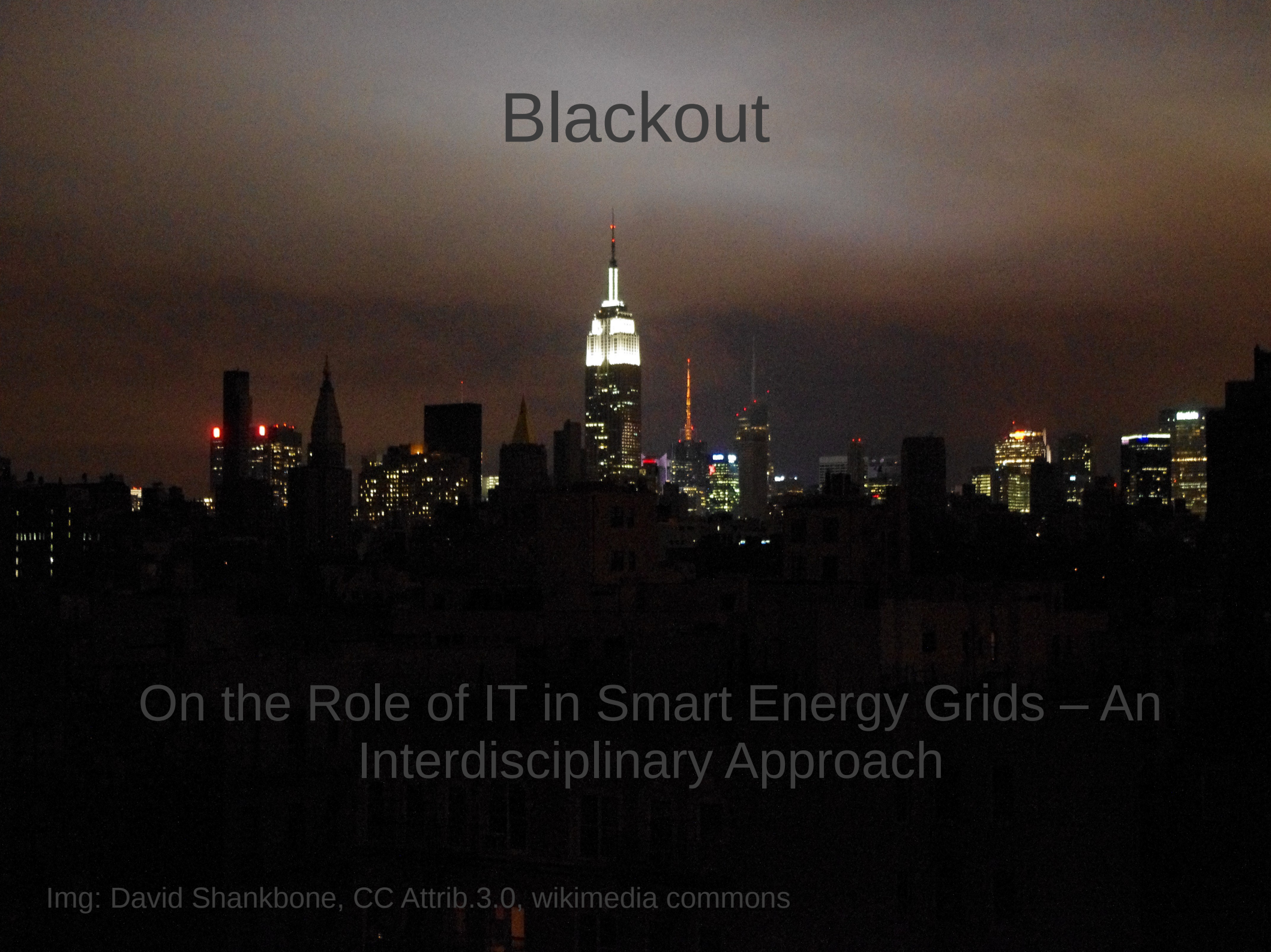
Blackout



On the Role of IT in Smart Energy Grids – An Interdisciplinary Approach

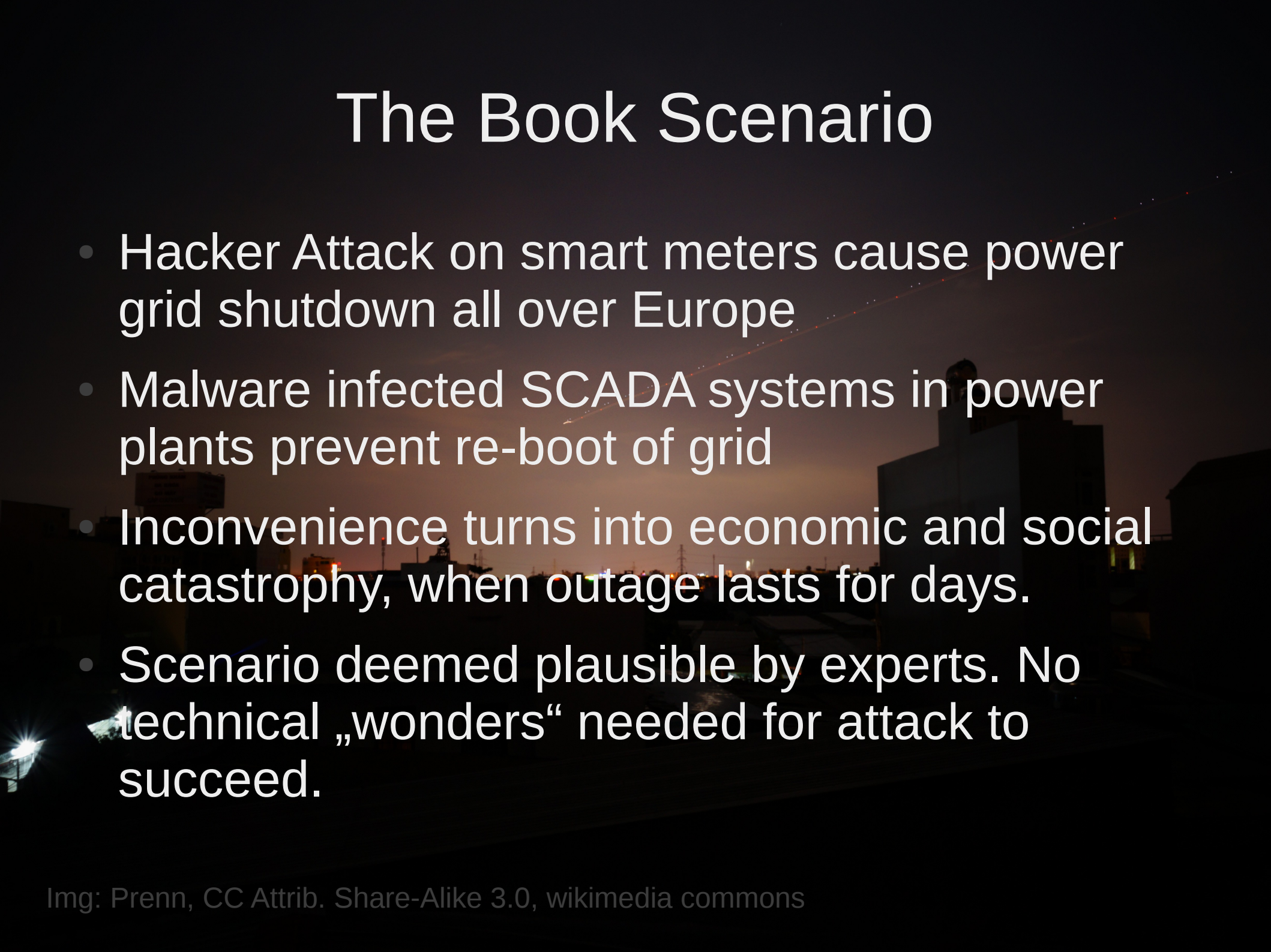
Img: David Shankbone, CC Attrib.3.0, wikimedia commons

Agenda

- Blackout Scenarios
- Power Grid Basics
- Research Motivation, Questions and Method.
- IT and Energy Ecosystems
- Some Case Studies
- Topic 1: Energy Networks
- Topic 2: Secure Components

The Book Scenario

- Hacker Attack on smart meters cause power grid shutdown all over Europe
- Malware infected SCADA systems in power plants prevent re-boot of grid
- Inconvenience turns into economic and social catastrophy, when outage lasts for days.
- Scenario deemed plausible by experts. No technical „wonders“ needed for attack to succeed.



Img: Prenn, CC Attrib. Share-Alike 3.0, wikimedia commons

Consequences

- People die (e.g. a patient in an ICU in Berlin recently)
- Cold-load pick up makes re-start hard
- Estim. 600Mio Euro/hour economic damage

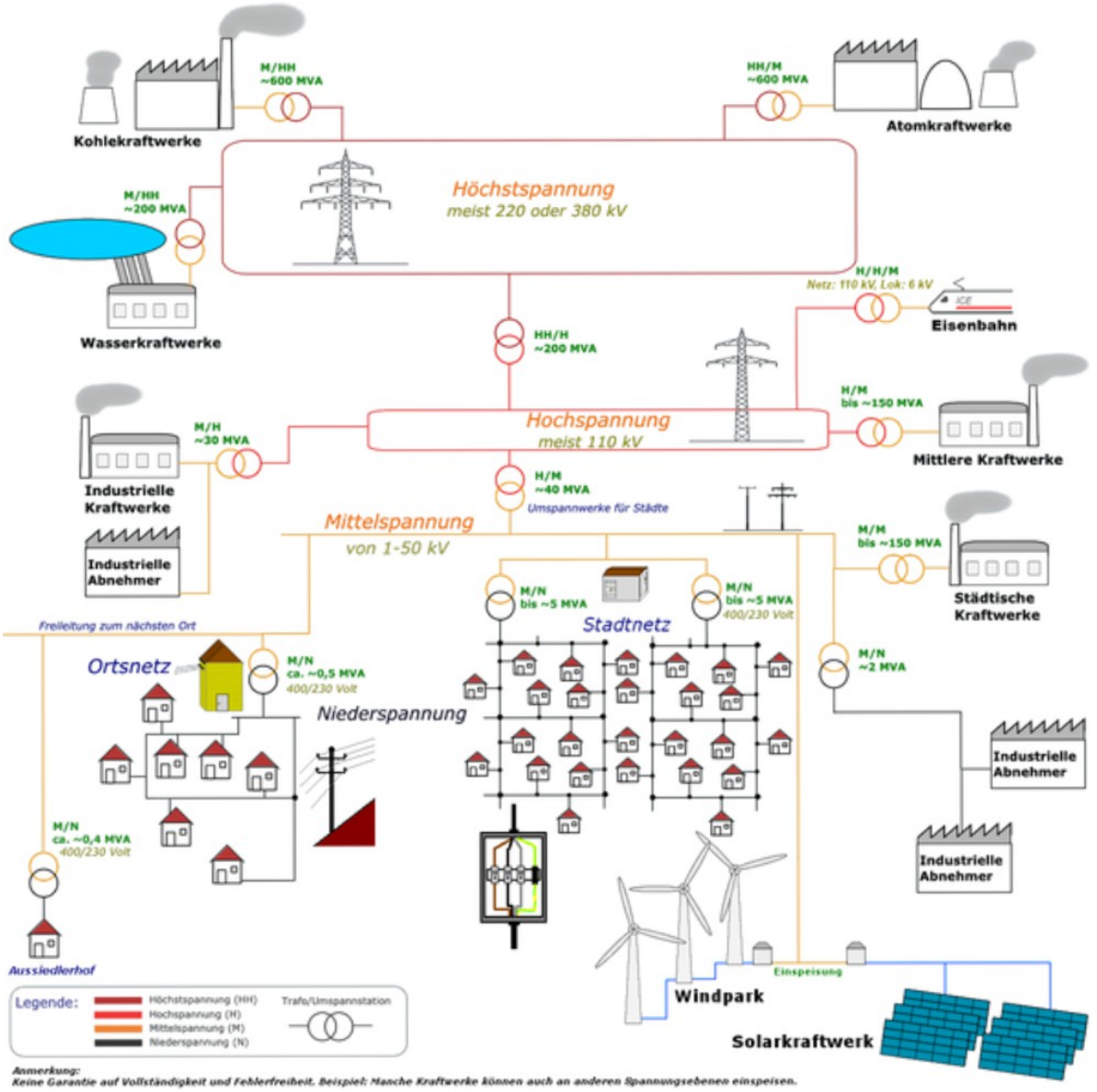
This raises questions about the fundamental approach towards catastrophes and disasters: resilience or avoidance?

Other Disaster Scenarios

- Global pandemia, results similiar to blackout
- MRSA, caused by drug abuse in food industry
- State supported cyberwar against critical infrastructures

There is a growing interest in critical infrastructures. After 9/11 „resilience“ became a competitor to „avoidance“ strategies.

Energy Transmission and Distribution



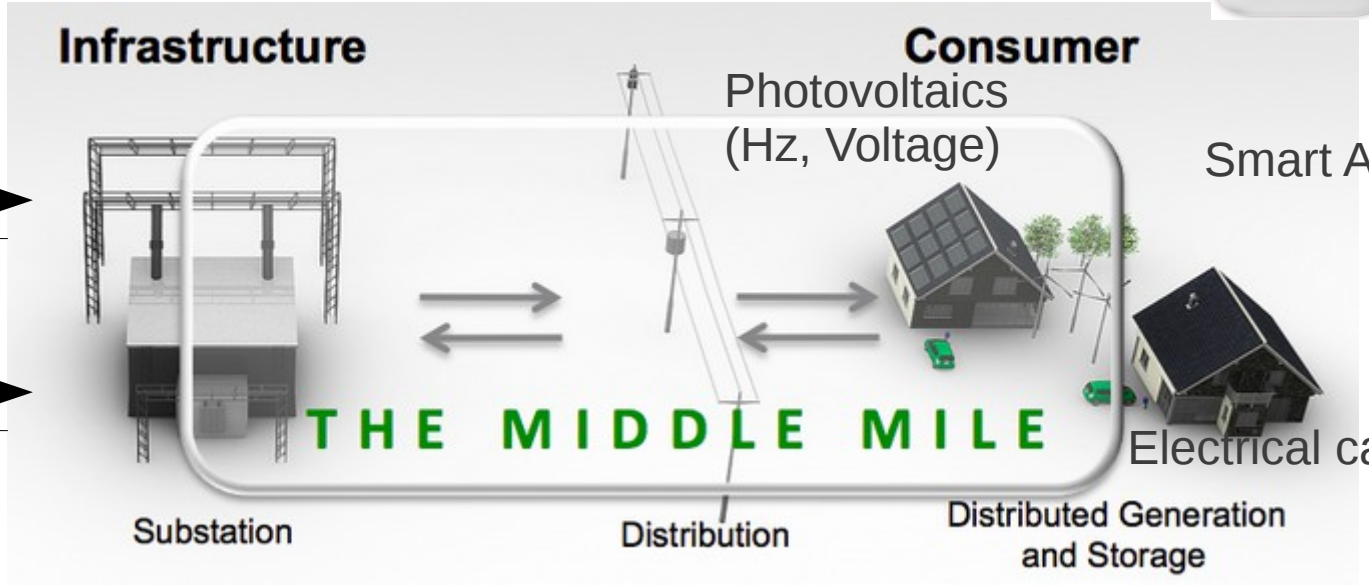
Diag: Stefan Riepl, CC Attrib. Share-Alike 2.0, wikimedia commons

The „Energiewende“

- Shutdown of nuclear facilities after Fukushima
- Consumers turn into providers of energy, causing distribution network overload. High costs of new distribution lines.
- Wind and solar energy are spiky, no storage, not enough long-distance lines.
- Enormous growth of renewable energies threatens local distribution networks. Requires dynamic control of supply and demand patterns.
- Privatized energy generation and distribution with network neutrality enforced
- Distributed production of renewable energy threatens high-equity business models

IT to the Rescue: Smart Grids

Smart meter



Power net

Control net

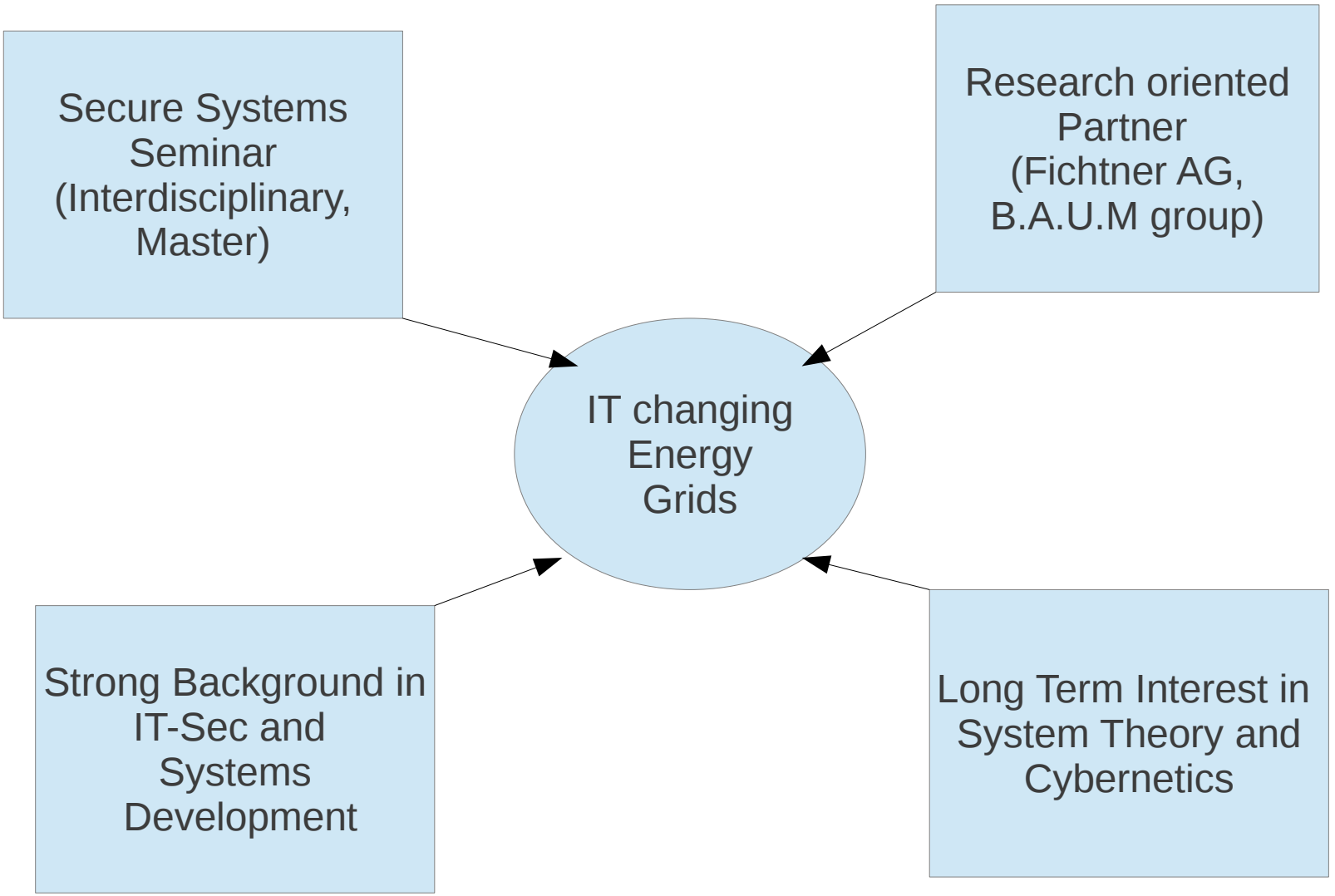
Smart Appliances

Electrical cars

Smart transformer
(Voltage, Amp)

Images:B.Zaugg, PD, Sina Luckhardt EVB Energy AG (CC Attr. Share-alike 3.0), DOE,

Research Motivation and Context



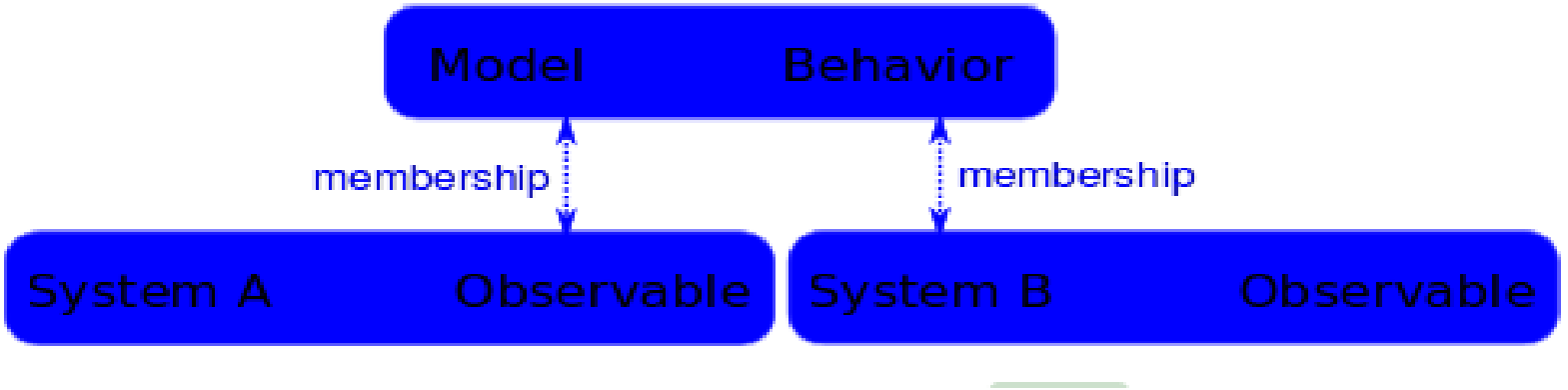
Activities

- Talk on Security at the Smart Grids Week Conference in Salzburg, May 2013
- Smart Grids Roadmap Baden-Württemberg, September 2013
- IT-Security Conference on Critical Energy Infrastructure (2014, with Energy Companies)
- Cooperation with Hochschule Furtwangen in the Area of Critical Infrastructure

Some Research Questions

- IT and Energy are different communities with very different cultures and behaviors – how will they interact? Will they repeat errors made by others?
- How does IT and IT-Security influence the techno/economic foundation of our energy systems? Are there only variables?
- What is the role of IT and IT-Security in democratic vs. centralized models of energy production?
- How does IT behave in critical infrastructures?
- Can we compare IT systems and Energy systems? Are holistic models useful? Can we transfer solution patterns from one model to the other?
- Will analogy modelling help us to find better solutions?
- How does interdisciplinary research work? Do I have to become an EE eng.?
- Can we build secure components for smart grids?
- Damage reduction strategies in IT and Energy – the right approach?

Holistic Models

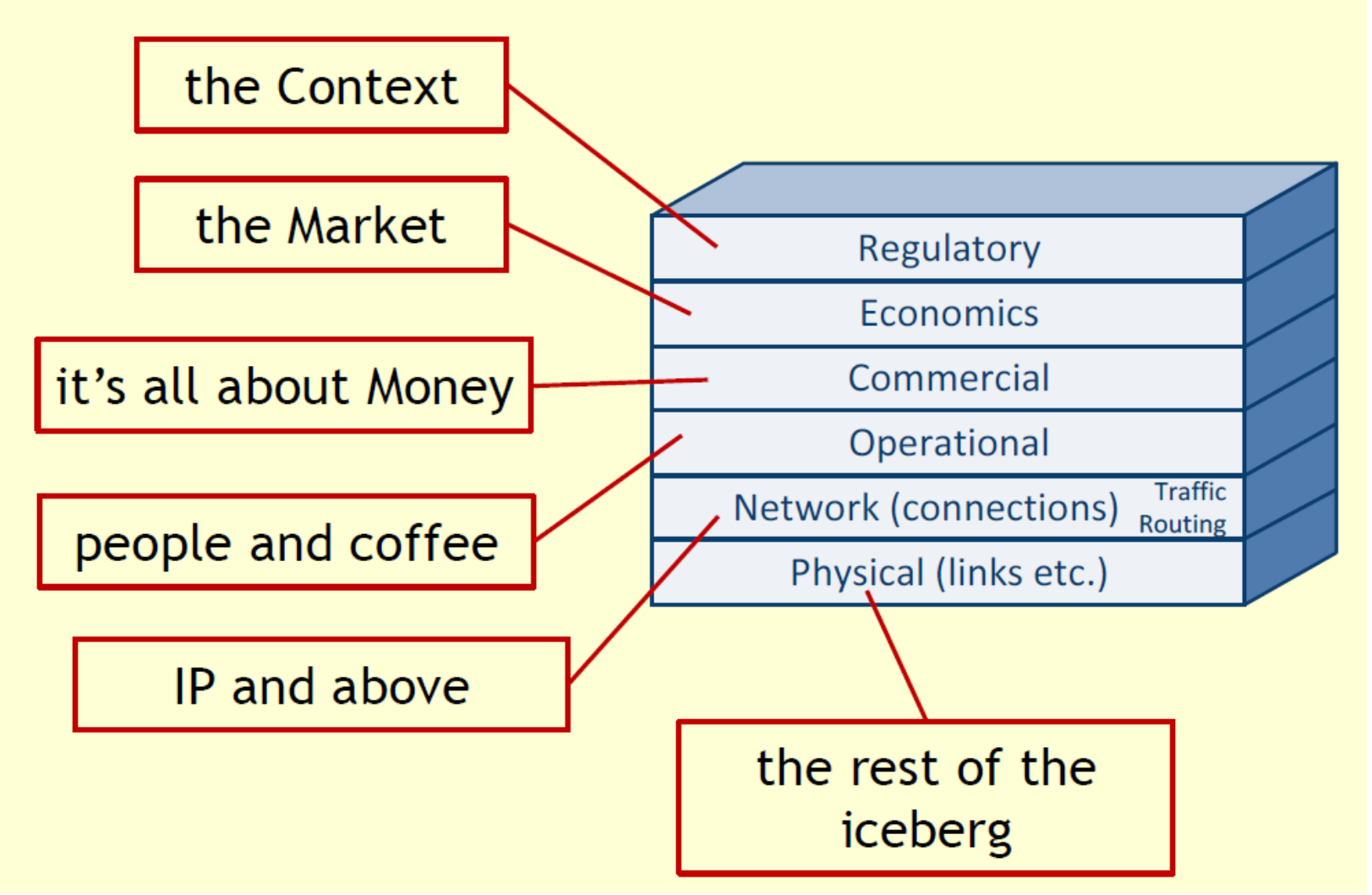


Holistic models are more focused on similarities between systems and less interested in analogous parts. A holistic approach to modeling often consists of two steps, not necessarily in this order:

- Identify a kind of behavior that appears in a variety of systems.
- Find the simplest model that demonstrates that behavior.

(from: Think Complexity, Allen B. Downey, http://greenteapress.com/complexity/thinkcomplexity.pdf)

Internet Ecosystem



from C.Hall, Summary of Inter-X Study. Network neutrality is a guiding principle.

Why is it robust (rather)?

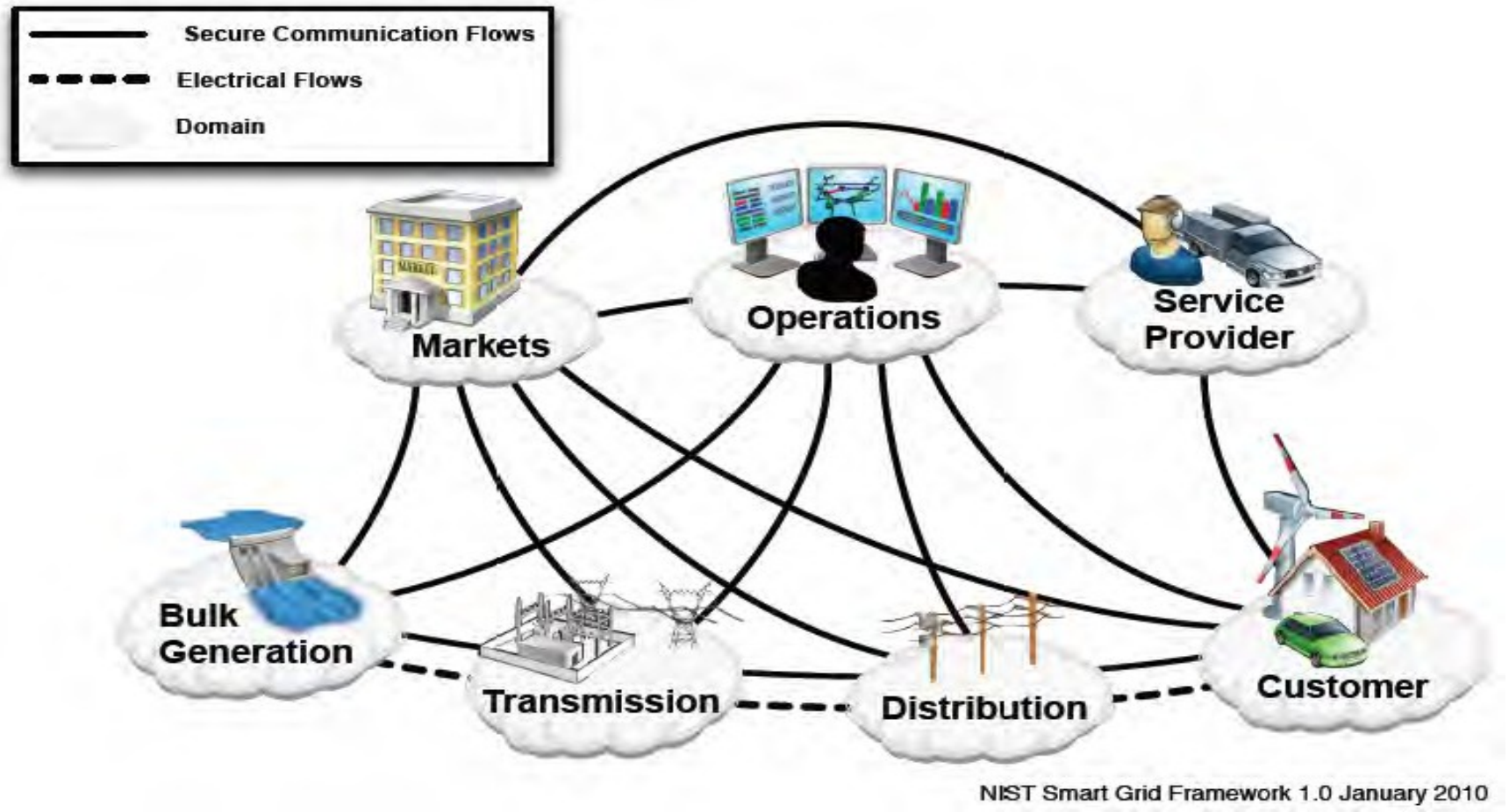
- Many IXPs (exchange points) available because there is an incentive for large providers to connect with small endpoint providers
- Many different providers are prohibiting intra-provider failures from becoming global ones
- Sudden capacity changes are not financial threats through 5% rule (providers do not have to pay for 5% overcapacity in one month. This prevents panic actions)
- Considerable amounts of spare capacity are available (overprovisioning), even though CDNs threaten both distribution of flow as well as capacity reserves.
- Routers do not provide alternative traffic information (why do I believe that this is a good thing?). No map of internet traffic routes and capacity exists.
- BGP does not influence routers in other networks
- Specialists take care of problems on a daily base, SLAs are not cross-network
- There is no global or centralized control of individual machine behavior
- TCP adjusts service to available capacity (large range of what is called „best effort“)

Attacks

- Take-over of individual end-point routers by hackers (e.g. backdoor in D-link routers)
- Take-over of end-user machines and creation of large bot-nets
- Distributed Denial-of-Service (DDOS) attacks by 10.000-100.000 machines
- Large-area power failures
- Extreme traffic spikes due to special events (Olympics, catastrophes, announcement of new Apple phones)
- Sudden disconnect of whole countries for political reasons

Those events have threatened individual sites or users, but they did not take the internet down.

Energy Ecosystem between Physics and Markets



NISTIR 7628)

Energy Ecosystem Core Properties

- Few exchange points for overflow or underflow conditions
- Hierarchically organized transmission network with many weak spots
- Strict limits for voltage, energy and frequency degradation (otherwise machine failures occur)
- No information below 20kv level
- Energy problems easily span countries
- Not an overlay network like IP

$\Sigma P \sim 0$
$f(min) < f < f(max)$
$U(min) < U < U(max)$
n-1 redundancy

There are substantial differences to the structure of the Internet. Is there still a chance to gain some knowledge from comparing the models?

Why is it robust (rather)?

- The weak points (power lines e.g.) are not known to the general public
- Modifications to local systems (e.g. transformers) frequently require manual action
- Frequency stability is/was provided through huge masses in power plants.
- Protocols used are proprietary, just as the hardware in use.
- Local shut-down procedures in case of overload
- A rather small group of electrical engineers involved (compared to the internet)
- Remote and centralized control of equipment is not ubiquitous yet
- User behavior is rather static and can be predicted easily
- A culture of dedicated specialists who want to prevent black-outs.

Lit.?

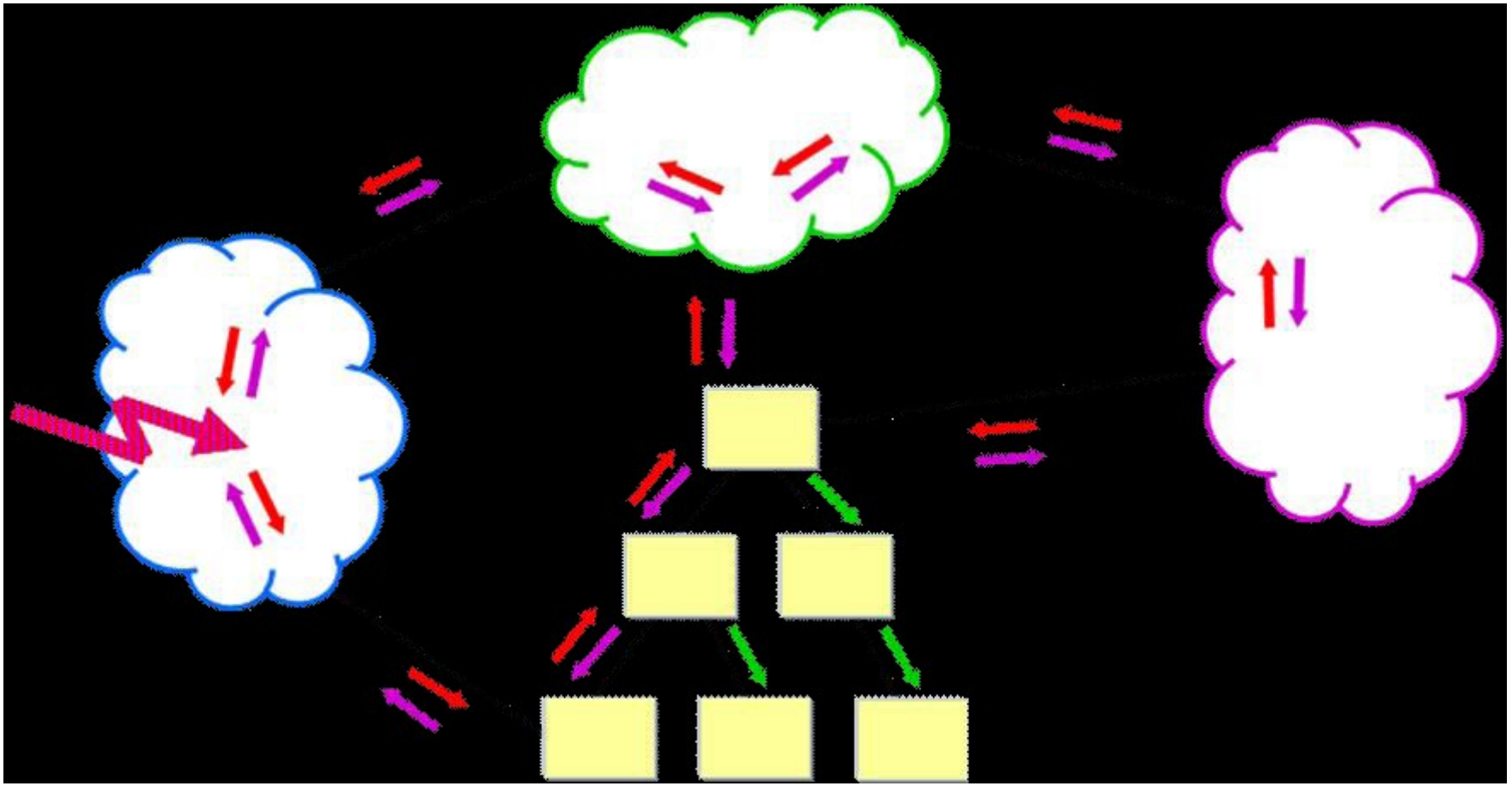
Attacks and Problems

- 50.2 Hz. problem
- Overload through alternative energies
- Virtual Energy providers/consumers through bundling
- Attacks on smart meters
- Higher level activities can crash distribution networks
- Re-start after crash can be a general problem (cold load pick-up) or one for smart grids especially (black start ability)
- Vulnerable hardware (SCADA) in power plants etc.
- Modern electronic equipment very much dependent on good energy quality.

Cases

1. Broadcast gone wrong
2. 50.2 Hz
3. Dynamic but partial control of PVSs
4. Virtual Energy Companies
5. Equipment Security

1. Broadcast Storm and Cycles



Siemens Aktiengesellschaft Österreich, CEE RC-AT IC-SG EA PRO,

A broadcast command (send report) from a gas network „escaped“ into the el. Power network. The results completely overwhelmed and crashed control stations, almost shutting down Austria (and as a consequence Germany as well).

Self-inflicted DDOS in Energy Grid

- Wrong broadcast command – missing software updates, administration error?
- Is this robustness?
- Compare to Broadcast Handling in the Internet?
- Fixes: new firmware, resets,
- What if those dangerous commands are inserted by hackers???

This incident should be reason enough, to re-think global remote control features. (see. Dr. Hein). Another lesson learned on the Internet: Crypto algorithms age fast and need to be replaced by stronger ones frequently.... (e.g.SHA-1, perfect forward secrecy)

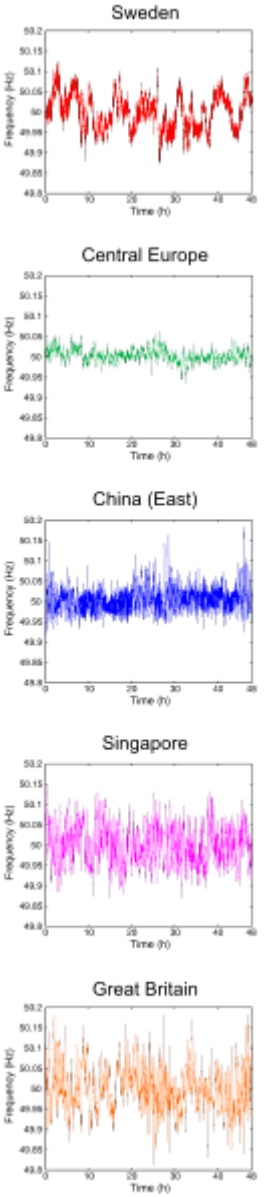
The answer from IKT recently at BaWü Smart Grid Presentation was: Yes, we can do large scale, secure remote control. Can we?

2. Distributed Solution: 50.2 Hz

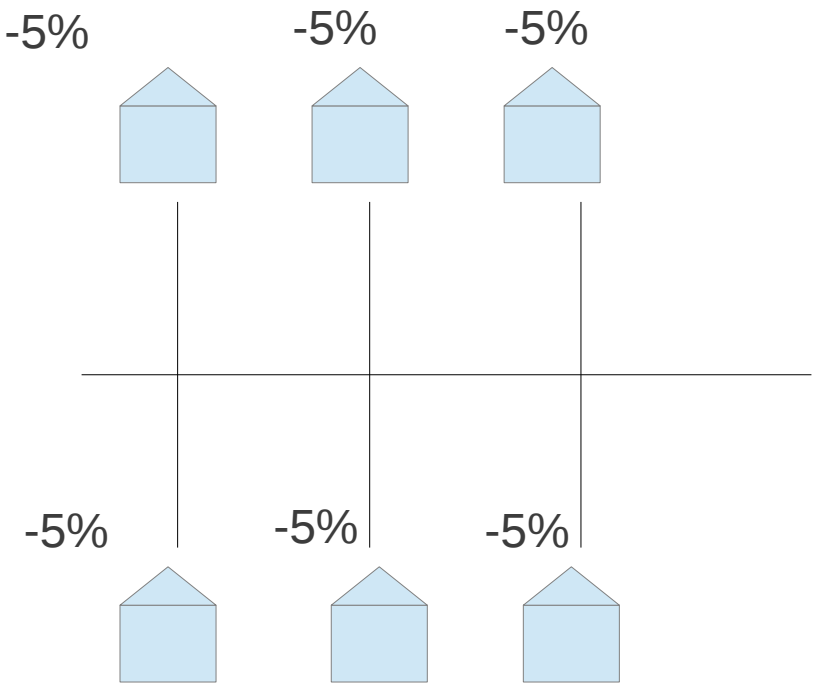
- Automatic shut-down of PVSs bring down power grids
- Solution 1: stochastic distribution of shutdown levels across systems
- Solution 2: frequency dependent load generation at local PVSs

  Forum Netztechnik/Netzbetrieb im VDE (FNN), März 2011

Analogy in IT: TCP backdown strategy, Ethernet CSMA/CD with random wait?



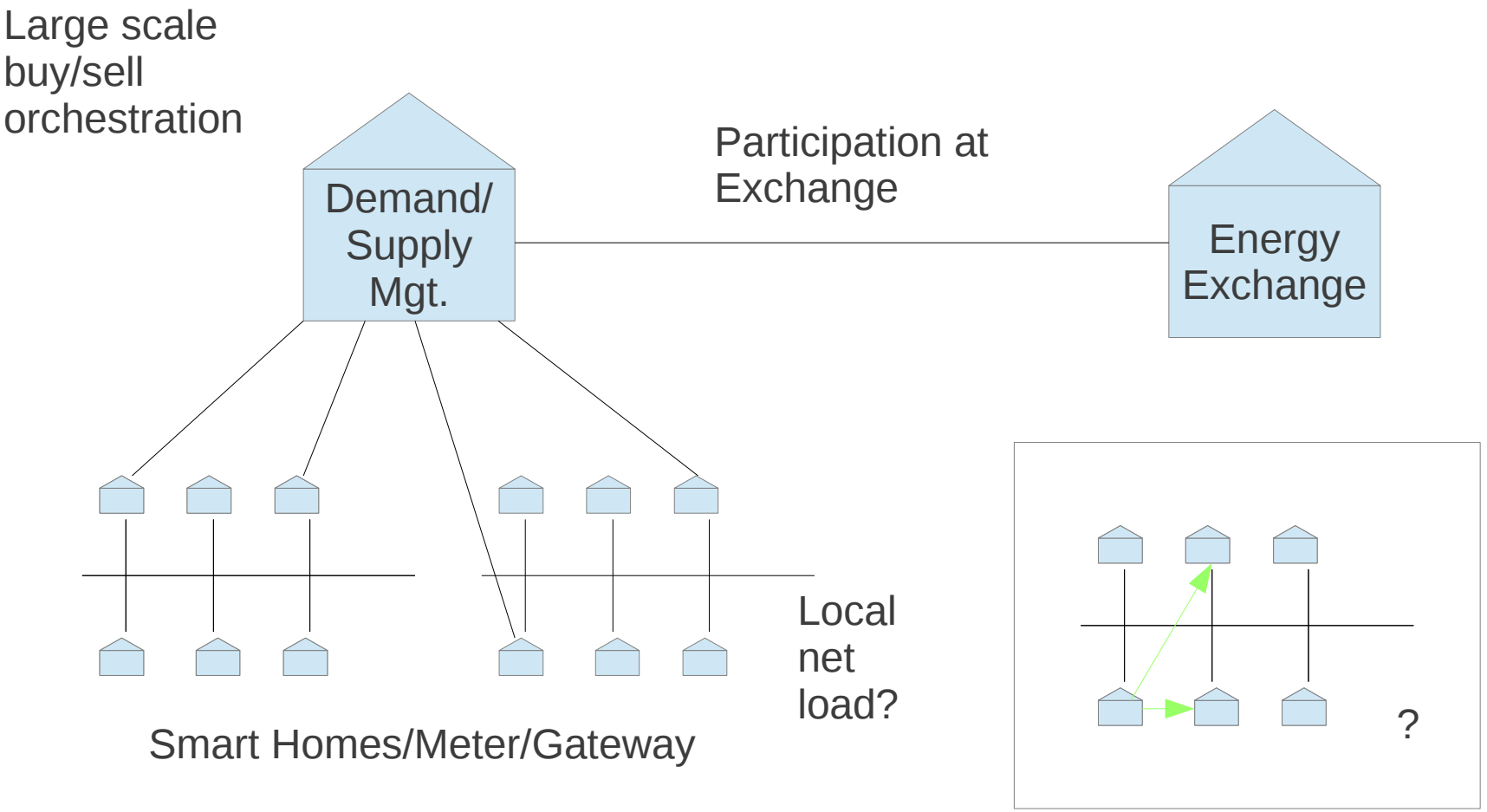
3. Controlled Reactions



Limited adjustment.
Controllable by distribution network without financial consequences

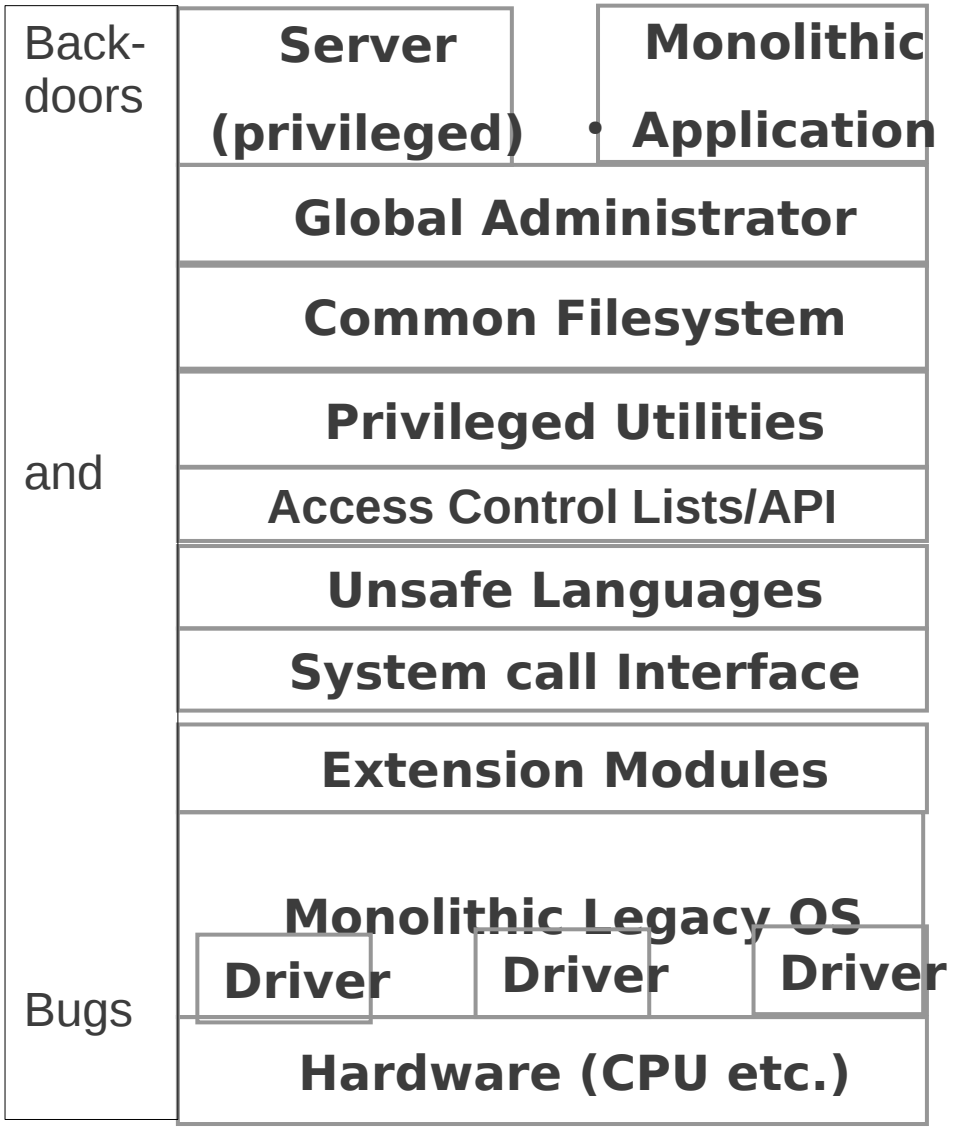
This pattern is used in the Internet to attenuate the consequences of sudden traffic increases on providers. It is also robust, as it prevents a remote access from turning off everything.

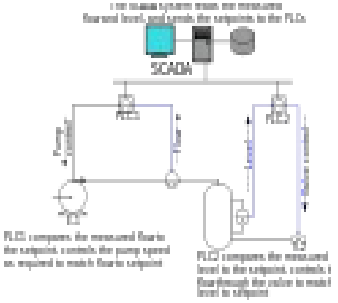
4. Virtual Energy Companies



This pattern (overlay networks) is very similiar to botnets or p2p networks on the internet. Except for the effects on the distribution network. This model does not try to stabilize or optimize the local cell. How would a robust intra/inter-cell flow of information and energy look? How would control and energy flow in a self-stabilizing cell with interfaces to other cells?

5. Can we build secure Components?





We seem to be unable to do so on the Internet. Why should the application of the same methods and technology lead to something secure in the energy sector??

Global Forces: The Axes of Evil

- State-financed IT-Terrorism (Stuxnet, PRISM, backdoors, weak crypto, government-educated hackers and hacking organizations, see http://www.zeit.de/digital/datenschutz/2013-11/nsa-infektion-netzwerke)
- Transfer of „cyber-war“ technology into the enonomic and civil area (see HBGary case)
- Security-Industrial Complex moving into society
- A very disturbing dependency between finance and security

ITK vs. EE – a Culture Clash?

- Attitudes towards disaster: acceptance, damage control (resiliance) or avoidance?
- Solutions: public vs. proprietary?
- Software Development vs. Engineering?
- Security for finance vs. security for el. Power?
- Intelligence vs. Robustness?
- Markets or Physics?

Should we build more power lines or rely on smart, dynamic control?

Model Clash?

- Are degeneration patterns compatible?
- Are the model stacks compatible? (layered vs. Self-reflexive)?
- Is network-neutrality really an option for the energy ecosystem?
- Are the edge components comparable (dsl-routers vs. Smart-meter, smart grids)?
- How big is the influence of components vs. Network structure on the robustness of the whole system?

Next Steps

- Security-Conference on Critical Infrastructure 2014
- Cooperation with University of Applied Sciences Furtwangen on Critical Infrastructure
- Step 2014
- Gametechnology for Smart Grids – Research Project

Exercise

Build a network of networks of semi-autonomous cells with a high degree of robustness. Make renewable energies and stable energy for everybody a priority. Make sure that energy is consumed close to where it is generated and make this part of the robustness. Make sure that all components are fault tolerant and that the overall network is not susceptible to DDOS attacks. Make sure that overflow energy can be transported across regions and countries. Allow use of mobile electricity and new home control systems. Allow business models and markets ....

Literature

- Ergebnisse und Erkenntnisse aus der Smart Grids Modellregion Salzburg, AIT Austrian Institute of Technology GmbH, Friederich Kupzog, Helfried Brunner et.al. http://www.salzburg-ag.at/fileadmin/user_upload/content/download/Erkenntnisbericht.pdf
- Präsentation der Smart Grids Roadmap Baden-Württemberg, Dr. Dierk Bauknecht, Öko-Institut e.V. http://www.um.baden-wuerttemberg.de/servlet/is/110756/09_Bauknecht_20130927.pdf
- Lewis J. Perelman, Shifting Security Paradigms: Toward Resilience, Critical Thinking Series (Arlington, VA: Critical Infrastructure Protection Program, George Mason University, October 2006).
- Walter Kriha, IT-Security in Finance and Beyond._Principles and Examples from Banking, http://www.energiesystemederzukunft.at/edz_pdf/events/20130514_sgw_workshop_06_kriha.pdf
- Inter-X: Resilience of the Internet Interconnection Ecosystem Panagiotis Trimintzios (Editor, ENISA), Chris Hall, Richard Clayton, Ross Anderson, Evangelos Ouzounis — April 2011 www.enisa.europa.eu/act/res/other-areas/inter-x
- Chris Hall, Summary of Inter-X Study ENISA Workshop on Resilient Interconnections Amsterdam, 21st March 2012, https://www.enisa.europa.eu
- Sandro Gaycken (2010), Cyberwar: Das Internet als Kriegsschauplatz
- Yasar Demirel (2012), Energy: Production, Conversion, Storage, Conservation, and Coupling
- Forum Netztechnik/Netzbetriem im VDE, (2011), Technischer Hinweis Rahmenbedingungen für eine Übergangsregelung zur frequenzabhängigen Wirkleistungssteuerung von PV-Anlagen am NS-Netz
- Heise News 13.05.2013, Chaos im Stromnetz, http://www.heise.de/newsticker/meldung/Chaos-im-Stromnetz-durch-verirrte-Zaehlerabfrage-1865269.html
- Dr. Franz Hein, Verantwortung für die Zukunft, Vortrag HS Albstadt, Nov. 2013