemic risk.

There are some particularly difficult questions about the involvement of stakeholders. Systemic risk requires decentralised as well as centralised risk governance so there are questions about the involvement of national, subnational, international stakeholders. There are

also questions of participation by stakeholders such as industrial users and individual consumers, trade unions and public interests. Participation might also include a range of stakeholders from interconnected sectors, such as industry, technical experts, consumers and public interests. In addition to questions about who is involved there are questions about how they are involved and what their place is in the process. There are wide range of ways of involvement, from information transparency, close consultation to co-decision making.

This all suggests a research agenda focused on the following questions:

- how is systemic risk currently governed at national and European levels in the network industries, particularly in relation to technocratic and socio-political forms of management and governance?
- what are the strengths and weaknesses of current systemic risk governance and how might it be improved?
- what might governance institutions, structures and processes look like at national and international levels in the context of emerging systemic risks in particular their cross-national and cross-sectoral nature? How should uncertainty be addressed? In particular which stakeholders should be involved in systemic risk governance?
- what sort of involvement should the various stakeholders have? Should it only be a limited form of information and dialogue, or should there be close consultation and co-decision making amongst wide ranging stakeholders?
- To what extent are existing institutions, which have been set up mainly for competition and trade, suitable and adaptable for the regulation of systemic risk, or should entirely separate institutions of risk governance be established?

Bibliography

- Adam, B. and Loon, J. v. (2000) 'Introduction: Repositioning Risk; the Challenge for Social Theory', in U. Beck, J. v. Loon and B. Adam (eds), *The risk society and beyond: critical issues for social theory*. London: Sage.
- Andersson, G., Donalek, P., et al. (2005) 'Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance', *Power Systems, IEEE Transactions on*, 20 (4): 1922-1928.
- Baldwin, R. and Cave, M. (1999) *Understanding regulation: theory, strategy, and practice*. Oxford ; New York: Oxford University Press.
- Bartle, I. (2008) *Risk-based regulation and better regulation in the UK: towards what model of risk regulation?* Paper presented at the 2nd Biennial Conference of the ECPR Standing Group on Regulatory Governance. Utrecht University, the Netherlands.
- '(Re)Regulation in the Wake of Neoliberalism. Consequences of Three Decades of Privatization and Market Liberalization', June 5th -7th, 2008.
- Bartle, I. and Vass, P. (2008) *Risk and the regulatory state - a better regulation perspective*. Bath: Centre for the study of regulated industries, School of Management, University of Bath. CRI Research Report 20.
- Bühler, W. and Prokopczuk, M. (2007) *Systemic Risk: Is the Banking Sector Special?* Universität Mannheim.
- CRMPG III (2008) *Containing Systemic Risk: The Road to Reform*. The report of CRMPG III, CRM Policy Group, August.
- Elsinger, H., Lehar, A., et al. (2006) 'Risk Assessment for Banking Systems', *Management Science*, 52 (9): 1301-1314.

- Gheorghe, A. V. (2006) *Critical infrastructures at risk: securing the European electric power system*. Dordrecht: Springer.
- Gheorghe, A. V., Masera, M., et al. (2007) 'Critical infrastructures: the need for international risk governance', *International Journal of Critical Infrastructures*, 3 (1/2): 3-19.
- Hansson, S. O. (2007) 'Risk', available at Stanford Encyclopaedia of Philosophy <http://plato.stanford.edu/entries/risk/>.
- Hellström, T. (2007) 'Critical infrastructure and systemic vulnerability: Towards a planning framework', *Safety Science*, 45 (3): 415-430.
- Hermansson, H. (2005) 'Consistent Risk Management: Three Models Outlined', *Journal of Risk Research*, 8 (7-8): 557-568.
- Hood, C. and Jones, D. K. C. (1996) *Accident and design : contemporary debates in risk management*. London ; Bristol, Pa.: UCL Press.
- Ilic, M. D., Allen, H., et al. (2005) 'Preventing Future Blackouts by Means of Enhanced Electric Power Systems Control: From Complexity to Order', *Proceedings of the IEEE*, 93 (11): 1920-1941.
- IRGC (2006) *Managing and reducing social vulnerabilities - From coupled critical infrastructures*. Geneva: International Risk Governance Council. White paper no. 3.
- Kambhu, J., Weidman, S., et al. (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 ; John Kambhu, Scott Weidman, and Neel Krishnan, rapporteurs*. Washington, D.C.: National Academies Press.
- Kaufman, G. G. (2000) 'Banking and Currency Crises and Systemic Risk: A Taxonomy and Review', *Financial Markets, Institutions & Instruments*, 9 (2): 69-131.
- Kaufman, G. G. and Scott, K. E. (2003) 'What Is Systemic Risk, and Do Bank Regulators Retard or Contribute to It?', *The Independent Review*, VII (3): 371- 391.
- Kemshall, H. (2002) *Risk, social policy and welfare*. Buckingham: Open University Press.
- Kendall, G. (2001) 'Power outages during market deregulation', *Control Systems Magazine, IEEE*, 21 (6): 33-39.
- Klinke, A. and Renn, O. (2006) 'Systemic Risks as Challenge for Policy Making in Risk Governance', *Forum: Qualitative Social Research*, 7 (1): 13.
- Kröger, W. (2008) 'Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools', *Reliability Engineering & System Safety*, 93 (12): 1781-1787.
- Künneke, R. and Finger, M. (2007) 'Technology Matters: The cases of the liberalization of electricity and railways', *Competition and Regulation in Network Industries*, 8 (3): 303-335.
- Lee, S. T. (2008) 'Probabilistic online risk assessment of non-cascading and cascading transmission outage contingencies', *European Transactions on Electrical Power*, 9999 (9999): n/a.
- Makarov, Y. V., Reshetov, V. I., et al. (2005) 'Blackout Prevention in the United States, Europe, and Russia', *Proceedings of the IEEE*, 93 (11): 1942-1955.
- Milne, A. (2007) 'The industrial organization of post-trade clearing and settlement', *Journal of Banking & Finance*, 31 (10): 2945-2961.
- OECD (2003) *Emerging systemic risks in the 21st century : an agenda for action*. Paris: OECD.
- Ottens, M., Franssen, M., et al. (2006) 'Modelling infrastructures as socio-technical systems', *International Journal of Critical Infrastructures*, 2 (2/3): 133-145.
- Pourbeik, P., Kundur, P. S., et al. (2006) 'The anatomy of a power grid blackout - Root causes and dynamics of recent major blackouts', *Power and Energy Magazine, IEEE*, 4 (5): 22-29.

- Rinaldi, S. M., Peerenboom, J. P., et al. (2001) *Identifying, understanding, and analyzing critical infrastructure interdependencies*. Control Systems Magazine, IEEE. 21: 11-25.
- Royal Society (1983) *Risk Assessment, Report of a Royal Society Study Group*. London: The Royal Society.
- Royal Society (1992) *Risk: Analysis, Perception and Management, Report of a Royal Society Study Group*. London: The Royal Society.
- Sajeva, M. and Masera, M. (2006) 'A strategic approach to risk governance of critical infrastructures', *International Journal of Critical Infrastructures*, 2 (4): 379-395.
- Schläpfer, M. and Glavitsch, H. (2006) 'Learning from the part - electric power blackouts and near misses in Europe (appendix 1)', in A. V. Gheorghe (ed.), *Critical infrastructures at risk : securing the European electric power system*. Dordrecht: Springer. pp. 163-194.
- Schoustra, F., Mockett, I., et al. (2004) 'A new risk-based design approach for hydraulic engineering', *Journal of Risk Research*, 7: 581-597.
- SFOE (2003) *Report on the blackout in Italy on 28 September 2003*. Ittigen: Swiss Federal Office of Energy.
- Taylor-Gooby, P. and Zinn, J. (2006) *Risk in social science*. Oxford ; New York: Oxford University Press.
- UCTE (2006) *System Disturbance on 4 November 2006*. Union for the Co-ordination of Transmission of Electricity.
- UCTE (2007) *Emergency Procedures*. UCTE. V1.0/03.05.06 Final version
- Vrijling, J. K., van Gelder, P. H. A. J. M., et al. (2004) 'A framework for risk criteria for critical infrastructures: fundamentals and case studies in the Netherlands', *Journal of Risk Research*, 7 (6): 569-579.
- Zimmerman, R. and Restrepo, C. E. (2006) 'The next step: quantifying infrastructure interdependencies to improve security', *International Journal of Critical Infrastructures*, 2 (2/3): 215-230.
- Zio, E. (2007) 'From complexity science to reliability efficiency: a new way of looking at complex network systems and critical infrastructures', *International Journal of Critical Infrastructures*, 3 (3/4): 488-508.