The Limits to Digitalization

The (forgotten) value of analog fallbacks & control mechanisms
Countries that built complete analog physical plants have a signal advantage over countries that leapfrogged directly to full digitalization.

Dan Geer
The current situation

• Everything is getting connected, “smart” & digitalized
• Control in more and more areas is continuously “handed over” & shifted to digital technologies
• Growing societal dependence on their reliability & correct working
• Lots of (hidden) fragility introduced since digital technologies often possess hidden interdependencies & SPOFs
• Risk of attacks & cascade failures is constantly increasing
• Cyber hygiene is critical but not always enough
• Loss of sovereignty & maintainability (think right to repair)
• Analog (fallback) mechanism resp. layers are decommissioned or are not maintained & rot
The idea

• There is a huge **value in simplicity**
  o Complexity is the worst enemy of security\(^1\) – Bruce Schneier

• Analog & manual mechanisms can offer a **higher level of resilience**
  o Due to being simpler, easier to understand, less interdependent, more repair friendly, slow & visible degradation before failure...

• There exists a (forgotten) **value in preserving** (or reinstating) analog (control) **mechanisms**

• **Critical processes or goods**\(^2\) should not solely rely on **digital technology**
  o Analog mechanisms & **fallbacks** should exist to ensure a minimum “service” level can be upheld in adverse or **crisis situations**
  o **Digitalization is no end in itself** – not everything has to be digitalized!

---

1) The same thought also applies in a broader context to resilience!
2) Also think of societal processes like elections or public goods like cash, emergency notification systems etc.
Is this idea entirely new?

- No – e.g. Dan Geer, Andy Bochman, Ralph Langner, Richard Danzig
- **Securing Energy Infrastructure Act** 2019 (USA)
  - Two-year **pilot** program to research & test solutions, including **analog** and **nondigital control systems**
There exists proven value of analog fallbacks

- Serious **security incidents** (e.g. Norsk Hydro, Salzburg Milch) have shown the value of being able to – to some extent – **keep production running** in a non digital technology dependent way.

Inside Norsk Hydro, the internal response focused on multiple fronts. They launched old-school methods to resume full production and repair business operations. And they worked to protect the safety of employees and the environment. The entire workforce did their jobs with pen and paper during the attack’s first days. Some plants switched to manual procedures to meet manufacturing orders. Retired employees – familiar with the old paper system – volunteered to return to their plants to keep production rolling.

"Dass wir noch einen Fuß in der von uns selbst oft kritisierten vordigitalen Welt hatten, hat uns gerettet"

Florian Schwap, Prokurist und Kommunikations-Chef von SalzburgMilch

Problems due to lacking fallbacks

• Colonial Pipeline 2021:
  o OT network **unaffected by attack**. Nevertheless fuel delivery stopped – supposedly due to dependence on billing system which was placed in IT network

• Facebook outage 2021:
  o Some reports that employees were **not able to enter buildings/server room** due to problems with the **access control system** (no [?] or not working offline mode)

• Maersk & NotPetya 2017:
  o No **offline Backup** of the Domain Controller. Saved by DC in Ghana which was offline due to a local power outage.
Problems due to lacking fallbacks II

• **Tesla** cars
  - Two incidents where drivers were trapped in fire due to failure of automatically activating (exterior) electronic **door handles**

• Faking iPhone restart due to all **controls becoming software controls**
  - No more **physical buttons**. Almost no more USBs with manual write blocker
  - Malicious BIOS/firmware updates could be thwarted via hardware jumper

• **John Deere** tractors
  - Restricted access to hardware & software, only usage of coupled resp. registered machine parts possible, right to repair? **Remote bricking** possible (Ukraine 2022)

• **“Smart” gun**
  - Secured from usage by unauthorized person via RFID watch – **jamming** possible

• Cloud-only controlled **IoT Systems**...
Aurora Generator Test 2007

- INL shows that cyberattack can destroy physical components
- Used a program to rapidly open and close a diesel generator's circuit breakers out of phase from the rest of the grid,
- Caused abnormal torques and ultimately causing it to explode

- I can deal with disruption – what I can't handle is destruction of long lead time to replace capital equipment (e.g. like transformers etc.)

CEO of a Florida power company. Book Interview Countering Cyber Sabotage Introducing CCE (34:00)
Cases proving value of manual or analog means I

• **Ukraine power outage** 2015 & 2016
  - Manual control capabilities important to resolve power outage

• **NHS**
  - Usage of “outdated” **fax machines** during WannaCry incident

• **PLCs & Safety** Instrumented Systems **Controllers** with **external switch** (e.g. key) for maintenance/troubleshooting
  - If key is not turned no firmware upload/logic change possible

• **FAA recommendation for pilots**
  - Spend **less time using autopilot** to **maintain & hone** their **practical skills**

• “**Old-school**” **paper based elections** (at least in Austria)
Cases proving value of manual or analog means II

- US Navy
  - Replacing Tablets with buttons & levers due to increased danger of accidents
  - Starts teaching navigation by the stars again
- Usage of analog mechanical typewriters & paper documents (e.g. Bundestag's Confidential Committee)
- Meeting in person (without electronic devices) for confidential discussions
- Cash
- Printed Books
- Military carrier pigeons in the era of electronic warfare
Examples for analog control mechanisms & fallbacks

• Analog safety systems
  o E.g. relief valves, rupture disc, elevators, traffic lights

• Speed regulator/mechanical governor
  o Limit engine to a certain speed so that device can’t kill itself (think of Stuxnet)

• Analog hardwired vibration or speed sensor
  o To automatically trip off a system if it is in danger of killing itself

• Independent monitoring
  o Get humans acting as independent monitoring/control mechanism back in the loop (e.g. to monitor a mechanical pressure gauge or thermometer to verify trustworthiness of digital information – think of Stuxnet again)
Example: Spring Based “Cyber Secure” Device

- Simple, **spring-based design** can be used to **prevent** hackers from getting the **centrifuges** to **spin too fast**
- As a spinning object gains speed, a spring with a weight at its end will be pulled toward the system’s edge by the centrifugal force
- When the spring reaches the point defined as the maximum speed, it **trips a relief valve**, venting steam or whatever powers the mechanism
- That’s a design that **cannot be hacked**
Challenges & Limitations

• Only makes sense for certain kind of organizations & processes

• Economics
  o **Cost**\(^1\) & **efficiency**, misaligned incentives, short term thinking, no policy requirement, hard to sell – perceived as “old-school”

• Operational
  o Enough **people** available to control via analog means?
  o Still enough **knowledge** & confidence how to do it the old way -> **need** for **regular exercise & usage** (see book CCE, “Day without SCADA exercise”)
  o How to send people in emergency to **distributed** remote **locations**

• Supply Chain & Globalization
  o Own resilience (in some scenarios) “useless” due to own **dependence on supply chain** which might lack fallbacks
  o Analog **products**\(^2\) **not offered** by suppliers anymore (push to digitalization)

---

1) While it might be true that manual mechanisms & fallbacks come with additional costs it will never be as cheap again as now to keep & maintain them! Rebuilding them in the future would be much more expensive or even impossible
2) and spare parts!
What to do if an analog fallback is not possible?

• **Only** suitable for **most critical processes** (see literature CEE)
• If not feasible or achievable at least **prepare** for disaster & ideally **strive** for an **independent** (digital) **mechanism**!
  - BCM & emergency planning
  - Try to identify critical dependencies & SPOFs
  - Isolation & strong segmentation
  - Reduce number of digital pathways into system
  - Offline backups
  - Diversity & voting mechanisms
  - Reproducible builds
  - Internet independent control interface (think IOT & Smart Home)
Open Questions

• In **which fields & areas** do analog or manual mechanisms & fallbacks **make sense**
  o Try to systematically research and identify fields/areas
  o Not only think about critical infrastructure & manufacturing but also about the whole society
• How can **awareness** be raised and it’s value “sold” (overcome Turkey illusion)
• Is it **feasible** to **require by law** that some fields, organizations (e.g. critical infrastructure) or vendors **preserve** or **rebuild** analog **fallbacks**?
• Should there be **incentives** or subsidies to **create a market** for such controls?
  o Can suppliers be required to **continue offering analog products** and spare parts in addition to their new digital products?
Conclusion

• We are still in the **honeymoon phase** of digitalization
• The ideas presented are **not** about relinquishing all **benefits** of **digital technologies** and going back to the “**stone age**”
• It’s about **recognizing** that **not everything** has to be **digitalized** and that there is a often unrecognized and forgotten **value** in analog & manual **fallback mechanisms**!
• **Preservation** and maintenance of these mechanisms **creates costs** but brings **huge long term benefits** and increases **resilience**
  ○ It’s never going to be as cheap as now to keep them
Literature

- Dan Geer:
  - A Rubicon

- Andy Bochman (expert Idaho National Laboratory):
  - Internet Insecurity (Paywall) https://archive.ph/JrPSD (archived Version)
  - The End of Cyber Security (Paywall)
  - Book: Countering Cyber Sabotage: Introducing CCE
  - The Case for Simplicity in Energy Infrastructure

- Idaho National Laboratory

- Ralph Langner
  - Back to the Future: Putting analog hard stops to cyber attacks

- Is Analog the Fix For Cyber Terrorism? (Interesting discussion & good examples)
  - https://itslashdot.org/story/14/03/18/021239/is-analog-the-fix-for-cyber-terrorism
Don’t it always seem to go
that you don’t know what you’ve got
till it’s gone

Joni Mitchell
The active preservation of the analog option must come soon if it is to have the cost-effectiveness of preserving fully amortized infrastructure and not the sky-high costs of recreating it under emergency conditions

Dan Geer
Questions & Discussion