Emerging risks related to large-scale engineered systems[1]

Wolfgang Kröger
Director, Laboratory for Safety Analysis, Swiss Federal Institute of Technology (ETH) Zürich, Switzerland

Growing complexity and mutual dependencies

Mankind has always succeeded in developing technologies, integrating them into systems and operating them to improve its welfare and security - but becoming dependent on them at the same time. In recent decades these systems have grown into a large-scale array of interconnected networks, spanning long distances, mostly privately owned or operated, that function collaboratively and synergistically to produce and/or distribute a continuous flow of goods and services. They are called infrastructures. This note will focus on physical-engineered networked infrastructures, often called lifeline systems, with electricity supply (high voltage transmission) systems and transportation by rail as the examples, both using information and communication technology (ICT) for data acquisition and industrial control (SCADA) to different degrees.

With reference to the electricity sector the pervasive use of digital systems has allowed for larger and tighter integration (e.g., extension of the synchronised ENTSO-E (former UCTE) grid from Lisbon to Bucharest) and operation of the system at its original limits.

This occurred alongside market liberalisation and the unbundling of owners/operators whose specific aims and logics were different from those of the former monopolists. Furthermore, the increasing share of "new-renewable" electricity generation, which is intermittent/stochastic by nature, implies a less predictable generation capacity. All this led to the development of unforeseen complexity in the European electric power system – a tendency which is ongoing due to innovative technological trends (decentralised generation/smart grids, smart metering/closer customer interaction, etc.) and continuing organisational-operational changes (see report, Section IV, **Recognising Complexity**).

According to [Dueňas-Osorio, 2008] complex systems are made up of "a large number of interacting components (real or virtual), show emergent properties difficult to anticipate from the knowledge of single components, are characterized by a large degree of adaptability to absorb random disruptions and are highly vulnerable to widespread failure under adverse conditions." Indeed, small perturbations can trigger large-scale consequences in critical infrastructures (e.g., due to '**Positive Feedbacks'** or '**Loss of Safety Margins**'). "Many complex systems have critical thresholds - so called tipping prints - at which the system shifts abruptly from state to another" [Scheffer et al., 2009], take the November 4, 2006 Western Europe blackout as one example.[2]

Such disruptions may be triggered by a multifaceted set of events, including technical and unintentional human failures, local and wide-area natural hazards, or malicious targeted attacks (terrorist, cyber). As physical-engineered systems consist of a large array of components interacting in complex ways and are interconnected and mutually dependent (also in complex ways),

[1] This paper accompanies the IRGC report "The Emergence of Risks: Contributing Factors" and is part of phase 1of IRGC's project on Emerging Risks. More information can be found online at http://irgc.org/Project-Overview,219.html
[2] A controlled line cut-off in NW Germany, under high load flow conditions led to a separation of the continental grid into three islands and affected 15 million households.

unidirectional dependencies and bidirectional interdependencies are therefore a more than abstract feature which may facilitate or undermine their robustness/resilience. The relevance of this issue has been demonstrated by various past events, the January 2, 2004 mini Telecom blackout in Rome may serve as an example[3] (See annex).

Rinaldi et al., [2001] introduced six dimensions for describing infrastructure interdependencies and delineated four general types of interdependencies (see Figure 1):

- physical interdependencies, e.g., a pipeline network provides gas to fuel a gas-fired power station while the electricity generated is used to power compressors and controls the gas supply network;
- geographic interdependencies, e.g., flooding or a fire affecting multiple infrastructures in close proximity;
- cyber interdependencies, e.g., a SCADA system monitors and controls elements of the electric power grid – but it may also provide pieces of information or intelligence supporting another infrastructure or a decision-making process elsewhere;
- logical interdependencies – these exist between infrastructures that do not fall into one of the above categories.

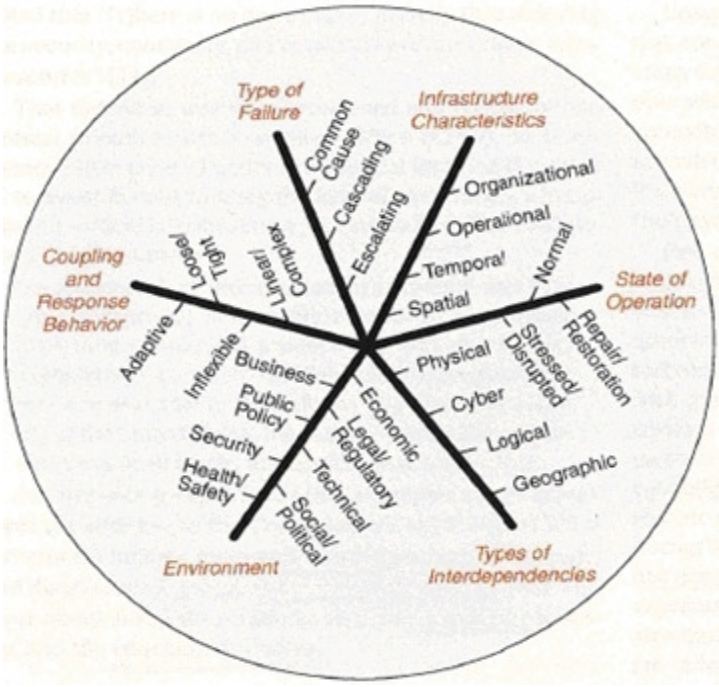


Figure 1: Dimensions for describing infrastructure interdependencies [Rinaldi et al., 2001]

The coupling and response behaviour deserves special attention as it directly influences whether the infrastructures are adaptive or inflexible when perturbed or stressed. [Rinaldi et al., 2001] introduces three primary coupling characteristics:

[3] See also ETH-LSA report on interdependencies for FOCP, 12/09.

- the degree of coupling can be either tight or loose, e.g. a gas-fired spatial heating system without storage is closely coupled to the gas supply system without "time to give" or slack;
- the coupling order can be either directly connected or indirectly connected through one or more intervening infrastructures (second-order up to n-order effects), e.g. loss of electric power may directly affect the pumps and control of the spatial heating system and indirectly affect the fuel supply via the electrically-driven compressors of the gas supply system;
- the linearity or non-linearity/complexity of the interaction, e.g. a large-scale areal event such as extreme heat affecting various agents simultaneously.

Gaps in understanding

With regard to physical engineered infrastructures these six dimensions (type of failure; infrastructure characteristics; state of operation; types of interdependencies; environment; and coupling and response behaviour) seem to be appropriate for facilitating the identification, understanding and analysis of interdependencies, and for framing the requirements for modelling and simulation approaches. These approaches must be able to describe the behaviour of the complex system as a whole (not as the sum of its parts) as stated by many authors (e.g. [Kröger, 2008]). Unfortunately, "there are indeed gaps in our understanding of complex systems and our ability to engineer them. Specifically, general principles for engineering and analyzing complex systems are still inadequate to design and operate the complex systems in transportation, comminication and power distribution that have become part or our daily lives." [NSF Workshop, 2008]. Obviously, a combination of models following different basic approaches and working on different scales is necessary.

Based on the author's experience, network theory can provide valuable insights into the structure (topology) of networks, while agant-based modelling has proven to be promising for functional analysis and identifying (hidden) vulnerabilities. For expample, it was possible to simulate the behavior of the Swiss electric power system with regard to the sensitivity of blackout frequency versus size on intitial load conditions (Fig.2) as well as the influence of operator response to potential disruptive events [Schläpfer, 2008].

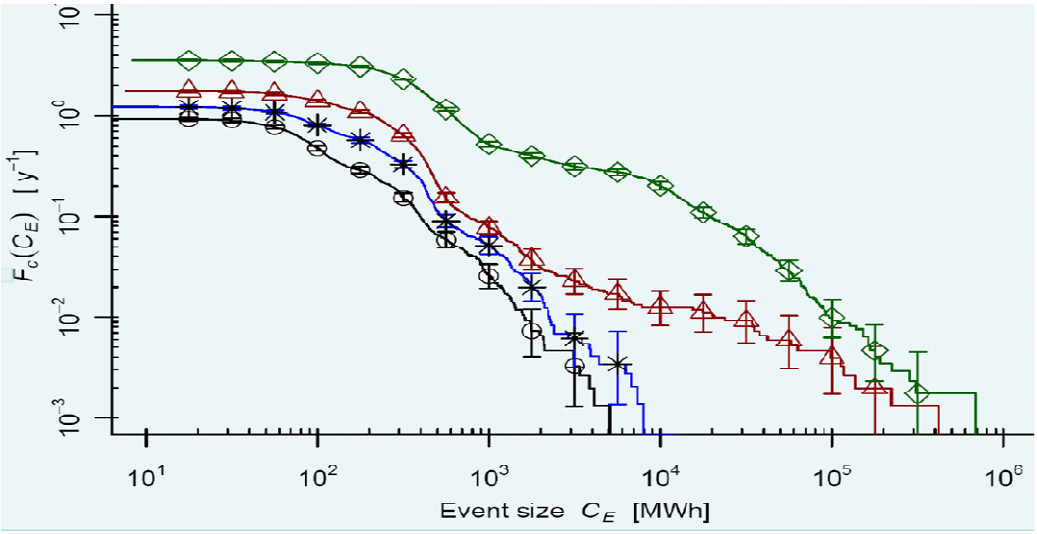


Figure 2: Complementary cumulative blackout frequencies F_c versus event size C_E for different grid load levels: 100% (circles), 110% (stars), 120% (triangles) and 137% (diamonds) [Schläpfer, 2008]

Inadequate policies and lack of concern

Besides reliability and vulnerability assessment methodologies, security policies have not kept pace with these developments and have not sufficiently reflected the new risks of disruption of continuous operation/service:

- The use of open access internet and of data and command transfer varies from country to country, which is essential for cyber security. The use of non-dedicated commercial soft and hardware may aggravate the risk of common cause failures. The merger of (still often separated) trading/business and industrial control systems may further aggravate the risks.
- The N-1 security criterion, applied to many infrastructures and limited to deterministically predefined single failures, becomes questionable as experienced events show the importance of failure combinations/cascades and "surprises".

While the systems get more-and-more stressed and the risk of system collapse is increasing, the public continues to take the services they provide for granted, treating them as common goods, e.g., electricity, mobility, data and information exchange. The potential (or realistic) trade-off between the price for a certain service and the reliability and robustness of the infrastructure is widely ignored, even in the political sphere (see [IRGC, 2006] for the EU): this lack of concern and awareness tends to result in a lack of precaution and preparedness.

Some of the risks related to physical engineered systems are known from the past, some of them are re-emerging (e.g., major blackouts), others are emerging (e.g., failure of one system snowballing unexpectedly into others, targeted massive cyber attacks). The provided set of contributing factors seems to be (at least partially) applicable to this area; see table, below.

Contributing factors

Context: System complexity

Some emerging risks are driven, positively or negatively, by the complexity of systems. Whether this emerging risk is positively or negatively driven by complexity is hard to judge. The lack of ability to understand and model complexity may attenuate the risks. The role of pervasive use of digital systems and open access, not sufficiently secured internet is of paramount importance.

Scientific unknowns *Tractable and intractable unknowns contribute to risks being unanticipated, unnoticed, and over- or under-estimated.*	• The knowledge about the risks as well as the ability to understand the complex systems and processes is incomplete and lacking behind the ability to engineer them.
Social dynamics *Risk may emerge when social dynamics change at a pace where institutions are not capable of maintaining enough stability for society to function in a fair, equitable, effective, and efficient manner.*	• Trend towards globalisation > increasing market liberalisation > unbundling of owners and operators > result is increased connectivity, interdependency and complexity, all of which have the potential to amplify risks related to large-scale engineered systems • Risk is largely ignored by society but, if it becomes tangible, e.g. via the occurrence of a major disruption, this may amplify perceived risks and promote changes in social dynamics that finally attenuate factual risks.
Technological advances *Risk may emerge when technological change is not accompanied by prior scientific investigations or post-release surveillance of the resulting public health, economic, ecological and societal impacts. Risks are further exacerbated when economic, policy or regulatory frameworks (institutions, structures and processes) are insufficient, yet technological innovation may be unduly retarded if such frameworks are overly stringent.*	• The positive attitude towards technology development employed within deregulated competitive markets combined with an ignorance of "early warnings" and scepticism may amplify risks. • Increasing dependence on technology, which is largely taken for granted > potential to amplify risks
Varying susceptibilities to risk *Risk does not affect all individuals and groups in an equal manner.*	• The whole of society/economy seems to be susceptible to this risk, at least in developed countries (countries with lower levels of development and less complex and integrated infrastructure networks will be less susceptible)
Malicious attacks *Malicious motives give rise to emerging risks and risk profiles need to consider*	• Increased use of non-dedicated commercial software and hardware and the internet in industrial control systems > increased vulnerability to cyber attacks

intentional as well as unintentional causes of risk. Malicious attacks are not new, but in a globalised world with highly interconnected infrastructures (trade, information and communication systems, etc.) they can have much broader-reaching effects than in the past.	

ANNEX 1[4]

Mini telecommunication blackout in Rome 2004

Date: January 2, 2004

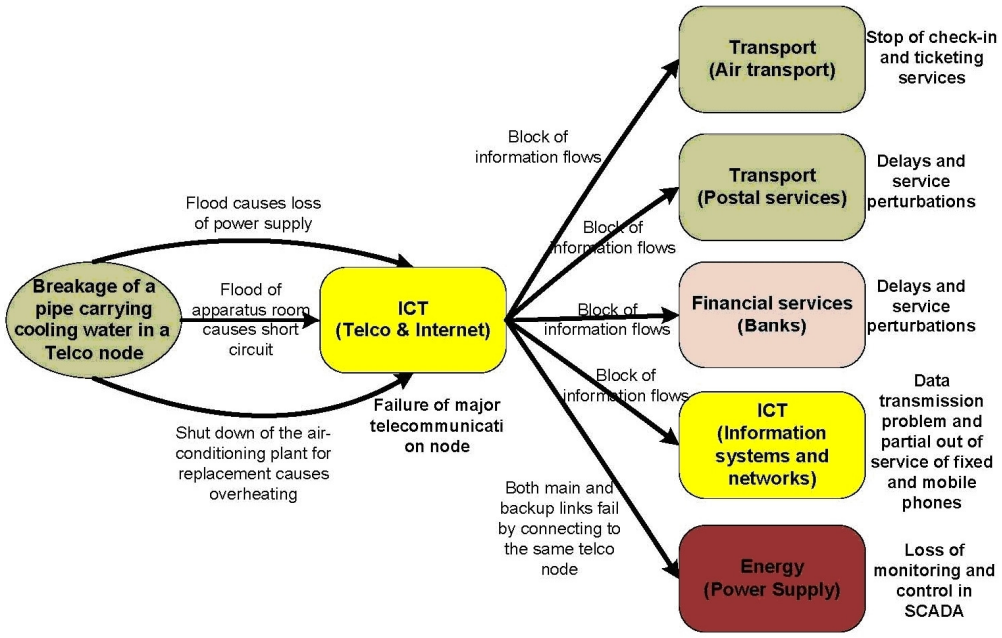
Cause and Development of the Event:

Flooding of a Telecom Italia major telecommunication service node in the Tor Pagnotta area of Rome occurred when a metallic pipe carrying cooling water for the air conditioning plant broke. The flood led to several boards/devices failing due to short circuits, and the main power supply going out of service. Diesel Generators, part of the Telco emergency power supply, failed to start due to the presence of water; only batteries provided power to the boards/devices still working; however eventually, the batteries went flat

.

The Fire Brigade arrived and worked to pump out the flood water and finally located the point of the metallic pipe breakage. To start repair actions, technicians had to shut down the air conditioning plant. Without the air-conditioning plant working, Telco node devices very soon became overheated and tilted. The mini black-out of Italian Telco infrastructure, caused problems and delays in different infrastructures, including Fiumicino airport (closure of check-in, ticketing and baggage services and transfers), ANSI print agency, post offices and banks, ACEA power distribution and the communication network (both between landlines and between landlines and mobiles) connecting the main Italian research institutions.

Affected Infrastructures/Services:



[4] ..... from Focal Report on Interdependencies, ETH-LSA for BABS (draft), 12/09

Consequences:

Impacts on ICT Sector: The mini black-out, which occurred in the Telecom Italia major telecommunication service node in Rome (the node of Laurentina-Inviolatella on Tor Pagnotta street), caused all connections to this node to fail.

Impacts on the Energy Sector: The Telco blackout of the Torpagnotta node also impacted on services of the ACEA power grid. ACEA has two Control Centres: the manned Main Control Centre (Ostiense) and the unmanned Disaster Recovery Control Centre (Flaminia). All the tele-measures, commands and alarms managed by the unmanned control centre are dispatched to the manned one using two redundant TELCO communication links at 2Mbits/sec. One is the main link, the other one is a backup link that is always in stand-by mode. Such links were expected to be located on two different geographical paths. Due to a maintenance operation, both links were traversing the same flooded node. Therefore, both links were out of service during the Telco blackout. As a consequence, there was no chance of exchanging alarms or signals on the status of the power distribution network and commands between the unmanned centre and the manned one. In such a situation, ACEA completely lost the ability to monitor and control all of the remote substations managed by the unmanned Control Centre.

The effects of the Telco black-out on ACEA (limited to the absence of the link between the two control centres that produced the uncontrollability of a large set of remote substations) started at 9.32 and ended at 10.55, lasting for a total of 1 hour and 23 minutes. The manual diagnostic and recovery actions taken by ACEA operators during the Telco Black-out made even more difficult due to the partial loss of service of fixed and mobile phones. ACEA also operates the remote monitoring and control of several power generators relying on Telco links. Such links (more than 900) were also were affected by the Telco Blackout.

Fortunately the ACEA power grid did not require any control actions by the ACEA Control Centres with respect to its RTU (Remote Terminal Unit) for the duration of the Telco black out. This was due to the weather conditions, which were very favourable during the blackout. In worse weather conditions, ACEA statistics show an average time lapse between controlling actions on its RTU, which is comparable with the Blackout duration time. In such a case, the propagation of the impact of the mini Telco black-out on the ACEA power distribution network should also be considered.

Moreover, TELCO SGT/PoP-BBN of Torpagnotta was powered by an ACEA electrical cabin, directly controlled by the manned main control centre. As stated previously, the Main Control Centre did not lose the ability to supervise or control its substations. This was a very important factor, which reduced the severity of the consequences of the Telco black-out of Torpagnotta. In fact, if the black-out affected TELCO SGT/PoP-BBN of Torpagnotta had been powered by an ACEA electrical cabin controlled by the unmanned control centre, the failure of the two redundant Telco links between the two ACEA control Centres would not have allowed the monitoring and control of such a substation, causing possible additional cascading and interdependency effects.

Impacts on Financial services Sector: Delays and service perturbations occurred at banks.

Impacts on Transport Sectors: Delays and troubles occurred at Fiumicino airport. The failure impacted the ARCO system, which supports the check-in operations of Alitalia and other airlines, which represent about 70% of the total airlines operating at Fiumicino.

Airport: During the failure, closures occurred at check-in, ticketing and baggage services as well as transfer services due to the blockage of information flows via the ARCO system. Starting from 11:04 a.m., all Airport operations were progressively restored. Delays and service perturbations also occurred at Post Office.

Other Impacts: ANSA print agency had transmission problems due to a satellite system whose connections were interrupted for a while.

Duration of consequences: The incident occurred at 5:30 a.m. From 5:30 a.m. to 10:00 a.m. battery banks partially worked. However the communication black-out started around 9:20 a.m. and ended around 11:15 a.m.

Vulnerabilities:

- The facilities and apparatus of the major Telco node were not checked and maintained carefully and regularly.
- Because of a maintenance operation, two redundant communication links between the two control centres of the ACEA power grids were actually routed through the same Telco node. When the node failed, both links failed too due to geographic common cause failures.
- Emergency power supply, such as diesel generators, was not kept safely enough and failed to start due to the presence of water.

Lessons Learned from this event

It is good for the ACEA power grid to have two redundant Telco communication links. One is the main link, the other one is a backup link that is always in stand-by mode. However, it cannot be assumed that each is always routed on a different geographical path. This assumption should be confirmed by a thorough investigation of the two redundant links. Network operators should be responsible for assuring that the redundant communication links of a critical infrastructure, like power grids, use completely disjointed geographical paths, even during a maintenance operation.

Any failure from even a small part of the apparatus in a Telco node will affect the service of the node and create further cascading impacts, which will affect the other communication networks and infrastructures. Considering the importance of a major Telco node, the security of facilities in a Telco node should be checked and maintained regularly and carefully.

Diesel-powered electric generators must be able to provide electric power when there is a failure of the primary power supply system, even if this if of short duration. For example, a diesel generator can be kept in a water-proof room and should be cleaned and maintained regularly so that it functions normally in case of emergency (dust and soot in the air may cause diesel generators to malfunction).

References:

[Dueñas-Osorio, 2008] Dueñas-Osorio, L. and Vemuru, S.V., Cascading Failures in Complex Infrastructure Systems, Structural Safety 31 (2009)

[IRGC, 2006] Kröger, W. (lead author), Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures, White paper no. 3, October 2006, Geneva, IRGC

[Kröger, 2008] Kröger, W., Critical Infrastructures at Risk: A Need for a New Conceptual Approach and Extended Analytical Tools, in Reliability Engineering & System Safety, Elsevier, Vol. 93, No. 12, 12/2008

[NSF Workshop, 2008] Guckenheimer, J. and Ottino, J.M., Foundations for Complex Systems Research in Physical Sciences and Engineering, NSF Workshop, 9/2008, http://www.siam.org/about/pdf/nsf_complex_systems.pdf

[Rinaldi et al., 2001] Rinaldi, M., Peerenboom, J.P. and Kelly, T.K., Critical Infrastructure Interdependencies, IEEE Control System Magazine, 12/2001

[Scheffer et al., 2009] Scheffer, M. et al., Early Warning Signals for Critical Transitions, nature Vol461/3 September 2009

[Schläpfer, 2008] M. Schläpfer, M., Kessler, T. and Kröger, W., Reliability Analysis of Electric Power Systems Using an Object-oriented Hybrid Modeling Approach, In: Proceedings of the 16th Power Systems Computation Conference, Glasgow, 14-18 July 2008