Trust nobody, but be available

Steffen Ullrich, genua GmbH

Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch

about:*

about:me

- Steffen Ullrich, genua GmbH, Germany
- 20+ years in cyber security:
  development, research, strategy, ...

Steffen Ullrich
Technology Fellow
steffen_ullrich@genua.de

about:talk

- What is Zero Trust and why it is useful
- Use cases: remote maintainance, remote monitoring, securing brownfield

We are under attack

Cyber-Attack Against Ukrainian Critical Infrastructure

On December 23, 2015, Ukrainian power companies experienced unscheduled power outages impacting a large number of customers in Ukraine. In addition, there have also been reports of malwar[illegible] found in Ukrainian companies in a variety of critical infrastructure sectors. Public reports indicate that the BlackEnergy (BE) malw[illegible] is important to note that the role of BE in this event remains ur[illegible]

Satellite hack on eve of Ukraine war was a coordinated, multi-pronged assault

The satellite hack that took the world by storm was more complex than initially thought, according to a Viasat executive.

Hackers Breached Colonial Pipeline Using Compromised Password

- Investigators suspect hackers got password from dark web leak

An Unprecedented Look at Stuxnet, the World's First Digital Weapon

Throwback Attack: How NotPetya accidentally took down global shipping giant Maersk

Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch

We fail even w/o attacks

Toyota blames factory shutdown in Japan on ‘insufficient disk space’

New hotness: VW-Produktion steht wegen IT-Problem st
Geschichte, die ich nicht prüfen kann, daher behandelt e

Ebene 1:

Lizenzproblem mit den Switches. Nach einer Warr
bestimmte Features ab. Darunter auch verschlüss
deaktiviert wurde, war das normale LAN zwar noch erreichbar, aber alle sicheren Netze,
einschließlich des Admin-Netzes, nicht mehr. Admin-Netz hätte man in einem normalen
Wartungsfenster patchen können, ohne BGP im C
alle verfügbaren IT-Mitarbeiter, nach einer kurzen
Konsolen-Port patchen. Bin an dem Tag ca. 15km

Ebene 2:

Der Lizenzkauf war automatisiert. Alle X Jahre wu
geschickt und die Netzwerker erhielten dann die E
Aufforderung zum Refresh). Da die Personen, die diesen Automatismus eingerichtet hatten, nicht
mehr im Unternehmen sind und die Buchhaltung anscheinend nicht wusste, was dieser Posten war,
wurde er nicht freigegeben.
Die Warnungen der Netzwerkkomponenten wurde

https://blog.fefe.de/?ts=9be8642a

‘Just in time’ production system minimises costs but technical glitch highlights risks

Volkswagen production restarted after IT halt: attack is “unlikely” cause

Oldsmar water treatment plant incident allegedly caused by human error, not remote access cybersecurity breach

Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch

Loss of control

Increased **complexity** causes loss of control

- Larger attack surface
- More inherent fragility

But increased **criticality** requires more control

- More critical digital assets
- Availability and integrity are crucial for both companies and society

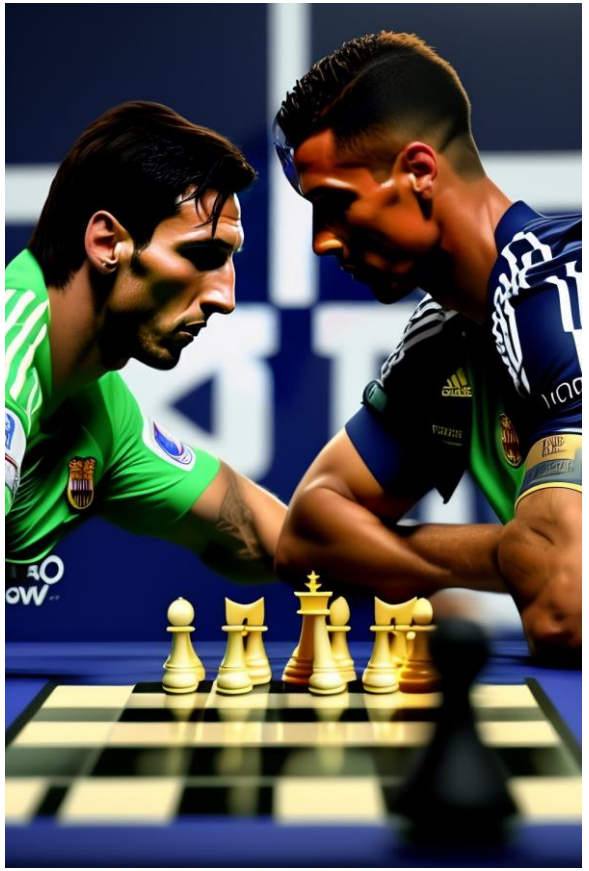
Cause of complexity

Driven by customer demand and competition

- Need to be more flexible, efficient, faster to market → more digitalization, Industry 4.0
- Risk of losing to competition vs. risk of cyber attack

OT/IT convergence - culture clash

- OT: focus on stability, availability, safety
- IT: moving fast, "release now fix later"



Aspects of complexity

Large inherent complexity

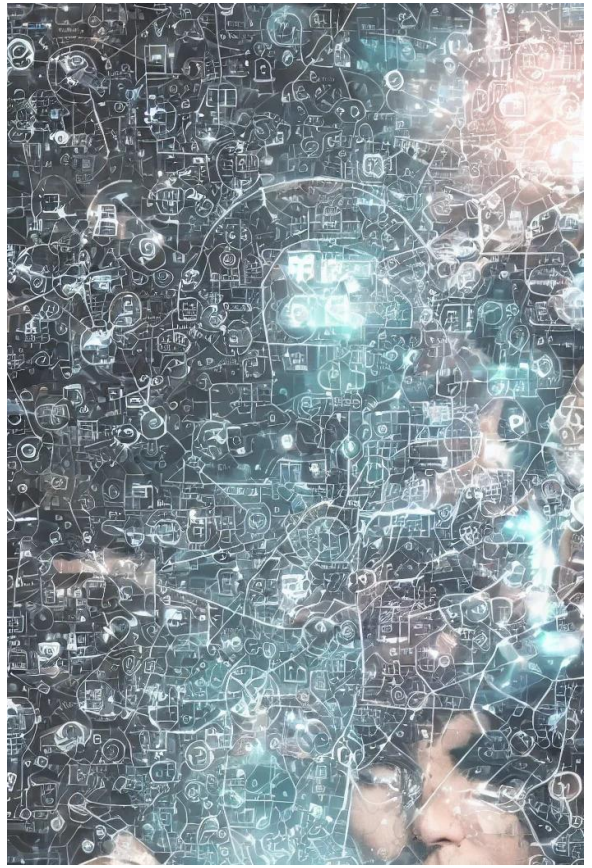
- Size of software and hardware stack
- Many interactions between components

Broader and deeper expertise needed

- vs. shorttage of skilled workers

Many external dependencies

- Software and hardware supply chain
- Infrastructure: energy, communication, transport ...
- Data exchange between OT and surrounding IT



Tackle complexity

Reduce complexity	Add robustness	Reduce learning curve	Reduce dependencies
• Fewer features • Refactoring • AI • ...	• Redundancy • Error checking • Self-correction • Defense in Depth • ...	• Use standards • Fewer vendors • ...	• DIY? • ...

No ideal solution. Lots of options with their own trade-offs.

Divide & Conquer

Partition into managable segments

- Lower inherent complexity and criticality
- Observable interaction between segments

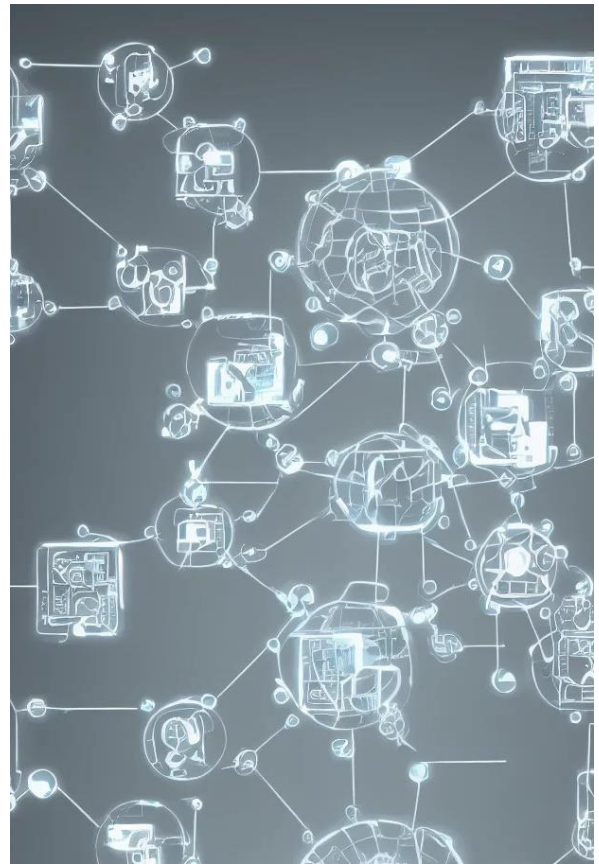
Restrict interaction between segments

- Minimize access: just in time, just enough
- Assume compromise: verify trustworthyness

Zero Trust

Can be implemented step by step

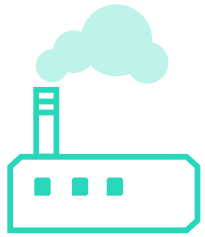
- Start with easy steps having large impact



Remote Maintenance

Access of remote service provider

- Not fully trusted
- With potentially compromised credentials
- From a potentially compromised users system and network
- Over the untrustworthy internet



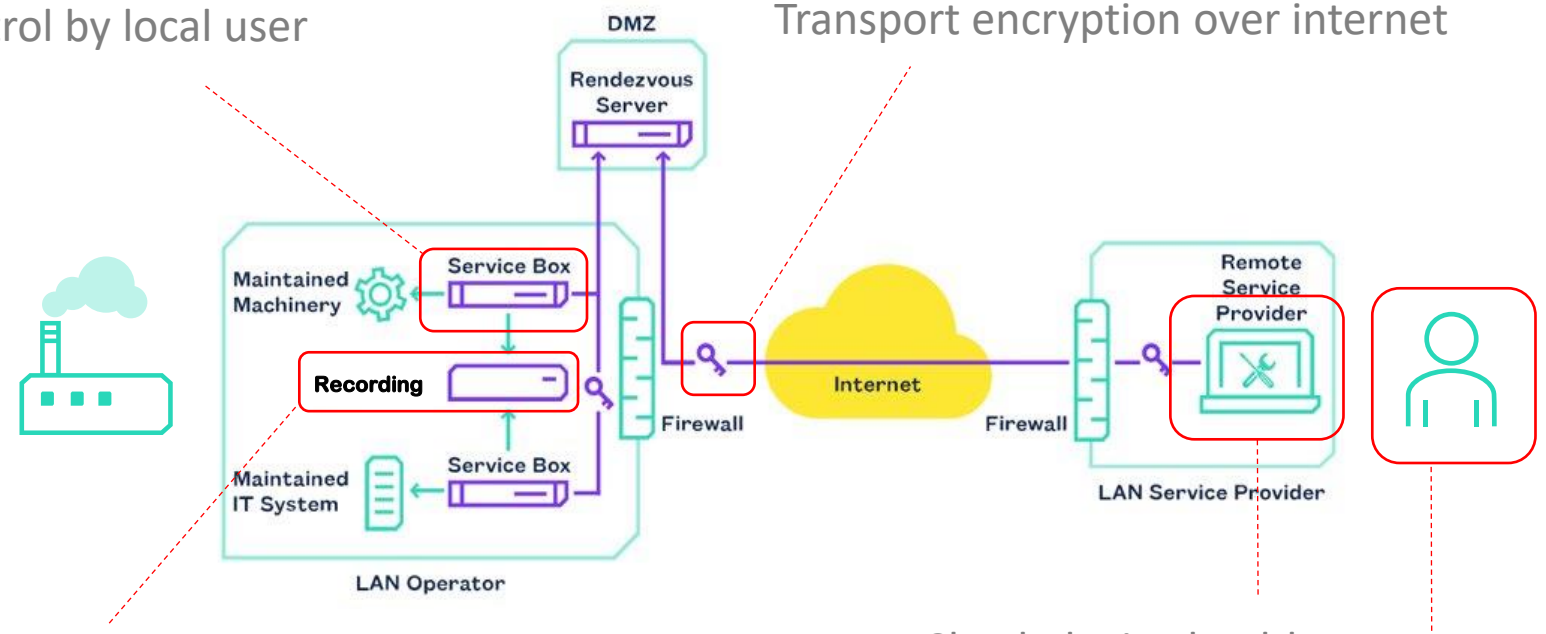
To a local system

- Critical and potentially vulnerable
- Connected to critical and potentially vulnerable network

Limit risk from remote user

Additional access control by local user

Transport encryption over internet



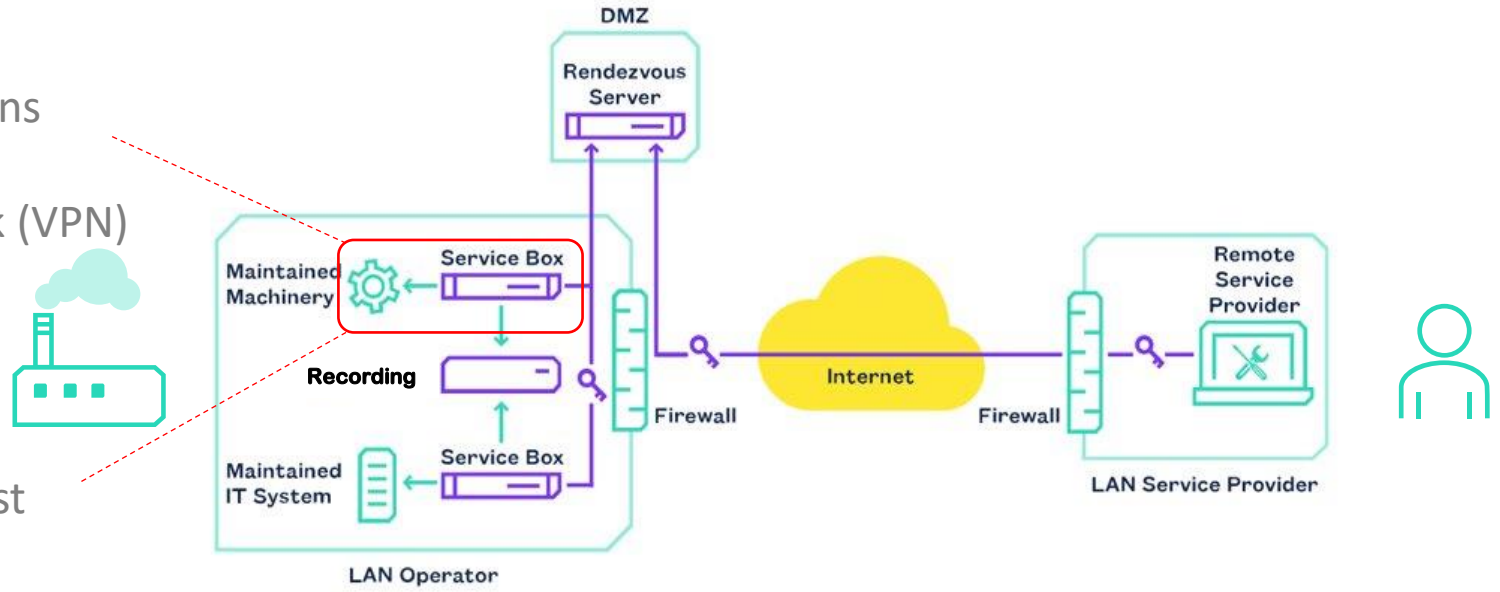
Don't fully trust service provider: record all activity

Check device health.
Strong MFA to secure credentials.

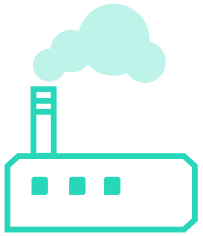
Limit potential impact

Minimize inbound
- Only selected connections from service provider
- No full network interlink (VPN)
- Scan transfered files

Minimize outbound
- Network isolation against lateral movement



Remote Monitoring



Sending monitoring data from operations

- Critical, potentially vulnerable systems and networks

To external provider

- Sufficiently trustworthy to receive and process data
- Potentially compromised –
  prevent propagation into own environment

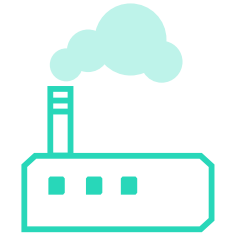
Data diode

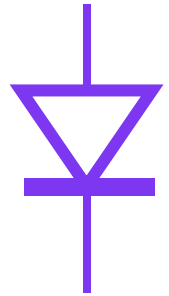
Guaranteed unidirectional data transfer

- Compromise of local OT not possible since no back channel

Guaranteed by physics - Light emitter and receiver

- Minimal access = physically impossible back channel
- no control over failure and success :(

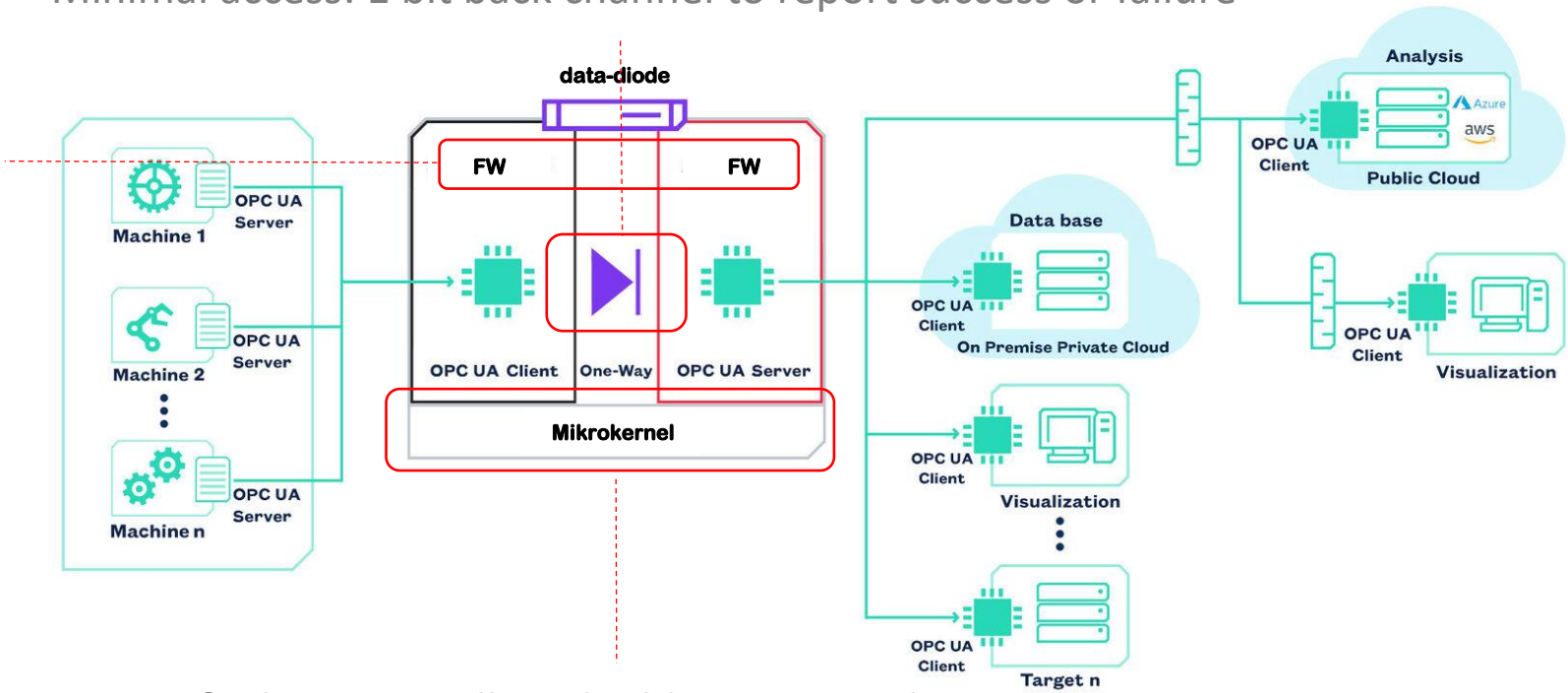




Data diode +

Minimal access: 1 bit back channel to report success or failure

Emulation of bidirectional protocols (TCP, FTP, HTTP, OPC/UA ...)



Verified trust: small, auditable source code

Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch

Securing brownfield

System in the network

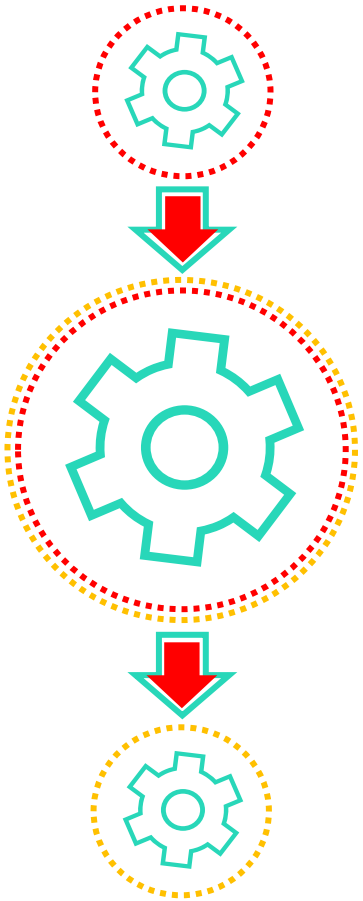
- Potentially vulnerable

Receives data from inside and outside the network

- Sender cannot be fully trusted

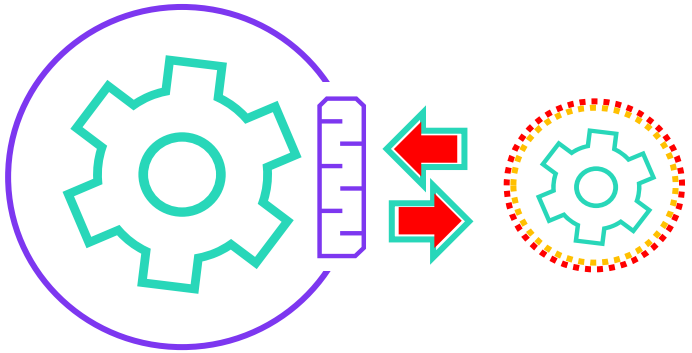
Sends data inside the network and to the outside

- System might be compromised
- Receiver might be vulnerable

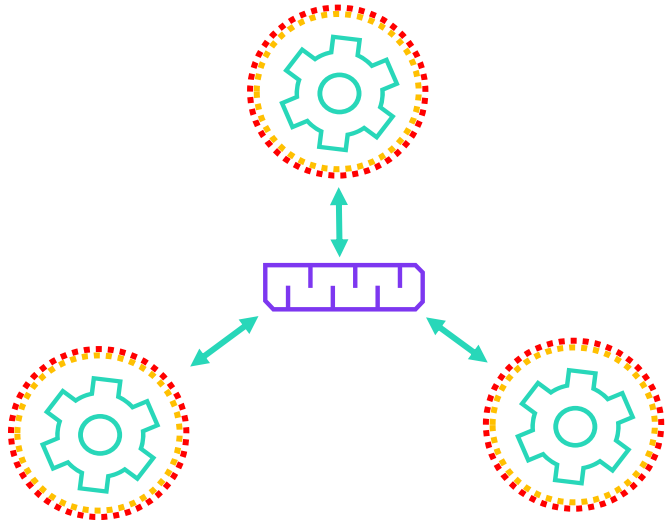


Minimize access

Inbound: decrease attack surface
Outbound: limit impact to others



Microperimeter
around vulnerable systems



Microsegmentation
to separate vulnerable systems

Can be transparently integrated into existing environments

Summary – Get control back

Divide into smaller segments

- Easier to understand and control
- Less impact when compromised

Conquer with restricted interaction

- Minimal access
- Verified trust

Step by Step