Resilience is an Emergent System Property: A Partial Argument

Bernd Sieker   Peter Bernard Ladkin

University of Bielefeld and Causalis Limited

February 2016

Systems[1]

Some systems mentioned in this presentation

- The London Heathrow crash of BA Flight 38 (Boeing 777)
- The Human Body (briefly)
- The financial system built on mortgage equities (briefly)
- Various electricity grids (European, Swiss Railway, North American)
- Air Traffic Control (briefly)
- Autobahnen/freeways/motorways and mass-collision accidents

- The first examples are by way of introduction to phenomenology
- The last three constitute infrastructure

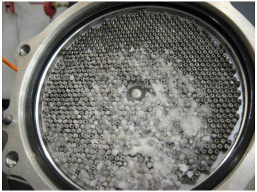
Systems

Basic vocabulary:

- **System:** collection of objects
- ..... with mutual behaviour
- **Behaviour:** change of state
- **State:** properties of objects and relations they have with each other

This suffices as a framework for ontology. Does not magically tell you the things you want to know, such as causal influences.

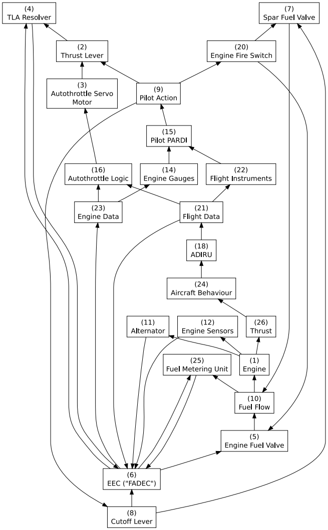
System Operation: Going Wrong in the Large



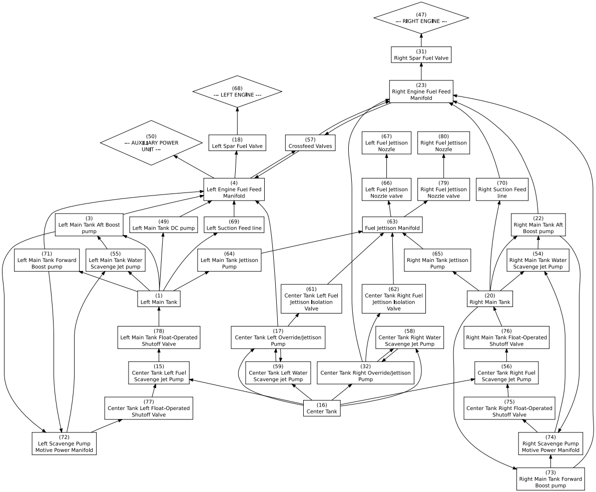
What Happened?

- Insufficient fuel flow on short final
- No physical blockage found upon inspection: ice formation suspected
- Maybe due to unusually cold fuel and atmospheric water vapour at lower altitudes
- Nothing had been broken: Main causal property was *emergent*

Boeing 777 Fuel System: Causal Control Flow Diagram

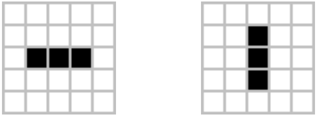


Boeing 777 Fuel Flow

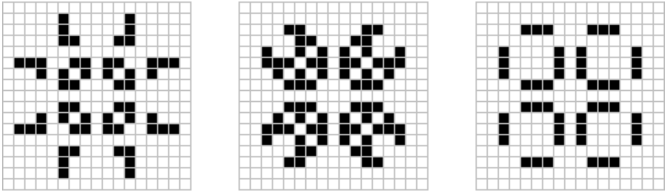


John Conway's *Game of Life*[2]

- two-dimensional grid, discrete time, very simple rules
- emergent properties



Graphic: Wikimedia under Creative Commons



Graphic: Wikimedia under Creative Commons

Speaking of Life: The Human Body

- Large collection of mutually-dependent organisms and subsystems
- If they all die off, your body stops working, for example *digestion*
- very resilient to many small and moderate disturbances, *self-healing*
- *ill* and *well* are emergent properties, described on the phenomenological level
  - the beginnings of a cold
  - runny nose
  - inflamed throat
  - .... which goes away
- much of biomedicine is oriented towards discovering the biological causal basis of these emergent ill/well phenomena
- in engineering, we often have the inverse problem
  - we know the intricate workings in detail
  - we know the emergent properties hardly at all

The Housing Market

- Mortgages were packaged into derivatives
- Those derivatives were sold on
- It became hard to tell what assets were secured and how
- It became hard to tell, ultimately,
  - who could "call in" a loan
  - what security could thereby be appropriated
  - how the security could be divided amongst the creditors
- ... and this not only in the original "repackaged" assets, but also in their derivatives
- since these three matters constitute the risk in a financial instrument, it followed that risk could no longer be assessed

The Housing Market II

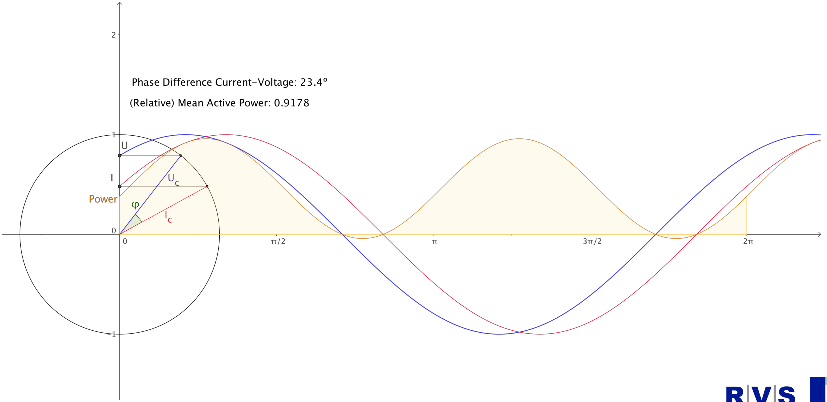
- The larger market is way larger than the US sub-prime mortgage / derivatives market
- If risk can no longer be consensually assessed in existing contracts, then
  - contractual parties can no longer be assured that counterparties can meet their obligations
  - which entails that the risk of new contracts, of whatever sort, can also not be assessed
  - which in turn entails that people are unwilling to make new contracts
  - which in turn entails that the financial market in general reduces and/or collapses
- When the risk in US subprime derivates became no longer assessable, then general market risk became no longer assessable

Emergent System Properties

- *Key observation*:
  it turned out that risk is an emergent property of such markets
  - rather than being an objective property set by established rules
- market-confidence and trust are emergent properties of such markets
  - both causally dependent on perceived-objective determination of risk
  - but also on other factors

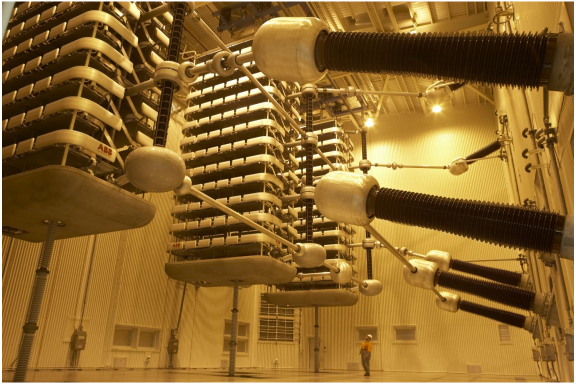
Electricity Grid — Physics I

- Synchronised AC network
- Frequency differences lead to phase differences
- phase differences lead to blind power and reactive power



Electricity Grid — Physics II

- Historic reasons for AC use: much easer to transform voltages
- Still requires huge efforts to convert high-voltage AC↔DC



Electricity Grid — Switching, Monitoring and Control

- High voltage more efficient for transport — low voltage easier and safer to handle for consumers
- Current flows following the laws of Ohm and Kirchhoff laws
- Cross-border-, and inter-company flows are negotiated on free market
- Lines can be switched, generation stations can be turned on and off and regulated
- In an emergency, consumers can be disconnected to preserve grid stability

The European Blackout 4 November 2006[3, 4]

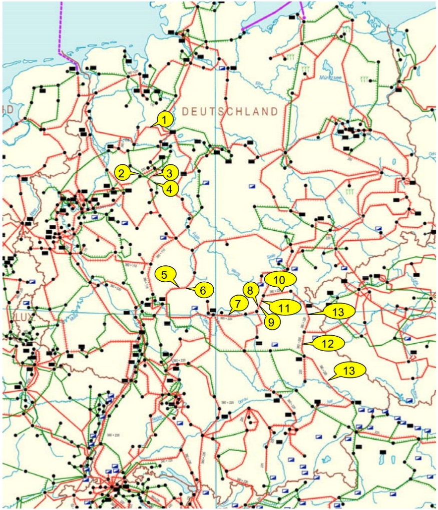
- 15 millions cut off from electricity
- European grid split into three parts
- Triggered by turning off of a 380kV line across the river Ems
- Line turned off to let cruise ship pass

European Blackout — Summary

- Grid operator erroneously assumes grid to be stable with the line turned off
- N-1 criterion was not (re-)checked
- Miscommunication and lack of cross-checking lead operators to make other adjustments
- Many more lines trip in quick succession

Tripping Cascade

Nr.	Zeit	kV	Leitung
1	22:10:13	380	Wehrendorf-Landesbergen
2	22:10:15	220	Bielefeld/Ost-Spexard
3	22:10:19	380	Bechterdissen-Elsen
4	22:10:22	220	Paderborn/Süd-Bechterdissen/Gütersloh
5	22:10:22	380	Dipperz-Großkrotzenburg 1
6	22:10:25	380	Großkrotzenburg-Dipperz 2
7	22:10:27	380	Oberhaid-Grafenrheinfeld
8	22:10:27	380	Redwitz-Raitersaich
9	22:10:27	380	Redwitz-Oberhaid
10	22:10:27	380	Redwitz-Etzenricht
11	22:10:27	220	Würgau-Redwitz
12	22:10:27	380	Etzenricht-Schwandorf
13	22:10:27	220	Mechlenreuth-Schwandorf
14	22:10:27	380	Schwandorf-Pleinting



Universität Bielefeld
RVS Rechnernetze und Verteilte Systeme
CAUSALIS

European Blackout — Consequences

- Prior to the final tripping of the lines frequencies oscillate
- Grid is split in three, frequencies drift apart
- Consumers in part with under-production have to be disconnected

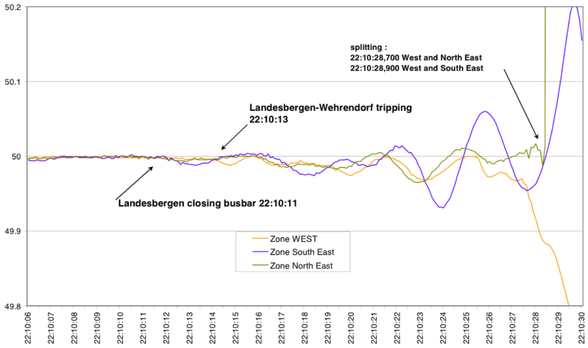


Figure 5: Frequency recordings until area splitting

Figure 6 is presenting frequency recordings as retrieved by Wide Area Measurement Systems (WAMS) in the three areas from 22:09:30 to 22:20:00

Universität Bielefeld
RVS Rechnernetze und Verteilte Systeme
Causalis

Frequencies — Oscillation, Split, Drift

Just after the split, frequencies quickly drift apart from the nominal 50Hz, precluding a quick reconnection.

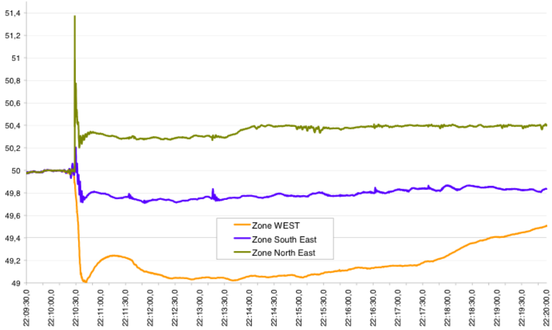


Figure 6: Frequency recordings after the split

The N-1 Criterion

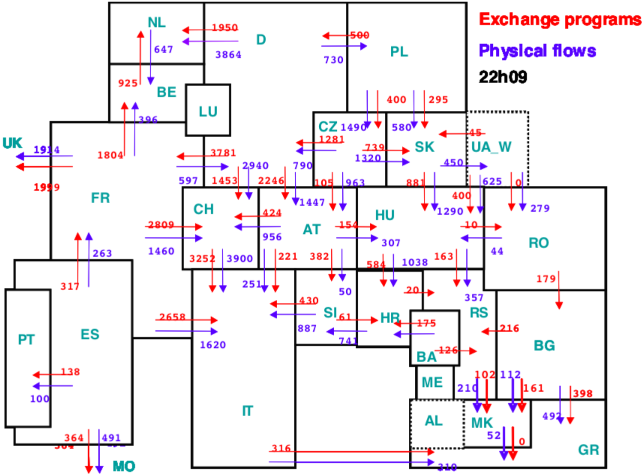
- Described in Operations Handbooks
- States that the net must tolerate failure of one major component and still work securely
- Regulations stipulate that N-1 criterion has to be met at all times
- No detailed description how to guarantee N-1 safety, or how often to perform calculations
- Insufficient specification

Checking for N-1 Safety

- RWE
  - has automated system that performs N-1 calculations every 15 minutes automatically
  - Personnel can easily trigger additional calculation runs
- E.ON
  - No automated system
  - Personnel have to initiate calculations manually
  - Left to Dispatchers' discretion when to perform calculations

Interconnected European Power Grid

- Unevenly distributed generation and consumption
- High-cross-boundary flows of power
- Use of AC requires frequency synchronisation



System Properties

- The European grid was divided into three parts
- Demand is variable, supply sources are regulated as required
- Very short regulation: physically, ca. 10 seconds, change in rotational energy
- After that: primary power regulation, partially automated
- Manual switching when required

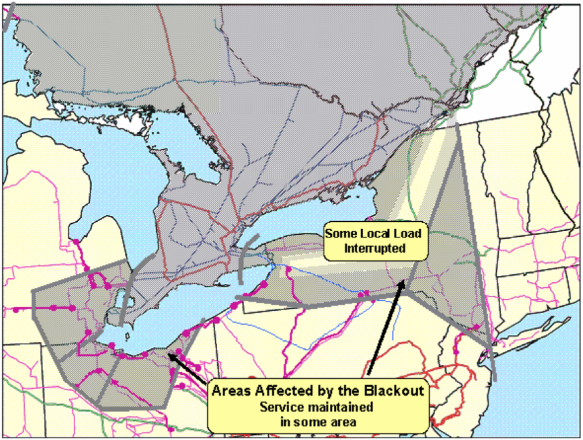
System Properties II

- Computer-assisted flow analysis was available
- Was started automatically at some operaters, not at others
- System is physically resilient only for very short time periods
- After that, frequencies drift too far apart
- Primary power regulation usually automatic in large power stations
- Further actions usually done manually, but rely on accurate and current information

Observations

- Current information of all settings is required
- This information must be coherent among co-operating operators
- Here, neighboring operaters used different cutoff loads for the same line
- Load-redistribution cannot be predicted intuitively
- Available computer assistance was not properly regulated and not used appropriately

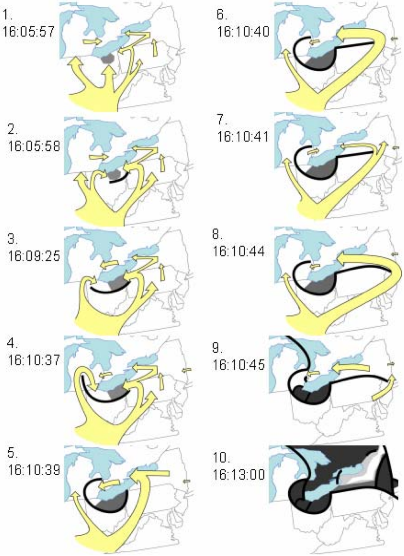
Other Grid Collapses: North American Blackout, August 2003[5, 6]



Graphic: North American Electric Reliability Corporation (NERC)

Power Flows Before the Sammis-Star 345kV line trip

Graphic: NERC

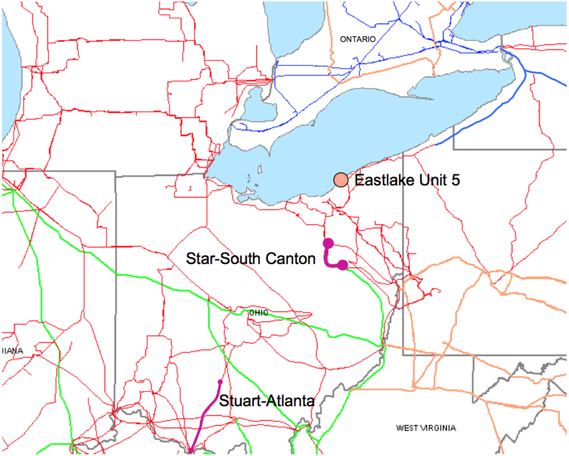


Universität Bielefeld

RVS Rechnernetze und Verteilte Systeme

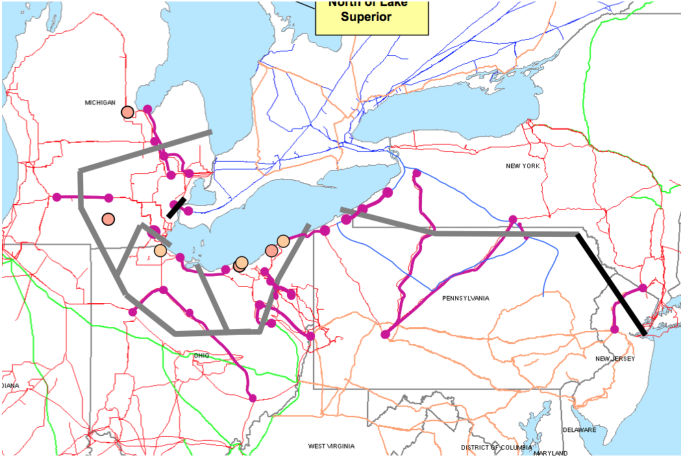
CAUSALIS

Some Initial Trips Due to Demand from Cleveland-Akron



Graphic: NERC

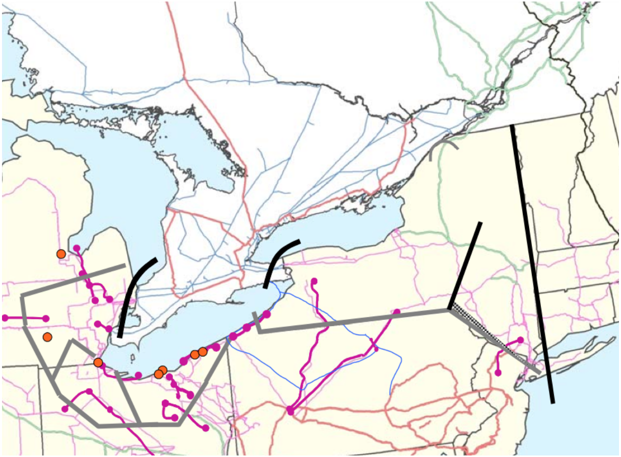
Several more lines trip in succession



Graphic: NERC

NY and New England Separate; Multiple Islands Form

... and eventually



Graphic: NERC

Universität Bielefeld
RVS Rechnernetze und Verteilte Systeme
CAUSALIS

System Properties

- The North American grid was divided into three parts, Eastern, Western and Texas
- The balance is maintained manually, continually, correct and current information is essential
- stability is defined as having enough resources on-line, in the right places, to satisfy demand
- One operator lost situational awareness
- Computer assistance was inadequate and not used appropriately

Observations

- it seems evident that, had the computer systems worked as intended, grid functionality could have been maintained
- *Key observation*:
  by the Counterfactual Test, the computer failures were causal
  - the computer systems could/should have been designated critical and designed/maintained accordingly

Other Grid Collapses

- The Swiss Railway grid collapsed completely in June 2005 - in 8 seconds elapsed time
- Selected phenomena:
  - the ostensible cause is implausible:
    - very many trains with regenerative braking putting energy into the system simultaneously in one section
    - there does not, however, seem to be any other, more plausible, explanation of the sudden imbalance
  - handling and recovery required all error messages to be manually acknowledged before display refreshed
    - they were coming in way faster than they could be ACKed
    - ⇒ no current and accurate information was available to operators
- WBA by Casten Weber, November 2005

Air Traffic Control

- Normal operation relies on:
  - Secondary Surveillance Radar
  - Radio telephony
  - Co-ordination with adjacent regions / countries
  - Well-trained personnel with good situational awareness
- So far, traffic density is such that the system appears to be resilient to
  - failures of radar coverage in one region
  - failure of main radio system
  - failure of computer systems
- Area can be cleared under contingency protocol
- with backup radio
- with help from adjacent regions
- unclear how resilient it will be with higher traffic density

Mass Motorway Collisions - Auffahr Accidents

- a motorway with non-negligible traffic
- a sudden patch of low visibility
- a mass collision involving tens to nearly hundreds of vehicles

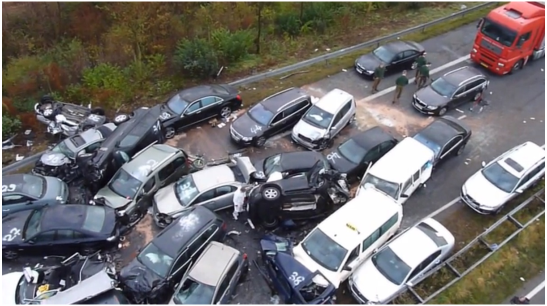


Photo: Uwe Renners (from YouTube video)

Mass Motorway Collisions - Auffahr Accidents

- such auffahr accidents have been regularly occurring for over fifty years
- the "authorities" always search for someone to blame
  - some driver or drivers behaving inappropriately
  - in this case, it was minor - a minor fender bender in fog
- *Key observation*:
  propensity for such accidents is an emergent property of the system
  - they can occur when every driver makes the most rational individual decision given the observable state
  - mostly they don't occur - the unobservable system state is favourable
  - when the system state is unfavourable, they almost-inevitably occur
- auffahr accident analysis by Ladkin, 2011[7]

References

[1] Peter B. Ladkin.
Formal Concepts of Systems, chapter 3: Foundation of system analysis.
2001.
http://www.rvs.uni-bielefeld.de/publications/books/CausalSystemAnalysis/.

[2] E. Berlekamp, J. Conway, and R. Guy.
Winning Ways for your Mathematical Plays, volume 2.
Academic, 1982.

[3] E.ON Netz GmbH.
Bericht über den Stand der Untersuchungen zu Hergang und Ursachen der Störung des kontinentaleuropäischen Stromnetzes am Samstag, 4. November 2006 nach 22:10 Uhr.
Technical report, E.ON Netz GmbH, Nov 2006.

[4] Bundesnetzagentur.
Report by the Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railways on the disturbance in the German and European power system on the 4th of November 2006.
Technical report, Bundesnetzagentur, 2007.

[5] North American Electric Reliability Council.
Technical analysis of the august 14, 2003, blackout.
Technical report, NERC, Jul 2004.
http://www.nerc.com/docs/docs/blackout/NERC_Final_Blackout_Report_07_13_04.pdf.

[6] North American Electric Reliability Council.
Joint us-canada task force report, 2004.
http://www.nerc.com/pa/rrm/ea/Pages/Blackout-August-2003.aspx.

[7] Peter B. Ladkin.
The assurance of cyber-physical systems: Auffahr accidents and rational cognitive model checking, 2011.
http://www.rvs.uni-bielefeld.de/publications/Papers/20111230CPSV2.pdf.


Thank You for Listen- ing!
Ques- tions?