Case Study: Information Flow Resilience of a Retail Company with Regard to the Electricity Scenarios of the Sicherheitsverbundsübung Schweiz (Swiss Security Network Exercise) SVU 2014

Patrick O. Leu[1(✉)] and Daniel Peter[2(✉)]

[1] Head of POS Infrastructure and Systems,
Migros Genossenschaftbund, Zürich, Switzerland
pleu@pleu.ch
[2] Lucerne School of Business, University of Applied Sciences,
Lucerne, Switzerland
daniel.peter@hslu.ch

Abstract. The Sicherheitsverbundsübung Schweiz 2014 tested the availability of critical infrastructures. The present case study examines the extent to which one of the largest retailers in Switzerland will be able to continue operations under this scenario. Various interviews, simulations and process categorizations were undertaken to this end. The findings clearly demonstrate that with a short-term black-out, damages incurred by the retailers focused on here quickly exceed the 100 million Swiss franc mark. Meanwhile, a longer power shortage situation would probably be an existential threat. Under these preconditions, it becomes obvious that the security of the food supply for the Swiss population via organised channels will not be guaranteed. The problem analysis clearly conveys that awareness as to critical infrastructures has far from reached decision maker level and that the resilience of processes has been weakened further due to strategic decisions.

Keywords: Resilience · IT security · Continuity management · Power blackout · Retail business · Process Assessment Model · COBIT 5 · Business Continuity Management (BCM) · IT Service Continuity Management (ITSCM) · Business impact analysis

1 Introduction

The availability of critical infrastructures such as the communications and energy infrastructures is of vital importance both for society and for the economy [1]. Next to threat scenarios arising from (terrorist) attacks on critical infrastructures, there is also an exposure to natural perils (a. o. storms, floods, avalanches, severe winters). A third hazard group is based on human or technical error [2].

Communication and energy infrastructures are distributed over huge areas and frequently very insufficiently protected against the risks mentioned above. Smaller events, for

E. Rome et al. (Eds.): CRITIS 2015, LNCS 9578, pp. 159–170, 2016.
DOI: 10.1007/978-3-319-33331-1_13

instance an excavator cutting through a power cable, mainly only have a local and temporary impact. In addition, companies are quite able to protect themselves against the effects of such events by employing suitable measures (e.g. emergency power generators).

While it is quite possible for crisis committees to manage any isolated events and/or events which are clearly geographically limited, the challenges clearly increase if several large-scale events occur at the same time, or if there is an event affecting a whole country. The Sicherheitsverbundsübung 2014 (SVU 14) simulated several large-scale events and had them occur in a serial and parallel manner [3, 4]. In particular, the SVU 14 describes scenarios such as drought, power cut, power shortage situations, cold spells and a pandemic. It was the aim of the exercise to check the effectiveness of preparatory measures, and to examine the co-operation between authorities, sectors and organisations during such scenarios [3].

On 27th June 2012, the Swiss Federal Council published the "Nationale Strategie zum Schutz kritischer Infrastrukturen" strategy paper (on the "National Strategy for the Protection of Critical Infrastructures") [5]. It describes the recording of critical infrastructures ("CI") in a classified register. The categorization is ordered by sectors and sub-sectors here (see Table 1).

The criticality of the sub-sectors is split into three groups and represents the relative importance in a normal hazard situation. Criticality can change depending on the event and the need for action arising from this. A derivation of the criticality to individual items in the sub-sector across the board is not possible.

In addition, the strategy paper states 15 measures split into two fields of action. The cross-CI field of action [5, p. 7726 et seqq.] safeguards a co-ordinated approach, which is meant to improve the robustness of society, economy and state against breakdowns in critical infrastructures. The second field of action [5, p. 7731 et seqq.] addresses specialist authorities and the operators of critical infrastructures. One measure is meant to check the self-protection or robustness of the critical infrastructure respectively, and to improve and thus increase them if necessary. To support the approach, the Bundesamt für Bevölkerungsschutz BABS (Federal Office of Civil Protection) has published a guide [6].

2 "SVU 14" Scenario

The hazard and threat scenario constructed for SVU 14[1] basically comprises of a countrywide pandemic and a country-wide power shortage situation [7]. A cyber attack onto the power industry in September leads to a power shortage situation. Consumers are asked to reduce their power consumption. Because there is only insufficient compliance with this request, the Bundesrat implements the "Verordnung über die Elektrizitätsbewirtschaftung (VEB, Provisions for electricity management)"[2] in accordance with art. 28 of Federal Law. This describes how to manage electric energy which is only available in limited quantities.

[1] In contrast to a hazard, a threat requires intent. The cyber attack intentionally leads to a power shortage situation. The pandemic however is a hazard.

[2] The "VEB" is available in draft form. The definitive version will be published by the Federal Council in a shortage situation.

Despite everything, the power grid in the western parts of Europe collapses for 48 h. Once it is possible to start up and stabilize the power grid, it will only be available with a severely limited output of a maximum 70 % for another 8 to 12 weeks [3]. This power shortage situation tries to keep the grid stable with the help of restrictions applied to power supplied. Quantitative restrictions and reduction models are used as tools for stabilization. At the same time the VEB is implemented, the Eidgenössische

Table 1. List of critical infrastructures by sectors and sub-sectors [5: 7719]

Sectors	Sub-Sectors		
	regular criticality	**high criticality**	**extreme criticality**
Authorities	Diplomatic missions and head offices of international organisations	Parliament, government, judiciary, public administration	
	Research and education		
	Cultural assets		
Energy		Natural gas supply	Crude oil supply
			Power supply
Disposal		Waste	
		Sewage	
Finances		Insurance	Banks
Health	Laboratories	Medical care and hospitals	
Industry	Engineering, electrical and metal industries	Chemical and drugs industry	
Sectors	**Sub-Sectors**		
	regular criticality	**high criticality**	**extreme criticality**
Information and communication		Media	Information technologies
		Postal service	Telecommunications
Food		Food supply	Water supply
Public safety	Army	police, fire brigade, ambulance service	
	Civil defence		
Transport	Shipping	Air	Rail
			Roads

Departement für Wirtschaft, Bildung und Forschung (WBF, Federal Department for Economy, Education and Research) implements the "Vollzugsverordnung für die Kontingentierung und Netzabschaltung" (Executive Statute for quantitative restrictions and grid disconnection) [7].

- **Quantitative Restrictions:** Industrial buyers with an annual electricity requirement of > 100,000 kW/h have the option of maintaining a sustainable power supply by reducing their electricity consumption to 70 % of their reference consumption (same month of the previous year). This is under the specific condition that there is a direct feed, and that the electricity purchased can be metered remotely [7].
- **33 % reduction model** means 8 h of power, then 4 h without power. **50 % reduction model** means 4 h of power, then 4 h without power. The period over which power is available will be changed over after a week, so that it is not always the same time that no power is available [7].

At the same time the power shortage situation occurs, a pandemic erupts across Switzerland, peaking in November [2]. About a quarter of the population is affected. Smaller peripheral events which despite their size have quite a significant influence on the power shortage situation scenario are a cold spell preceded by a drought. The former leads to an above-average demand for energy, the latter to below-average reservoir filling levels [2].

Below we will examine what impact the power cut and power shortage situation will have on processes inside the retailer's branch businesses. The retail companies and processes examined are typical for the company and critical with regard to the importance of country-wide supplies. Special attention is to be paid to the effects of transferring sales - currently organised in a decentralized manner - to a centralized solution.

3 Object of Analysis

The retail company analysed was founded in 1925 and is among one of the largest food suppliers in Switzerland. In the year 2014, the company generated a turnover in excess of 10 billion Swiss franc (some 10 billion Euro) in the supermarket and consumer market sector. Corresponding to an overall Swiss market share of some 40 %, this means the company is co-responsible for the well-being of the Swiss population to a significant degree. In addition, its group of companies also operates in the energy, finance and industry sectors with more than 50 companies. Historic, mainly politically motivated events lead to the company having a 45 % rate of in-house production compared to turnovers generated - a high, above-average proportion which is atypical for their industry[3].

[3] The authors are not allowed to mention the name of the examined organisation.

4 Methodical Approach

To procure the data and information required, we undertook various interviews with experts inside and outside the company [8]. Amongst others, these included the Heads of Informatics and of Infrastructure, Process Owners, Divisional Heads and IT Service Continuity Owners from the Informatics sector. With regard to operational aspects, those responsible for security services, logistics and energy supply were available for interviewing. To obtain an external assessment, four electricity grid operators were interviewed. Because sound data communications are just as important to the retail sector as the energy supply itself, we also interviewed exponents of the two largest communications providers.

With regard to external organisations, we interviewed OSTRAL (Swiss organisation for power supply in exceptional situations) and authorities such as the Oberzolldirektion (Customs Head Offices) and the Bundesamt für Bevölkerungsschutz (Federal Office of Civil Protection).

Using these expert interviews [8] and by also analysing secondary materials, we undertook a maturity level analysis of the internal processes. We based this on the recommendation of the guide for the protection of critical infrastructures by the Bundesamt für Bevölkerungsschutz, BABS [9].

During the investigation, we focussed on critical units of the company under evaluation. We therefore selected three companies from the group of companies involved, from the retail and branch network sectors, two companies from the logistics and product management sector as well as a joint subsidiary responsible for central IT services, marketing, central purchasing, logistics and HR. We assessed the organisational and technical measures taken by the CI operator. Within the context of this paper, critical infrastructures (CI) denotes the following:

- Data centre sites essential to the operation of the critical business process.
- Informatics workplace sites essential to the operation of the systems involved in the critical business process (do not necessarily have to be identical to the data centre sites).
- Branch sites necessary for the sales element of the critical business process.
- Logistics sites responsible for the replenishment of supplies in the critical business process.

With regard to organizational evaluation points, we checked up to which maturity level management systems are present in the areas of risk and continuity. The processes are assessed with the aid of a maturity level model. This is based on the process assessment model (PAM) of the COBIT 5 standard (based on ISO/IEC 15504). In particular, continuity management systems such as business continuity management (BCM), IT service continuity management (ITSCM) and crisis and emergency management concepts were evaluated. In connection with preventative measures, we focused on risk, security and protection management processes.

The technical evaluation points aim for the requirements derived from the SVU 14 (power cut and power shortage situation). The most important questions here were:

- Can the site be supplied with electricity using existing technical measures (power generating equipment) for 48 h?
- Are emergency work spaces set up at the site for informatics and operations employees?
- How is access to the building and work spaces safeguarded during these 48 h?
- Can the maximum power consumption be reduced to 70 % of the reference consumption (same month of the previous year) for a period of 8 to 12 weeks at company level?
- Is it possible to maintain operations on the site by using existing technical measures (power generation units), or by procuring such measures for a period of 8 to 12 weeks, with a reduction model (33 % or 50 %)?

The influences of an event on a business as described by SVU 14 are assessed in accordance with the company specifications of the business impact analysis (BIA). There are five grades of damage categories, specifying the extent of the impairment by damages incurred from different angles (from "very low" to "very high"). A time-line with 5 points of measurement (from 4 h to 30 days) also shows how an event can change in the long run. The event is assessed from different angles. Different angles and categories do not have to be related to each other. From a technical angle for instance, a category 3 event does not automatically mean there is a category 3 financial loss. The following angles are assessed:

- Time it takes for the company to recover from the event.
- Lost turnover potentially caused by the event.
- Additional costs potentially caused by the event.
- Damage to the reputation potentially caused to the company.
- Final consumers and how they are affected by the event.
- Business process and how this is impaired by the event.
- IT services disrupted by the event.

5 Simulation and Findings

The basis for the simulation is the SVU 14 scenario. The results of the technical and organizational assessment of the companies checked were integrated into the simulation (see Table 2). The result is a sobering one. Just about one site in Switzerland is able to survive all scenarios across the overall duration and under the aspect of all potential manifestations.

To calculate the monetary consequences, assumptions about turnover generated during this period were available. To assess the impact on processes, final consumers and reputation, specifications from the business impact analysis (BIA) were available (Table 3).

Table 2. Result of scenario applied to sites (addressing the resilience)

Site	Power cut			33% reduction model	50% reduction model
	without reduction model	with 33% reduction model	with 50% reduction model		
Data Centres West	1	1	1	1	1
Data Centres East	1	3	1	1	1
Data Centres East 2	4	4	4	2	2
Data Centre East 3	4	4	4	2	2
Work site East 2	4	4	4	2	4
Work site East 3	4	4	4	2	4
Data centre Central	1	4	2	1	1
Work site Central	4	4	4	2	4
Logistics site East	4	4	4	2	4
Branches	4	4	4	4	4
Information flow	4	4	4	4	4

Table 3. Damage impact assessment in accordance with "power shortage situation" scenario BIA

	4 hours	24 hours	48 hours	7 days	30 days
Lost turnover	1	1	1	3	4
Additional expenditure	1	1	1	2	4
Impact on final consumers	4	4	4	4	4
Impact on business process	4	4	4	4	4
Impact on IT services	4	4	4	4	4
Damage to reputation	1	1	2	4	4

If you consider the power cut with a view to turnover development, the following picture emerges. The bars represent the turnover development in the four retail sectors during a normal week-end in October. The curves however show the picture in case of the "power cut" SVU scenario (see Fig. 1).

Compared to the normal case, the curves are not rising (03/10/2014) because the cut resulted in a failure to replenish supplies, and a considerable amount of fresh and frozen product spoil. There is simply less to buy for final consumers. Fresh and frozen products are probably compensated for by groceries (tins, ready meals, etc.).

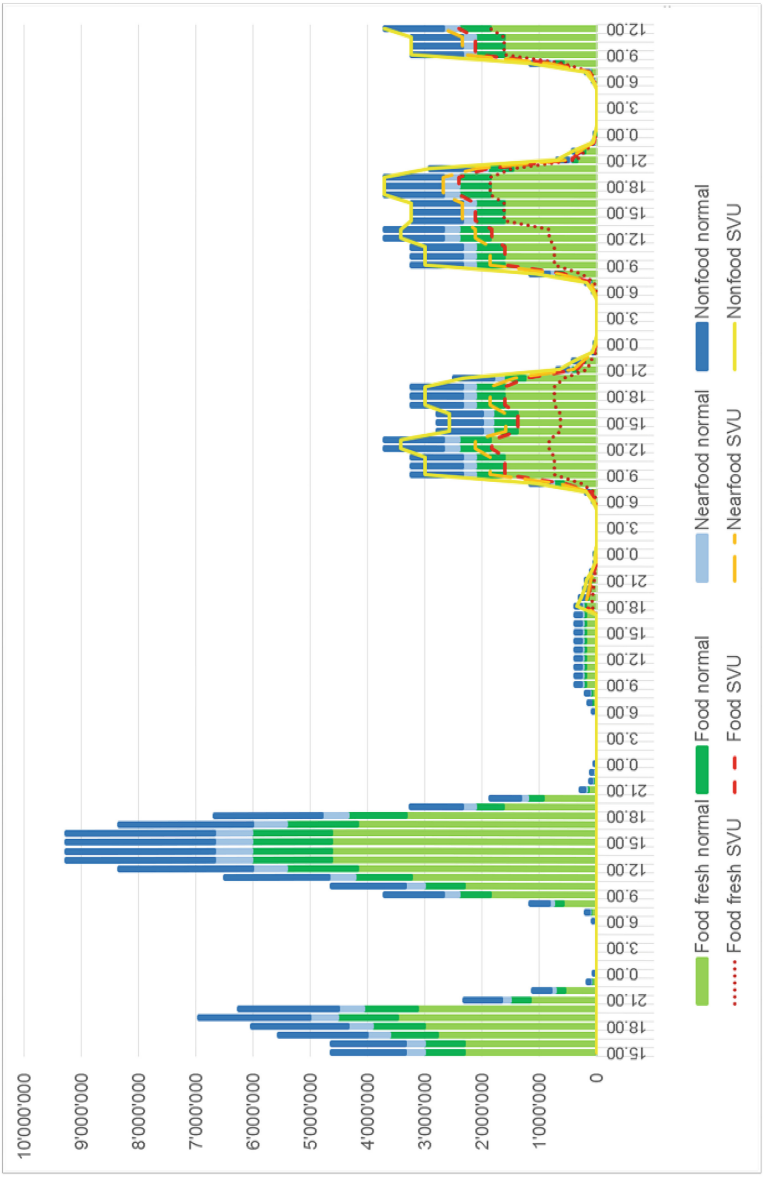

Fig. 1. Power cut scenario - comparison of normal sales vs. SVU scenario sales in CHF

6 Vulnerabilities Identified and Conclusion

All of the companies are prepared for quantitative restrictions either badly or not at all. All companies lack plans for power reductions of 33 % and 50 %. It is widely unknown which internal consumers consume how much energy. Although there is an idea of

possible savings potential (for instance cold storage rooms), it was widely unknown in how far savings could be realized in this sector, and what yield these will generate.

A similar picture emerges for the informatics sector: Data centre operators were not able to advise how high a room temperature they were able to run while still being able to run stable system operations.

Strategic connectivity partners are presumably also excluded from the allocation conditions. This assumption however is not currently a secure one.[4] This special position is explained by the impossibility of achieving savings around the 33 % mark, without refraining from partial shut-downs of services and infrastructures perceivable as discriminatory. A prioritization of data connection customers would have to take place analogous to the power suppliers. In an emergency, you will have to do without any consideration of non-discriminatory measures. It is probably better to have CI providers supplied for as long as possible than having to execute a non-discriminatory total switch-off.

If the case arises that electricity generators request their consumers to reduce their power consumption, i.e. quantitative restrictions are applied, there is no company-internal co-ordination process available at the moment. Authorities and associations are probably not currently clear about who to contact in the company, and which responsibilities are covered by a partner contacted this way. It is not clear either how to proceed in such a case inside the group of companies. There is an urgent need for action here.

6.1 Findings on Power Shortage Situation (Reduction Models)

All of the companies are prepared for a reduction model either badly or not at all. There are only few precautions to be found in individual companies from an organizational angle. Measures found are generally sector-specific, often have developed in a situational manner from an event encountered, and have not been co-ordinated in the company overall. Technical measures do work in isolated cases, although this is due to lucky coincidence rather than deliberate intent.

Generally it is to be stated that the company will not work in case a reduction model is applied, in particular due to the strong centralization of informatics services. In case a reduction model is run for longer than seven days, the retailer faces a serious existential threat. Even if power is available locally, nothing can be sold in branches if there is a central IT solution in operation. Since converting to displaying prices on the shelves in 2011, there is no additional information about prices any longer either. It is therefore not possible to use pocket calculators. The current emergency till consisting of mobile data input devices for the supply replenishment procedure will shortly no longer be in existence. A centralized facility will be commissioned in the near future.

With a decentralized till architecture, an hour a day should be sufficient to safeguard sales and supply replenishment processes. Loyalty schemes or electronic payment transactions are excluded here. The communication between data centres and logistical sites can also be maintained with just a few hours a day. As the reduction model has to

[4] 20 January 2015.

be worked out by every grid operator individually for their respective regions, there is a very slim chance that a Ticino branch remains in direct contact with one of the two data centres during this phase - which could stretch over several weeks.

An emergency program by the logistics companies safeguards smooth goods deliveries without follow-up orders by branches over 48 h. After a week, deviations will however become so severe that they have nothing much in common with actual needs locally. Existing internal emergency scenarios do not take into account a total failure across Switzerland. They are based on the assumption that suppliers still function.

The connectivity partners questioned reckon that a reliable and continuous communications link during a reduction model phase is nigh on impossible. The reason can be found in the uncoordinated power supply or one which is allocated by sectors and cannot be coordinated. In accordance with Cablecom statements, the type of connection of a site might play a role in deciding whether a connection (from branch to data centre) could also be possible without continuous power. Here, glass fibre-based connections are probably more resistant than copper-based cables, as a glass fibre connection is able to carry data across longer distances unamplified. However, this is only hypothetical. It is impossible to provide a qualification across the board. Even if this applies from a technological angle, every individual case, and in this case every cable, has to be checked first. Cloud-related network services such as MPLS where an exact location of data streams is impossible, further impede the implementation of measures.

Industrial companies will not be able to run any production jobs with a 50 % reduction model. These statements were heard quite frequently during our interviews in industry-related circles. Verification is not part of this paper.

6.2 Conclusion

A power cut does not present any or only minimal problems for the sites checked. However, processes will no longer run. Branches will have to make large staffing efforts. They will suffer financial turnover losses because all branches will have to be closed, but will be able to cope with the consequences of spoiled products in the fresh produce sector. An event in Italy 2003 presented retailers with losses of some 120 million Euro [10, p. 2]. For the company assessed, some 130 million Swiss franc were estimated. If you project this taking into consideration their market share of some 40 %, a total loss of some 320 million Swiss franc across Switzerland would result.

There is an existential threat by the reduction model in connection with a centralized till solution architecture. As continuous communication is no longer safeguarded, branches will not be able to keep selling. With the 33 % reduction model, chances are slightly higher than with the 50 % reduction model, because individual sites and sectors will have power for longer. Due to the different segmentation and different switching times (power on, power off, power on), it is possible that communication pathways can still be maintained with branches close to data centres.

Research confirms that only a handful of companies will be able to bypass even the less severe power cut scenario. The other companies will be out of action either immediately, or will have to struggle against the effects with high manual efforts. For the

other sites, it is recommended to run an orderly shut-down of all systems immediately after the cut starts to prevent worse from happening, because there are insufficient emergency power infrastructures.

None of the companies is prepared for the more severe scenario of a power shortage situation. None of them has preventative (for quantitative restrictions) or reactive (for cyclical power switch-offs) measures to hand. Measures found are only ever sector-specific (informatics only, logistics only, etc.), and have often been developed in a situational manner from an event encountered, and have not been co-ordinated in the company overall. Technical measures do work in isolated cases, although this is due to lucky coincidence rather than deliberate intent. In all companies, measures are taken to the best of their knowledge, instead in accordance with tactical or strategic specifications by the company management, the reason being that such approaches are simply lacking. Specifications from a business impact analysis (BIA) were nowhere in existence. If they were, they were largely obsolete (some of the BIA documents were seven years old). In consequence, precautions, although well-meaning and very effective in part, were neither co-ordinated with any business strategy nor other sectors within the company.

As a national company, you need to be able to co-ordinate the necessary preventative measures across the whole company. Structural bodies to do so, for instance appropriate co-ordination offices, were lacking. In case of emergency, i.e. if one of the scenarios arises, any company-external party does not know who to report to. This lack of knowledge clearly showed during interviews. Numerous names of people to be contacted in an emergency were mentioned. Whether it is then clear who is responsible internally for the one issue or the other, is difficult to assess, not to mention the availability of these individuals in case an event occurs.

The most important measure is to prevent cyclical power switch-offs by all available means. This can be achieved with effective power saving measures. For a better alignment of precautions, it is urgently recommended to request all companies to provide company management specifications. Work spaces must be available for any power cut scenario, where specialists have emergency power-fed work spaces available to them should an event occur. In case cyclical power switch-offs would need to be pushed through despite all efforts, the retailers' survival not least depends on autonomous branch stores. This in particular is being revoked in Switzerland at the moment due to centralization efforts.

References

1. Tagesanzeiger. 31 Attacken auf Schweizer Wasserkraftwerke. Tagesanzeiger. Retrieved 8 February 2015
2. EATON Corporation: Blackout Tracker; Jahresraport 2014 Deutschland, Österreich, Schweiz; Acherrn (2015)
3. Swiss Conferation: Sicherheitsverbundsübung 2014 (SVU 14) http://www.vbs.admin.ch/internet/vbs/de/home/themen/security/svu14/uebersicht.html (2015). Retrieved 14 June 2015
4. Häfliger, M.: Bund und alle Kantone üben nationale Notlage. http://www.nzz.ch/schweiz/tausende-in-sicherheits-verbundsuebung-2014-involviert-bund-und-alle-kantone-ueben-nationale-notlage-1.18413147, 28 October 2014. Retrieved 14 June 2015

5. Swiss Conferation: Nationale Strategie zum Schutz kritischer Infrastrukturen. https://www.admin.ch/opc/de/federal-gazette/2012/7715.pdf (2012). Retrieved 14 June 2015
6. Bundesamt für Bevölkerungsschutz. Leitfaden Schutz kritischer Infrastrukturen– Entwurf. Berne, 5 November 2014
7. Bundesamt für Bevölkersungschutz. Sicherheitsverbundsübung 2014 (SVU 2014) – Allgemeine Lage – Für Module Notlage. Berne, 1 September 2014
8. Helferich, C.: Die Qualität qualitativer Daten: Manual für die Durchführung qualitativer Interviews. Wiesbaden (2004)
9. Bundesamt für Bevölkerungsschutz: Leitfaden Schutz kritischer Infrastrukturen (2015) http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/ski/leitfaden.parsysrelated1.85483.DownloadFile.tmp/leitfadenski2015de.pdf. Retrieved 14 June 2015
10. Bundesamt für Bevölkerungsschutz: Nationale Gefährungsanalyse - Gefährdungsdossier – Ausfall Stromversorgung (2013). http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/gefaehrdungen-risiken/-nat__gefaehr-dungs-anlayse/gefaehrdungsdossier.html. Retrieved 14 June 2015