Two Kinds of Risk: Enacting Markets and Security in Neighbouring Electricity Control Rooms*

June 3, 2011

Antti Silvast

University of Helsinki, Department of Social Research

7133 words

1 Introduction

Electricity supply is commonly viewed as one of society's vital or critical infrastructures (Brunner & Suter 2008; EU 2008). In most European countries, it is also a relatively stable infrastructure (Council of European Energy Regulators 2008, 33-34). Failures of electricity supply do happen in Western countries, however, as demonstrated by several long-term losses of electric power in Europe and other countries. Latest example is Japan's recent string of disasters, which have led into major and continuing problems with the provision of electricity in the country (BBC 15 March 2011; Reuters 27 April 2011).

Similar crises with Western electricity supply have been relatively rare. Nonetheless, the possibility of electricity blackouts is often regarded as problematic and in need of intervention by economic, scientific, and political actors. Experts on emergencies, crises, and civil contingencies view the protection of electricity supply infrastructures as a national security problem (Brunner & Suter 2008; EU 2008; Höst et al 2010; see Collier & Lakoff 2008). The official regulation of free energy

*Paper for *The Finnish Post-Graduate School in Science, Technology and Innovation Studies summer school,* 6-7 June 2011, Helsinki, Finland. Pre-publication draft. Please do not quote without the author's permission. Correspondence: antti.silvast@helsinki.fi.

markets is increasingly justified by the perceived need for improving electricity supply quality (e.g. Council of European Energy Regulators 2008, 2005). Workable energy market competition can, in its turn, also be framed as a matter of achieving improved quality and security (e.g. EU 2009, 2003).

More theoretically, it could be said that there is increasing preoccupation with *risks* in electricity supply. Corresponding with what various social scientists regard as risk (e.g. Helén 2004; Luhmann 1993), a heightened worry over the potential of electricity infrastructure failures has emerged. Methods for analysing this potential as risk are explored and developed. Threats to the infrastructure are hence quantified and made less complex. Eventually, countermeasures for threats are informed and motivated (e.g. EU 2008, Annex II). Some recent examples of electricity-related risk control measures include financial electricity quality incentives (Council of European Energy Regulators 2008, 2005), the formal identification of national and European "critical infrastructures" (EU 2008), infrastructure risk and vulnerability analyses (Höst et al 2010), and the development of management and planning for emergencies in organizations (Höst et al 2010).

The instruments of risk analysis are hence being applied to electricity supply. At the same time, less research has been attracted to the notion and practices of risk of infrastructures or to the rationales that undercut the provision of secure infrastructures through risk techniques (but see Collier & Lakoff 2008). As researchers of risk have argued for several years, however, the notion, practices and rationalities of risk are a rich and varied research topic. Exploring risk from the perspective has major implications particularly because the whole topic is so ambiguous. Risk is now often seen as something unpleasant (e.g. "risk of injury"), but it also means a possibility (e.g. "taking a risk") (Furedi 2006). Professionals such as actuarians, insurance experts, and medical doctors draw on markedly different rationalities, knowledge, and practices of risk (O'Malley 2004). The political philosophies and practices of risk alter over time: for example, the risks viewed by 19th century industrial capitalists are not altogether same as the risks viewed by the 20th century welfare state (Beck 1992/1986; Ewald 1993/1986; O'Malley 2004). Definitions and uses of risk also vary according to situational context (Helén 2004). Risk, in short, is a multiple object (see Mol 2003), which also makes it a problematic notion in need of detailed empirical analyses.

This paper addresses the gap between the topics of risk and electricity supply and security by asking the following question: *What are the notions and practices of risk in the management of electricity supply?* Drawing on research on the multiplicity of risk (Helén 2004; O'Malley 2004), my assumption is that there are various kinds of electricity supply risks. These kinds are given effect by different concerns, propositions, knowledge, practices, and institutions. Overall, the different kinds of risk *enact* different threats to electricity supply (Collier 2008; see also Mol 2003). Especially, I claim

that we are observing two kinds of risk in the current worries over electricity supply and security: *technical security risk* and *financial market risk*.

Technical security risk (e.g. Council of European Energy Regulators 2008, 2005; Höst et al 2010; EU 2008; Brunner & Suter 2008; see Collier & Lakoff 2008) emphasizes electricity network threats: such as hardware malfunctions, operator errors, weather phenomenon, and sabotage. Central actors that drive this risk rationale are security experts, civil contingency agencies, energy market regulators, military strategists, researchers, and standardisation bodies, and the rationale is given effect by laws, emergency protocols, crisis exercises, quality regulations, and safety standards. With *financial market risk* (e.g. Nord Pool 2009, 2011; Viljainen et al 2011; EU 2009; see Graham & Marvin 2001), the key concern is different: it is with workable competition, affordable prices, electricity transmission capacity, efficiency, and activation of energy consumers. Institutions that worry about these matters include lobby organisations, energy market researchers, and energy stock exchanges, and the production of market-type risk knowledge is driven by economic theories and financial techniques.

Hence, electricity supply risk is multiple. But that does not mean that we are observing two altogether different social worlds or "risk cultures" (Douglas & Wildavsky 1982; Adams 1995). Rather, my concern is with the intertwining of the different kinds of risk. How does market risk deal with and incorporate technical risk and vice versa? To which extent are the two kinds of risks incommensurate?

The empirical case of the paper is an electricity distribution company in a Finnish town. The case concerns technicians who operate the town's electricity grid in two control rooms, continuously monitoring the grid, and brokering energy on the common Nordic energy stock exchange Nord Pool. Such case was deemed as relevant for measuring the local and situated implications of technical risks and market risks. Quite much is already known about the national and global policy processes of infrastructure privatisation, deregulation, and liberalisation, and the corresponding problematizations of universal infrastructure provision (Graham & Marvin 2001). At the same time, less has been said about the varied and complex manners in which these transitions and their rationalities of risk take effect in the constant efforts of managing infrastructures (but see Roe & Schulman 2008, 114-115). How do technical risks and financial risks figure in the actions of providing electricity? In this paper, the question was assessed by spending time in an electricity company, talking to its workers and observing their working practices in two control rooms where electricity supply is managed (see also Roe & Schulman 2008; Steenhuisen 2009; De Bruijne & Van Eeten 2007).

The structure of the paper is as follows. The following two sections address the working practices and sense makings in the electricity company, and discuss these topics in relationship to the rationalities and various intellectual technologies of risk. The fourth section concludes by returning to the research questions, and producing tentative answers to them.

2 The market control room and free market arrangements

The case of this paper concerns two control rooms in an electricity supply company of a Finnish town. These rooms are responsible for the continuous real-time management and control of the electricity grid and energy production on the town's region. As for their names, it is not that simple to decide what to call these rooms: previous studies (Roe & Schulman 2008) suggest calling the first of them energy market control room, while some Finnish electricity supply scientist-experts call it the energy market surveillance. The other room would be correspondingly called the electricity distribution control room or the electricity distribution surveillance.

Neither term, however, captures very well the work of the market side room. Rather than survey or control the markets, the basic responsibility of the workers is to seek to balance energy supply with energy demand. To this end the workers are continuously buying and selling on the Nordic common energy markets, as well as producing electricity locally. Particularly interesting in the light of my interest in risk practices is the central technique that is applied to reach the aims of the work: the energy market *contract*.

A contract is a voluntary agreement between free and rational actors (in practice, commonly presumed to be free males, see O'Malley 2004, 34). According to risk researcher Pat O'Malley (2004), the contract is given shape and justified by a particular political philosophy: *classical liberalism*. Made popular in the 19th century, this political philosophy stresses markets, and the responsibility of individuals (and companies) to anticipate future events by submitting to the "yoke of foresight" (O'Malley 2004, 32). Contractual decisions, it is viewed in classical liberalism, lead to the "best" outcome for all as they safeguard free market competition and the utilization of uncertainty; state interventions, in contrast, are only justified when they are needed to ensure that markets are functioning. The future is thus kept uncertain, though it should be noted this applies only to an extent. Indeed, the contract is also a way of making the future more calculable and controllable: business contracts specify prices and quantities for a future date, and the contracting parties have to submit to these prices and quantities lest the contract becomes invalid (O'Malley 2004, 35). Errors in calculation or failures to calculate the future, and various types of accidents from working accidents

to industrial catastrophes are viewed as the fault of the individual actors according to this political philosophy. When people or companies can presumably anticipate events, it follows that they are also held responsible for the impacts of the events (O'Malley 2004, 36).

In the control room, two contractual techniques are in particular operated with during daily work: ElSpot contracts concern the delivering of energy for the day ahead, and ElBas contracts are made on an hour-ahead real-time market place. In effect, these contracts are made and refined all the time. Firstly, the workers try to predict the levels of energy consumption and production for the following day, and send an "order" to the Nordic stock exchange Nord Pool before 13:00. Nord Pool for its part aggregates all the "orders" of different market parties, and on this basis, calculates each hour's "system price" where supply and demand meet. The energy company then in turn contracts (via ElSpot) to buy or sell energy for this system price. By and large this prediction is often quite accurate; however, as the workers emphasised to me it is also never precise. So secondly, the workers keep continuously making new ElBas contracts on the real-time market to improve the balance between electricity supply and demand.

The workers also explained that the balancing of supply and demand is increasingly happening on the real-time market place ElBas. Rather than just make predictions for the day ahead (and draw upon several routine risk mitigation measures such as archival stocks of knowledge, weather predictions, practical hunches, and local interactions; see Silvast forthcoming 2011), it is increasingly the control room worker's task to stay alert to the markets and their fluctuations. But what about the topic of technical risk? What possible role could technical risk governance play in these actions and operations, other than the somewhat vague notion that workable global energy markets contribute to technical security of electricity supply (e.g. EU 2009)?

The question is not at all simple, and I will answer it in several parts. First of all, there is a marked discontinuity between technical risk and market competition: to an extent, technical risk does not figure in contractual governance. It is thus justified to claim that risk is an "externality" (Callon 1998) to energy market practices, though this, again, applies only to an extent. The market players contract for buying or selling electric energy, but they do not deliver it locally all the way to customer; instead, as energy experts well know, it is another "unbundled" (Graham & Marvin 2001, 141-142) operator that takes care of the technical electricity supply and its risks. In one of its communications, Nord Pool (2009, 3) states that security of electricity supply should not even be relevant for operating on the markets:

> The commercial players (of energy markets) are not and cannot be responsible for the security of supply. If a South Swedish retailer, for example, has bought electricity from a North Swedish producer, the North Swedish producer cannot guarantee that there will be electricity in the plug at the retailer's customers. What the commercial players deliver to each other and the end users are only the prices (and the bills). Hence, the commercial players deliver financial services only.

Also in the company of my case, the technical functions are handled by another control room, the so-called electricity distribution surveillance or electricity distribution control room (see next section).

The management of risk is therefore separated and diffused into different social worlds and their practices. An example is the maintenance of an electricity blackout, a failure to provide electricity to the customer which in Finland often stems from weather conditions (e.g. storms, wind, or snow on pylons; other common reasons for them are failing power plants, human errors, and technical network malfunctions). Though both irritating and risky to the electricity end customers, as a strictly economic problem blackout is not a security threat. It is only a matter that the company now has too much energy which needs to be sold on the energy markets.

It should be emphasised that the neglect for electricity blackouts is not some sort of crass commercialism, but a more basic legal and technical issue: in any moment, energy supply can neither be too little nor too much in relation to the demand of energy, or otherwise the customer's electric appliances will not work. The market control room workers might of course be worried about the broader consequences of electricity blackouts; but as far as their work is considered, it does not concern solving the blackout as a technical breakdown, but finding the correct level of generation.

All of the above seemed to be reflected in the way that the market room workers talked about their work in terms of risks and security. A younger female operator in particular was not prone to talk about "things that do not belong to the work here" (Mf1[1]). This reaction was especially produced when I mentioned the concept of security. Another, more experienced operator highlighted a similar disposition during a conversation. I asked what happens in the scenario of a power plant failing in the grid, something which I proposed to be "an exceptional situation". The operator first argues how he does not think this situation to be exceptional, and then responds after a considerable pause:

[1]These codes refer to the informant. The first letter is the control room (M=market room worker, D=distribution room worker, B=worker of both rooms). Next is the gender (f, m). The number in the end is an indicator starting from 1.

> Mm1: There is nothing else to it. District heating has so many additional heat plants. The only thing is that money gets burned.
>
> AS: So it is just costs then?
>
> Mm1: Yes, there is not, there is no security risk. Except if a boiler explodes, then for the boiler men. But there is nothing else. If some plant is dropped out of production, one assembles the energy and heat from elsewhere.

In this case, the "crisis" – a notion that the worker does not agree on – thus gets only measured in money. The workers accordingly operate in an economic frame, and other things such as security risks simply are not taken into account when making energy market transactions. The recent European efforts where electricity utilities are submitted to customer compensations for blackouts are rather direct reflection of this: it is seen as problematic by regulators that utilities do not think about blackouts as a financial problem, hence the utilities are enforced to do so by adding new incentive mechanisms such as the returning a share of the customer's electricity bill if a blackout has lasted more than 12 hours (CEER 2005). Overflows are channelled, externatilities are internalized (see also Callon 1998).

Yet as interesting as the views by the workers are, it is also possible to disagree with them. In many ways, technical risk and security are inherent to the operations on the energy market even if this is not apparent when operating in a strictly economic frame. First of all, as has already been mentioned a contract is not a technique that concerns just money and not security: indeed it increases security by making the future more calculable, while at the same time also leaving space (or "uncertainty") for economic profits to be made. A contract is also a way of making market players accountable for risks: it is made explicit by a contract that these actors bear the consequences if they have made a bad estimate of the market situation. Also determining the offer to the day-ahead markets relies on many methods of planning ahead or "technologies of risk" (Silvast forthcoming 2011): such as data archives, weather predictions, and experiential hunches by the workers. Finally, one can also see the rationale of risk governance behind the increasing importance of the real-time market place: as Nord Pool (2011) wishes, the companies can try to manage the risk of energy imbalance more dynamically on the real-time markets than on the day-ahead markets. It would thus seem that technical risk is all over the work, but it somehow disappears to the people who are managing it. How far does this extend? Is it true as one of the workers claimed in above that even disasters and crises can only be measured in money?

To assess the last question, it should be noted that there are risky situations that are more directly related to the operations on the markets and, it might be said, even pose crises to these operations. These events are relatively rare, and I was not able to observe any; hence I asked the operators to imagine a more serious breakdown for their working routine. Even operators with very long experience could only remember one or two occasions when something serious had happened. One of them thought about a severely leaky pipe in the district heat networks which then results to one of the company‘s own power and heat generation plant shutting down. As the energy market exchanges have already been planned ahead and hence that plant had promised to generate energy which was also to be sold, this would also cause problems with the energy market brokering (Mm3).

Also, an opposite type of event can be imagined: the energy brokering on the markets causing problems with the technical supply of electricity to the end customers. From the early 2000s, an operator recalled what he called a “senseless event”: the so-called “Black Monday” of the Nordic energy stock exchanges.

> It was a situation that suddenly on Monday, when our spot market order came, the prices of that Monday were terrible. They were senseless, they were like the maximum prices that the energy stock exchange can have. We did not have enough electricity and then we had to buy it from the markets and it was terribly expensive. The guy who operated that day of course faced the worst. (Mm2.)

Thus, crises can happen, and the workers have to stay alert to them. The way that they are handled, however, reflects much more “business as usual” and the solving of practical problems than a raised awareness for disasters and crises (see Roe & Schulman 2008, 129-130). When imagining the aftermath of the above mentioned leaking water pipe, an operator explains to me:

> It could be that a power plant comes down. (...) Then we start to repair it and there we start the power plants in a way, and then the pack of the trading is all mixed up, but it gets built back step by step. If you start to build from scratch and you don‘t know exactly, what is the activation time of a power plant, then you simply have to guess what it is. (Mm3.)

When I ask in more detail, it turns out that this step by step recovery is also done in close practical coordination with other organisations.

AS: What kinds of means do you have to repair? Do you communicate with others?

Mm3: We are communicating with the district heat control room, asking what the situation is, so that we get information ourselves. The power plant does the conversation between these control rooms on what is to be expected.

AS: Is it very different then than normal working, when there is an exceptional situation?

Mm3: You have to be more in contact to get information, and they don‘t have the information either and then we try to guess and you have to play with that and against the markets. [You have to] guess how much you have to buy and how much the power plants possibly generate.

AS: Lots of guessing?

Mm3: It is guessing. Part of it comes of course from experience, (...) but everyone experiences it differently, the experience is always different.

The solving of crises, thus, requires tinkering, improvisations, skills and informal interactions between different organisations. But not much suggests that it escapes the "business as usual" of the control room: that is, economic frames have to be produced even in exceptional situations. This is according to the operators also a limitation of simulated crisis exercises that they are sometimes subjected to. When I ask about crisis training, an operator responds that market prices vary from one situation to the other and cannot be thus simulated:

In practice we don't have anything like that, that we would for example simulate something. Because they are so hard to develop, when you never know about those market prices, when even if you have some major situation, nobody knows the market prices. And they cannot be simulated either. (Mm2.)

Tellingly, while a plan that deals with exceptional crisis situations has in fact been trained to the operators, but its place is inside a binder:

AS: Do you know about or have you received some training here about crisis situations?

Mm3: In principle everyone has had to receive it and in principle everyone gets it. Then it is everyone‘s own responsibility how much you read it. But of course it can be found in the binder.

The key finding from all of the section is that the more these workers are pushed towards today's characteristic "just in time" production, the more their dispositions remind of what Pat O'Malley (2004) describes the classical liberalism of the 19th century, its "yoke of foresight" and reliance on market contracts as chief mean for mitigating future uncertainties. Production of this type, almost by definition, is not sensitive to the requirements of disaster and crisis situations: such as the need of energy generation backup reserves (Roe & Schulman 2008). The energy market workers are, in brief, calculative market actors, not actors who view that they are calculating other than financial risks. But what about the other control room that deals with the technical maintenance of the electricity grid? I turn to the question next in the next section.

3 The electricity distribution control room and security of supply

Even though both are control rooms by design, the work done in the distribution control room is in many respects different from that of the energy market control room. The utility had only one control room before the electricity market restructuring, yet, today only one of the operators of the study is able to work in both of the control rooms. He makes the following comparison of the rooms:

> The energy market control room is like keeping watch of a camp fire. You have to be constantly keeping up a small flame, that is, you should not fall behind from the energy stock exchanges. Working in the distribution control room, on the other hand, is like being a tin soldier. Not anything is happening all the time, however, when someone calls you have to be ready on-the-spot. (Bm1.)

Generally speaking three types of responsibilities are associated with the distribution control room: first, maintaining a functioning electricity distribution system; and in so doing, second, maintaining the well-being of customers; and third, operating the system so that large-scale material losses are avoided (Bm1). More specifically during daily work,

> we are monitoring [the electricity grid] and also using remote operated stations and switches and other accessories. And the normal use is that when a load-change causes a situation or because of building operations the switching [of the energy grid] has to be occasionally changed. (Dm4.)

The most typical routine of the working day is testing remotely newly installed accessories of the electricity grid in cooperation with teams of mechanics on the field. At the same time the room

is also monitoring the consumption of so-called "waste power" in the electricity cables continuously (Dm4). Overall, the name of the room given by electricity experts – the electricity distribution surveillance – seems to apply well to the work of the room: they are all the time observing and "watching over" the electricity grid.

Already, many of these explanations by the workers remind of the characterization of another political philosophy that deals with risk: *social liberalism* (O'Malley 2004, 41-48). Customer's welfare is at stake; expertise is needed; risk and uncertainties are, to extent, to be removed. This is further echoed in the ways that the workers solve a fault.

As already said, the components of the grid may also issue alarms at any moment: these are related either to the level of voltage, to the level of current or to the component's temperature (Dm4). When I ask about the number of alarms on a typical day, an operator says that he has not counted them (Dm2), but checks an "event list" that has 36 pages of events for that day on a computer screen, although some events do not issue an alarm to the operator. It is never the less clear that alarms are very frequent in the room. The task of the operator upon an alarm is to first report the details of the fault to a computer system, then determine whether a maintenance team is needed and if it is, send the team to the field and coordinate with them henceforth. The control room operators are both remote supervisors of the maintenance work and also continue to switch the electricity grid to new a configuration if necessary (Dm4).

In the previous sections about the energy market control room, it was discovered that the operators of the room rely on an improvisational approach to solving practical problems. The case is similar in this control room though not always straightforwardly. Practical actions and ever-changing contexts are emphasised upon by the operators. At the same time, however, the room incorporates many highly formal methods for solving faults, such as those associated with electrical safety while maintaining grid or fixing faults by rerouting electricity with the circular structure of the distribution grid (Dm1).

Let us see a conversation on this topic:

> AS: Are there many rules that are followed even though the situations change?
>
> Dm3: Well, of course security and other sets rules about what has to be done. You have to go according to them. And every man has to have the same viewpoints to those things. That does not change according to who sits here.
>
> AS: And then you are talking about electricity security? Electric shocks and others, fires?

Dm3: Yes, all of these, when the switching is done in such a secure manner and in the same way, that is where it starts. Of course [there are?] situations where anything can come.

AS: Yes, yes. Do you have machine standards then?

Dm3: Of course. We have certain standards and we make security guidelines ourselves.

AS: Well, is this then, this seems very specific this taking care of infrastructures. It seems that the use of these technologies cannot be set by strict rules, rather, the situation lives and you have to go along with that.

Dm3: It is like that for sure. Because every fault is little different and there will be faults, and you have to consider each time separately every thing about how you act then.

This long piece illustrates a practical conflict in respects coping with uncertain situations. On the one hand, it is emphasised that the practice of the room follows strict rules and standards when "security" is considered. Similarly, when Finnish rail control room operators were interviewed after several railroad system breakdowns in 2008, they insisted on following a "security principle": "If a fault is even suspected with traffic control, the whole traffic has to be stopped in spite of the danger of you being roasted, because it is a question of security."

On the other hand, the way "security" is guaranteed is still to some extent improvisatory and dependent on the circumstances. This can be seen in the way that framing is switched during the last question-answer pair above; from the following and making of strict security guidelines to the actions on-the-spot. Arguably, the last question might have been leading the participant to different way to approach the same topic, and perhaps he was following the lead or simply being polite when answering. But another of the operators has reflected on the similar converse between security and action:

AS: Earlier you mentioned that all the work is mutually agreed and standardised, then how much is this regulated by such standards, different standards and laws?

Dm4: In principle electricity work is usually highly standardised. If everyone follows the standard, then it is highly kind of structured. There is the problem, however, that when you go to the work destination, the destination might be highly varying. And then comes your own adaptation of how you want to do it.

As a rule, the electricity grid should be switched back on and during the maintenance work that part of grid is set dead of voltage. But the latter practice also involves a trade-off: this has to be done in such a way that there is not "an unreasonable harm to the other customers" (Dm4) who will also lose their electricity for the time of the fixing.

I was able to observe one occasion when the just mentioned operator (Dm4) fixed a customer fault. The situation was sparked when a customer called the company. The technician first talks with the customer who has his or her lights blinking at home. He then determines if this fault is the responsibility of the electricity company. He decides to send maintenance to the field because although the problem is at a home and not on the company's electricity grid, blinking lights may indicate a "ground fault" which has a risk of electric shock to the customer. He finds the location of the house on a computer map; and phones a maintenance team and tells them about the technical details of the fault. He determines how many other houses have to be, "in the worst case" as he tells me, cut off from electricity distribution during the fixing of the fault. He waits for the maintenance team to get to the house of the customer. He tinkers with a computer to start writing a new fault report. He talks with the maintenance on the phone again once they arrive. And finally after several attempts at finding the cause of the fault at the customer's house, he determines together with the maintenance that this was not a "ground fault" but a problem of loose electricity line, typical "of these old soldier houses" as he notes to me. He then concludes the fixing by sending the maintenance team off and checks with the details about their working hours which determine their billing.

The point in this long description is that there are divergent aspects in the work and only some of them are anticipated, or standardised. The above example documents constant tinkering, improvisations, independent decisions, team work, skills, using of computer systems, practical rules of thumb and know-how of the local region. It should also be noted that the workers contract the maintenance from an outsourced team: a significant intervention by the logic of classical liberalism to this control room. The social liberalism as depicted by O'Malley (2004) is in many ways about removing risk and uncertainty: for example, through standards, customer protection, laws and safety protocols. But it would seem that here it is not completely fixed practice. Risk and uncertainty still figure in the work: only they operate as it were "under" the formal rule-following. This result is further illustrated by the ways that the workers tell they handle crisis situations.

For more exceptional situations in the rooms, an operator (Dm4) recalls two major storms in the 1990s. During these storms (called Janika and Pyry, respectively), more than 800 000 Finnish customers suffered from a momentary blackout and over 1 600 household were without electricity for more than five days. When I ask an operator if the normal working routine had to be modified

during the Pyry and Janika storms, he responds that the control room had extra help in the form of another operator. When switchers of the remote using went off, one of the operators wrote the fault down and another switched them back on. It is however not easy to see that these situations had been unmanageable. Conversely, it seems to have been even instructive and to some extent cumulative in respects performance: during the faults one of the operators invented a new practice for writing down faults that is still in use in the room (see also Roe & Schulman 2008, 177).

4 Conclusions

The paper started with the following general research question:

- What are the notions and practices of risk in the management of electricity supply?

I assumed that there are two kinds of risks with electricity supply – the market risk and the technical risk – and introduced my empirical case in a local electricity company. The following more specific questions were then asked:

- How does market risk deal with and incorporate technical risk and vice versa? To which extent are the two kinds of risks incommensurate?
- How do technical risks and financial risks figure in the actions of providing electricity?

It is clear that the intertwining of market risks and security risks in the management of electricity supply is not a simple research topic. Instead, like research on multiplicity of risk already suggests, the control room working practices were ambiguous. To some extent, the social worlds of the two control rooms (market room and distribution room) were separate; indeed, the rooms were physically fenced off by a wall, and the workers were not officially allowed to interact with one another. The market room workers emphasized that they operate in an economic frame, the distribution room workers produced security frames. Not much escaped these frames: even disaster and crisis situations seemed to resemble "business as usual" more than a catastrophe.

This overall picture of the work and risk is not quite accurate, however. First of all, a frame does not mean that the actions were determined by governing rationalities. As I observed it, the production of a frame required informal interactions, skills, hunches, and intuitions among the drawing on diverse

data sources. The production of a risk frame is simply an end result and a requirement of the work, it does not necessarily reduce the work to a mindless routine.

Secondly, it is still difficult for me to see how market risks and technical risks are *not* intertwined. To start with, the notion of a market risk is indeed based on the effort to mitigate technical risk. Market contracts increase the predictability of actions and assign responsibilities for provision of security. Day-ahead and real-time markets both are manners of reducing risk of energy imbalance. As these markets did not exist formally before the electricity market restructurings in 1995, it might even be said that they make the work more *disciplined* in terms of risk. That the workers do not seem to acknowledge technical risk is an important finding; yet it does not make the role of technical risk in market risk less important.

What about the other way? How does technical risk incorporate market risk? For one, even technical security is provided on a market place. The workers calculate the working *costs* of fixing the electricity grid, determine whose financial and legal *responsibility* the fault is, and *contract* for outsourced maintenance teams. Sometimes, it would seem that the notion of security is a trump card that is applied before any considerations of financial efficiency. But it is dubious how such "security principle" would operate in long disturbances, with the pressure of making profit and providing continuous electricity supply on the other end. In the end the same phenomenon repeats as in the market room: the workers who operate with technical risk also operate with market risk, only they do not acknowledge it themselves. Or at least they do not acknowledge it in the interview speech.

The analysis in this paper is still continuing. The intertwinings of security risk and market risk is a rich and varied topic, and I feel that it demands more attention, especially more interpretation. Further benefits of exploring a local case is that it offers an uncommon perspective on the regionality of risk. So far, the territorial foundations of the multiplicity of risk have not attracted much attention to my knowledge. These foundations are an important topic to study, however. Global markets, and with them the mitigation of financial risk, are based on the notion that the world is "spaceless": put differently, that labour, goods, capital, information, and energy move over international markets without friction. Infrastructure networks, however, are situated on a region, infrastructure consumers live in a fixed place, and technical risks such as electricity blackouts always concern a specific region. Furthermore, infrastructures are produced by organizations with their physical premises: in the case of this paper, workers responsible for technical risk and financial risk respectively operate from neighbouring control rooms. How does region and space figure with technical risk and financial risk, what kind of tensions does regionality cause to the management of risk, and how are these tensions

resolved? Little is known about these matters, and the research results offer ground to evaluate them.

References

Adams, John (1995). *Risk*. London: UCL Press.

BBC (15.3.2011). Japan earthquake: Living with blackouts. Link checked 23 May 2011: `http://www.bbc.co.uk/news/world-asia-pacific-12731696`

Brunner, Elgin & Suter, Manuel (2008). International CIIP Handbook 2008/2009. An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies. Center for Security Studies, ETH Zurich.

De Bruijne, Mark & Van Eeten, Michel (2007). Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment. *Journal of Contingencies and Crisis Management* 15 (1): 18-29.

Beck, Ulrich (1992). *Risk Society: Towards a New Modernity*. London: Sage (German original 1986).

Callon, Michel (1998). An essay on framing and overflowing: economic externalities revisited by sociology. In Callon, Michel (ed). *Laws of the Markets*. Wiley-Blackwell.

Collier, Stephen (2008). Enacting Catastrophe: Preparedness, Insurance, Budgetary Rationalization. *Economy and Society* 37 (2): 224-250.

Collier, Stephen & Lakoff, Andrew (2008). The Vulnerability of Vital Systems: How Critical Infrastructure Became a Security Problem. In Dunn, Myriam & Kristensen, Kristian Søby (eds): *Securing 'the Homeland': Critical Infrastructure, Risk and (In)security*. London: Routledge.

CEER (Council of European Energy Regulators) (2005). Third CEER Benchmarking Report on Quality of Electricity Supply. Bruxelles: Council of European Energy Regulators ASBL.

CEER (Council of European Energy Regulators) (2008). Fourth CEER Benchmarking Report on Quality of Electricity Supply. Bruxelles: Council of European Energy Regulators ASBL.

Douglas, Mary & Wildasky, Aaron (1982). *Risk and Culture. An Essay on the Selection of Technological and Environmental Dangers*. Berkeley and Los Angeles: University of California Press.

EU (European Union) (2003). Directive 2003/54/EC of the European Parliament and of the Council of 26 June 2003 concerning common rules for the internal market in electricity and repealing Directive 96/92/EC.

EU (European Union) (2008). Council directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

EU (European Union) (2009). Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC.

Ewald, François (1993). *Der Vorsorgestaat*. Frankfurt am Main: Suhrkamp (French original 1986).

Furedi, Frank (2006). *Culture of Fear Revisited*. Cambridge: Polity Press.

Graham, Stephen & Simon Marvin (2001). *Splintering Urbanism: Networked Infrastructures, Technological Mobilities and the Urban Condition*. London: Routledge.

Helén, Ilpo (2004). Technics Over Life: Risk, Ethics and the Existential Condition in High-Tech Antenatal Care. *Economy and Society* 33 (1): 28-51.

Höst, M.; Kristofersson Nieminen, T.; Petersen, K. & Tehler, H. (2010). FRIVA – risk, sårbarhet och förmåga: samverkan inom krishantering. Lund: Lunds universitet.

Luhmann, Niklas (1993). *Risk: A Sociological Theory*. Tranlsated by Rhodes Barnett. Berliini & New York: Walter de Gruyter (German original 1991).

Nord Pool (2009). The Nordic Electricity Exchange and the Nordic Model for a Liberalised Electricity Market.

Nord Pool (2011). The Elbas market. Link checked 24 March 2011: `http://www.nordpoolspot.com/trading/The-Elbas-market/`

Mol, Anne-Marie (2003). *The Body Multiple: Ontology in Medical Practice*. Duke University Press.

Reuters (27 April 2011). Japan summer power curb target to be relaxed to 15 pct. Link checked 23 May 2011: `http://www.reuters.com/article/2011/04/28/energy-japan-power-idUSL3E7FS03K20110428`

Roe, Emery & Schulman, Paul (2008). *High Reliability Management: Operating on the Edge*. Stanford: Stanford Business Books.

Silvast, Antti (forthcoming 2011). Market Screens and the Management of Electricity Supply: The Case of a Finnish Electricity Grid Control Room. Accepted for publication in *STS Encounters*, published in September 2011.

Steenhuisen, Bauke (2009). Competing Public Values: Coping Strategies in Heavily Regulated Utility Industries. Dissertation: TUD Delft University of Technology.

O'Malley, Pat (2004). *Risk, Uncertainty and Government*. London, Sydney & Portland: Glasshouse Press.

Viljainen, Satu; Makkonen, Mari; Annala, Salla & Kuleshow, Dmitry (2011). Vision for European Electricity Markets in 2030: Final report. Lappeenranta University of Technology Faculty of Technology. LUT Energy Research report 13.