Industrial Cybersecurity Challenges

Andreas Reiter RC-AT DI FA DH-GRAZ SAS
andreasreiter@siemens.com

O&K

K
544
044
Im EGB - Bereich

IT – OT?

IT

- Dynamic
- Full spectrum of technologies
- Well connected
- Confidentiality, Integrity, Availability

- **Data is King**

IT – OT?

- Control production floor processes
- Process oriented
- Safety/Availability, Integrity, Confidentiality

- **Process is King**

OT

IT - OT Challenges

Information Technology		Operational Technology
3-5 years	**Asset lifecycle**	20-40 years
Forced migration	**Software lifecycle**	Usage as long as spare parts available
High	**Options to add security SW**	Low
Low	**Heterogeneity**	High

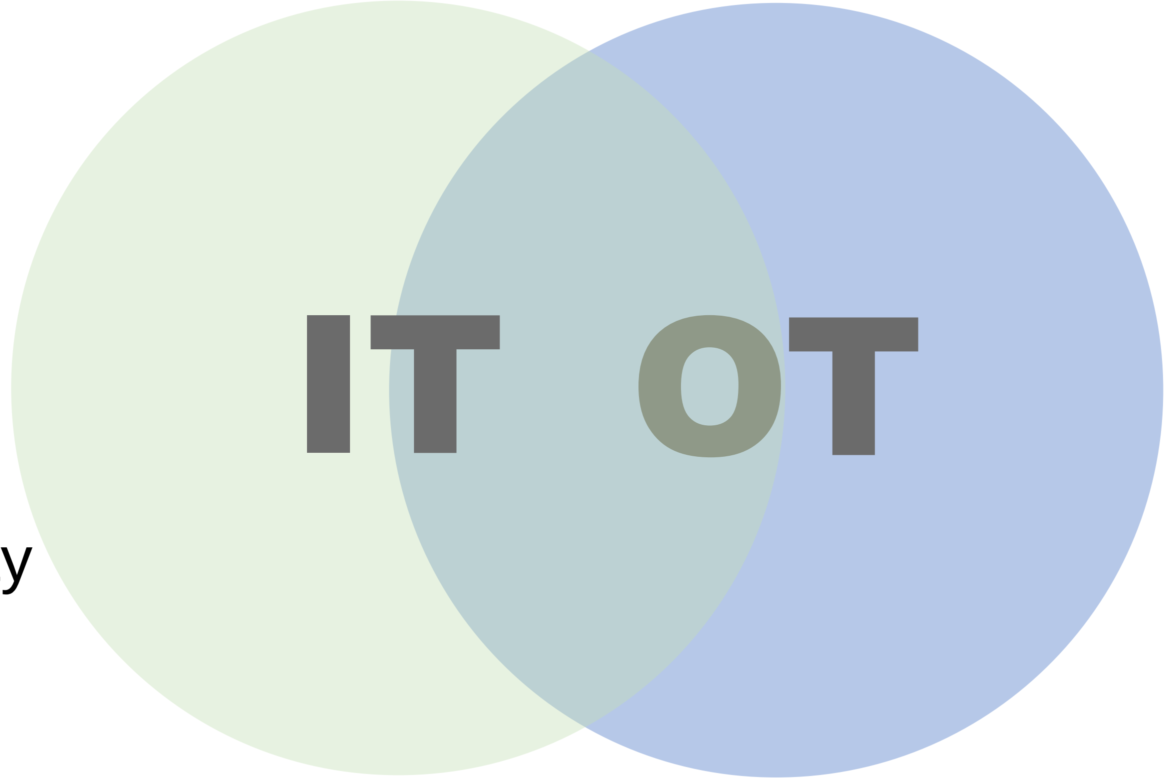
IT – OT?

SIEMENS
Ingenuity for life

- Massive data generation

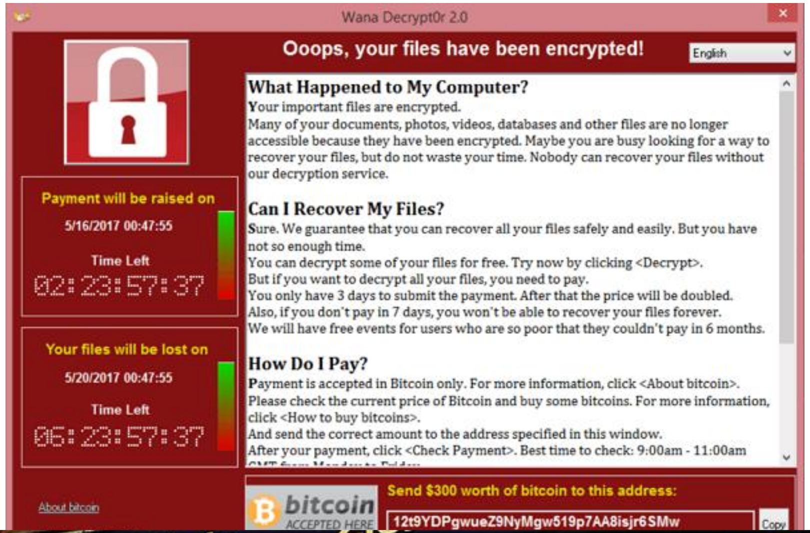
- Big data analytics capabilities
  - Real-time decisions
  - Predictive maintenance

- Increased efficiency and productivity
- Create new revenue streams



WannaCry

SIEMENS
Ingenuity for life



Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

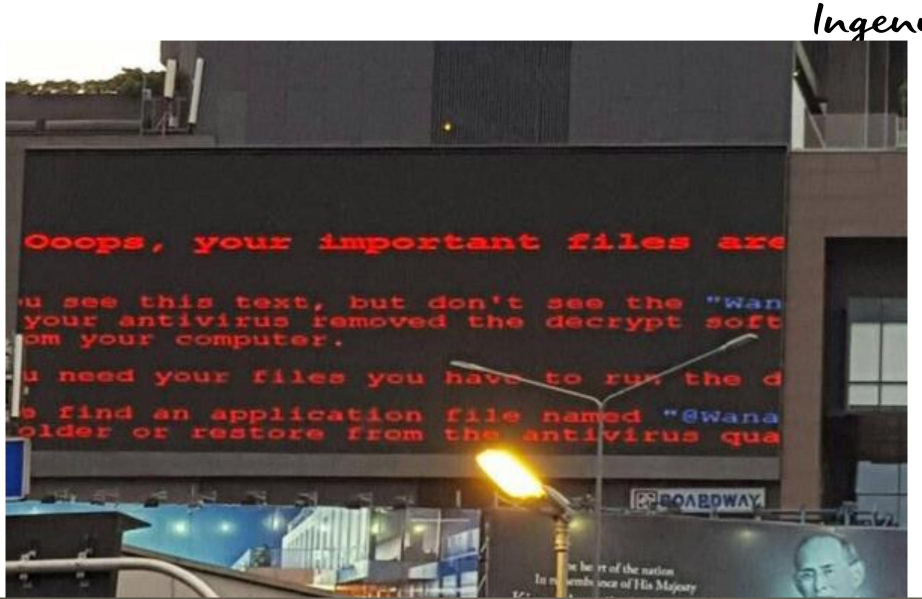
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

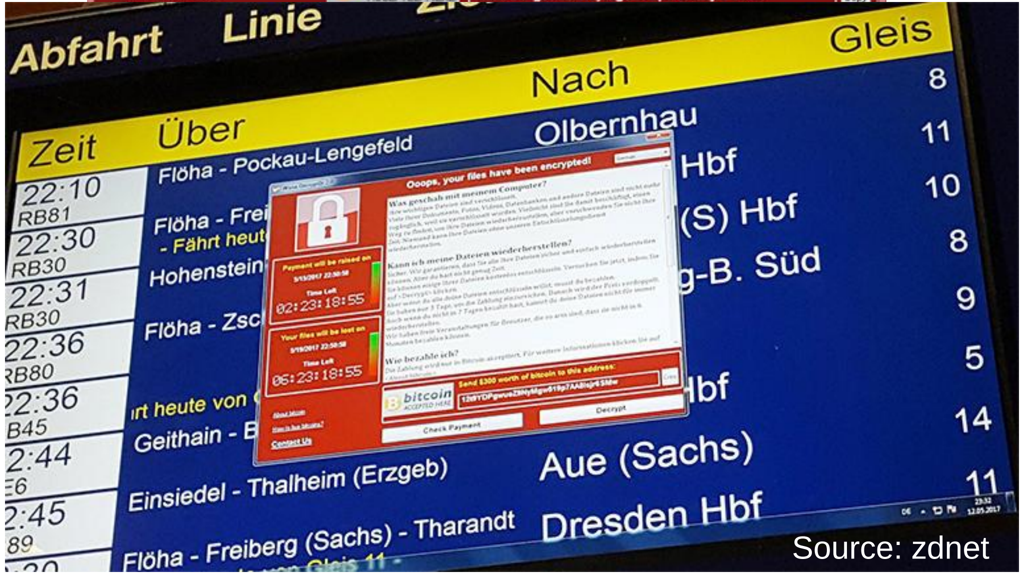
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

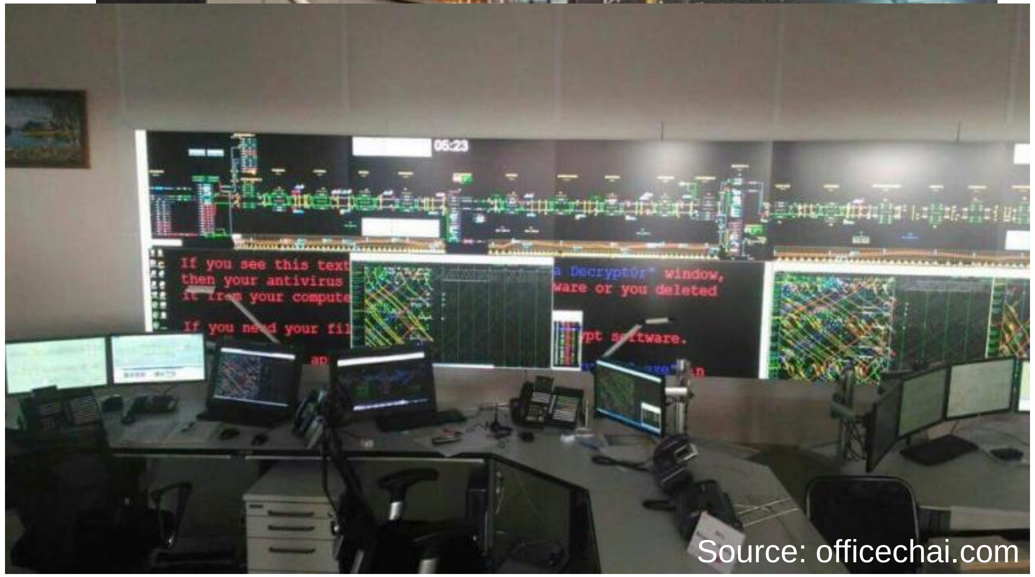
About bitcoin
bitcoin ACCEPTED HERE
Copy



Ooops, your important files are
u see this text, but don't see the "Wan
your antivirus removed the decrypt soft
om your computer.
u need your files you have to run the d
e find an application file named "@Wana
older or restore from the antivirus qua
BOARDWAY



Source: zdnet

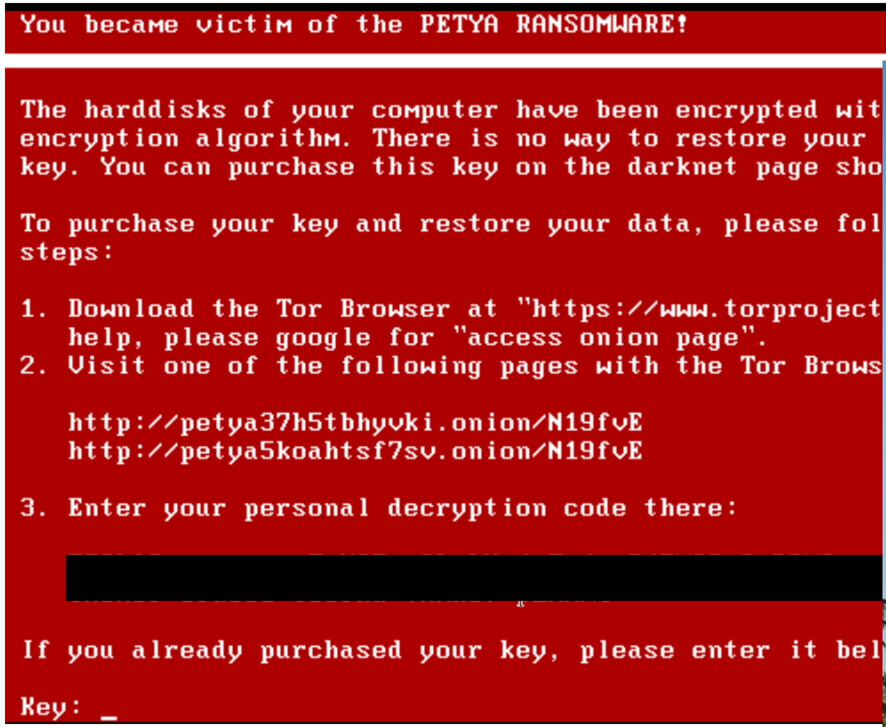


Source: officechai.com

Unrestricted © Siemens AG 2019

(Not)Petya

SIEMENS
Ingenuity for life

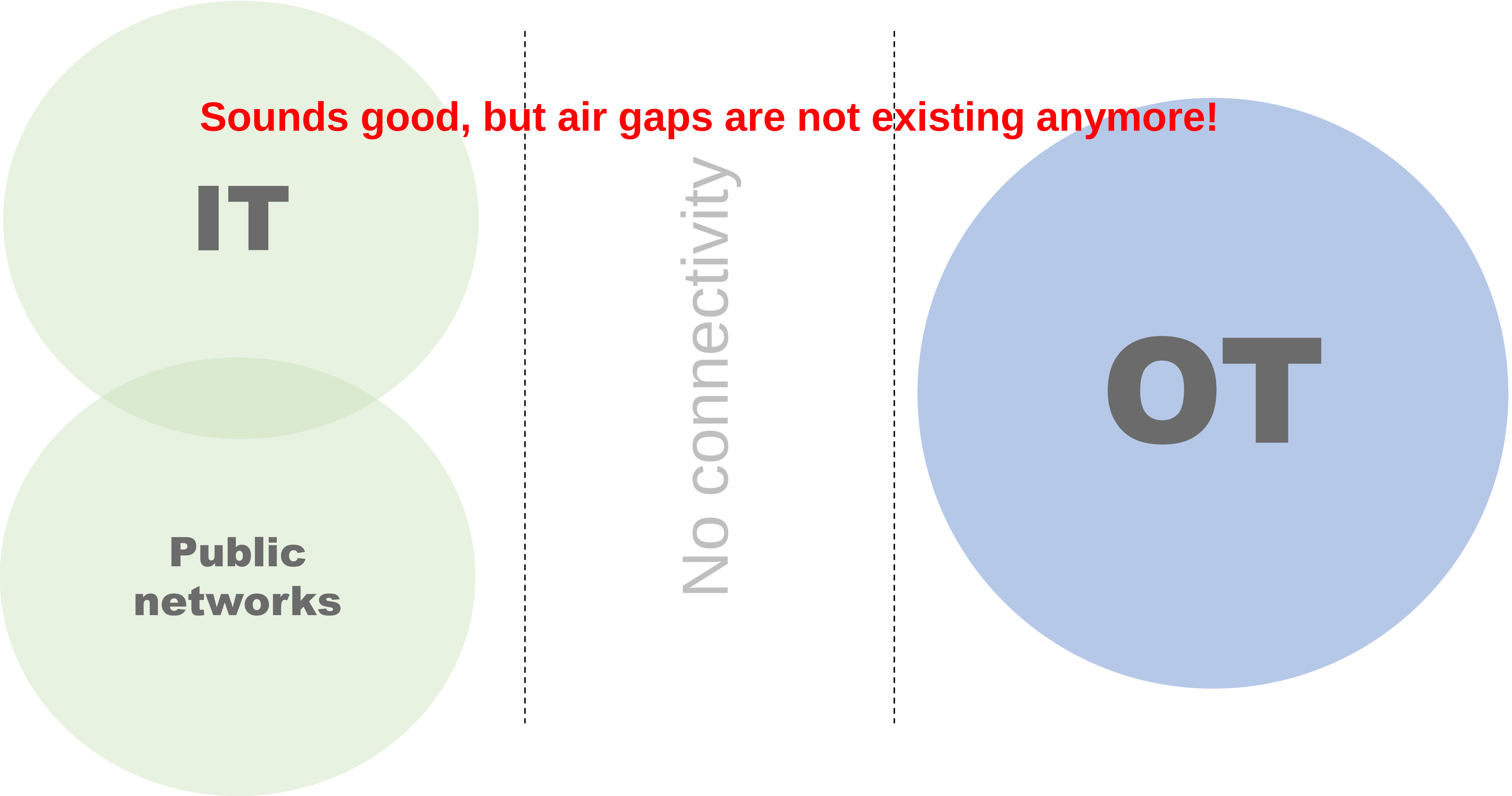


```
You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted wit
encryption algorithm. There is no way to restore your
key. You can purchase this key on the darknet page sho

To purchase your key and restore your data, please fol
steps:

1. Download the Tor Browser at "https://www.torproject
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Brows

   http://petya37h5tbhyvki.onion/N19fvE
   http://petya5koahtsf7sv.onion/N19fvE

3. Enter your personal decryption code there:

   [redacted]

If you already purchased your key, please enter it bel

Key: _
```

"…the mean time to identify [a data breach] was 197 days…"

Cost of a Data Breach (2018)

Air Gaps



Sounds good, but air gaps are not existing anymore!

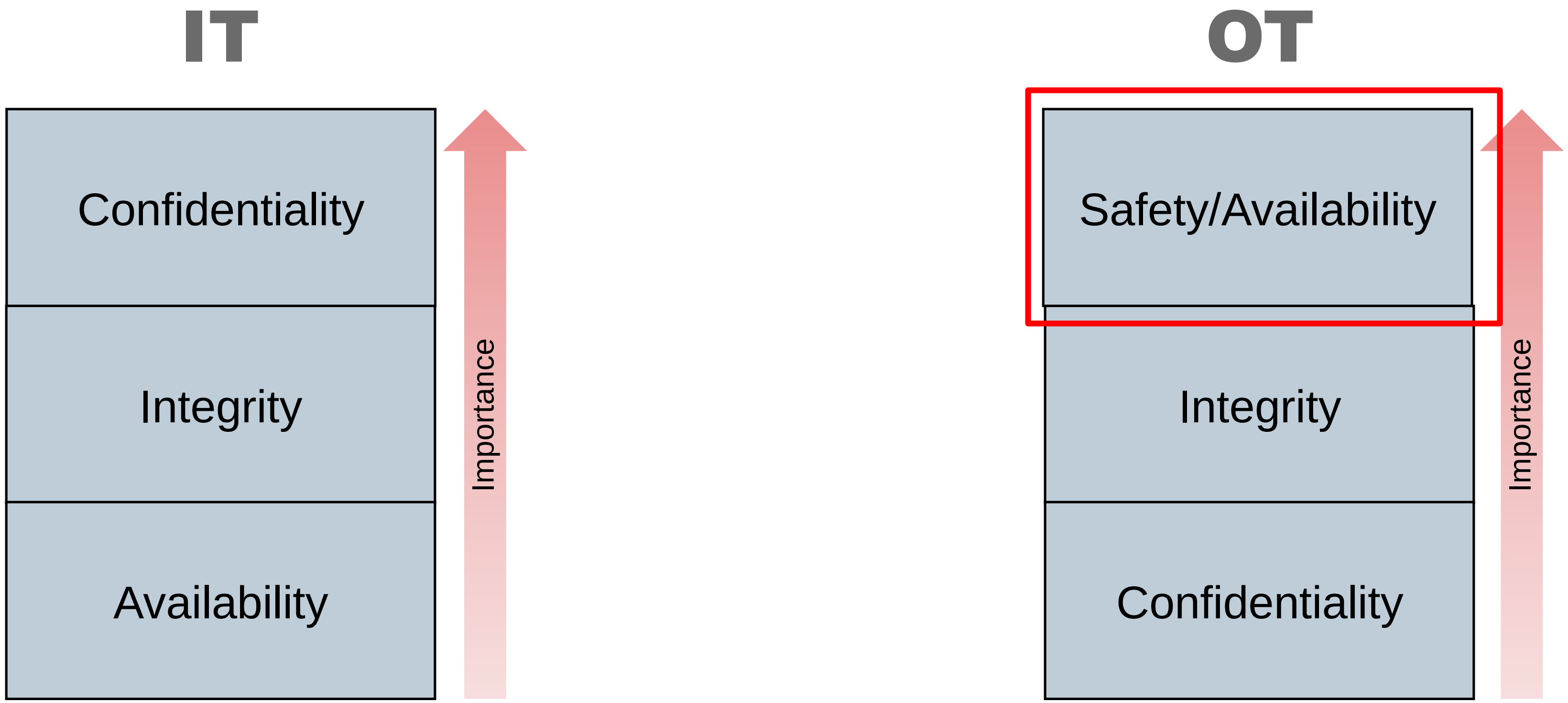
IT

Public networks

No connectivity

OT

Patch Tuesday?



IT	OT
Confidentiality	Safety/Availability
Integrity	Integrity
Availability	Confidentiality

No patch Tuesday in OT

Strong Perimeter Security

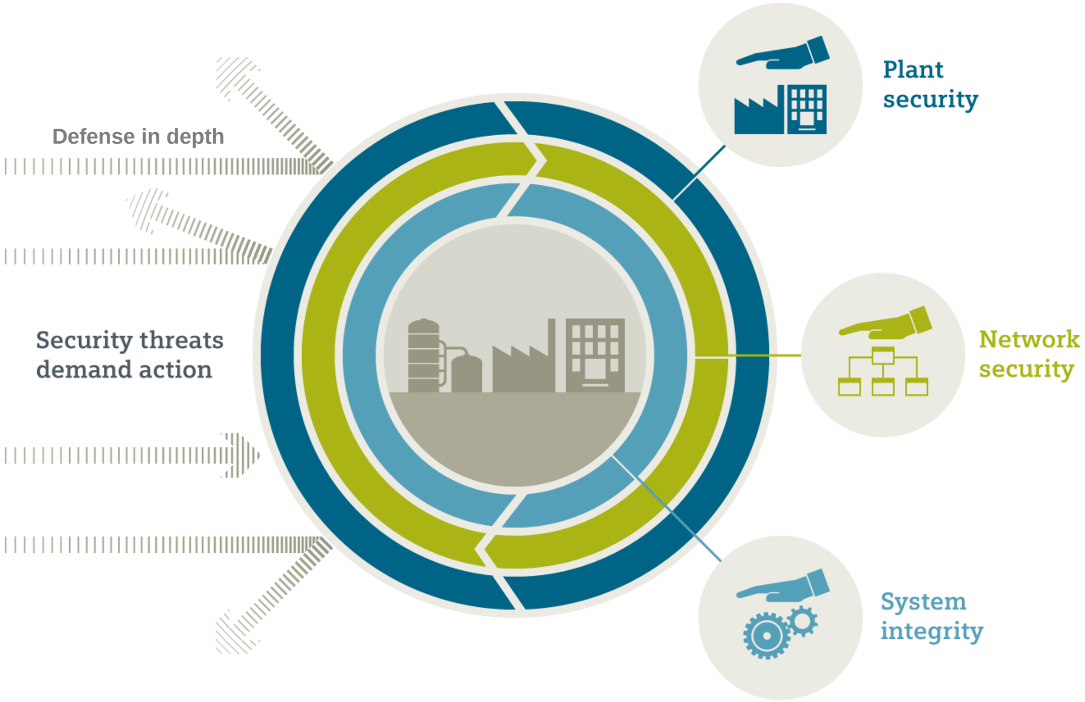
- Analog to air gapping
- Firewalls
- Traffic analyzers

Defence in Depth

SIEMENS
Ingenuity for life

- Know what's going on in your network
  - Network monitoring
  - Log analysis

- "Castle approach"
  - Multiple lines of defense
  - Network segmentation
  - Device security
  - Common cryptographic principles
  - Security-by-design
  - …

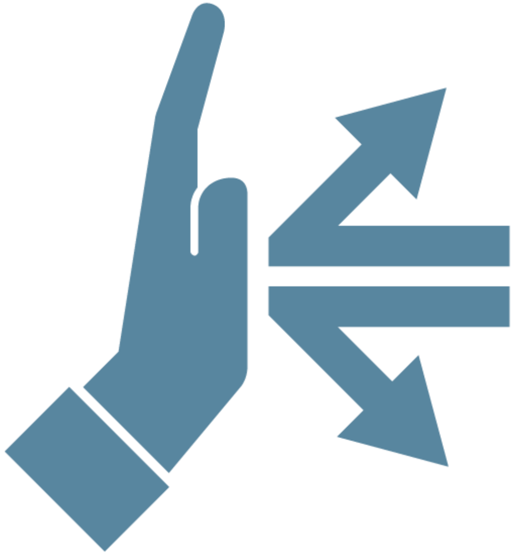


Vulnerability Scanning

- Be proactive
- Not only scan IT, but also OT networks and components
- Check against known vulnerabilities
  - Open vulnerability databases
  - Vendor specific databases

Processes

- Security Event Management (SEM)
  - Near real-time security alarms and events
- Security Information Management (SIM)
  - Long-term storage of log data
- Patch management



Siemens DH-Graz

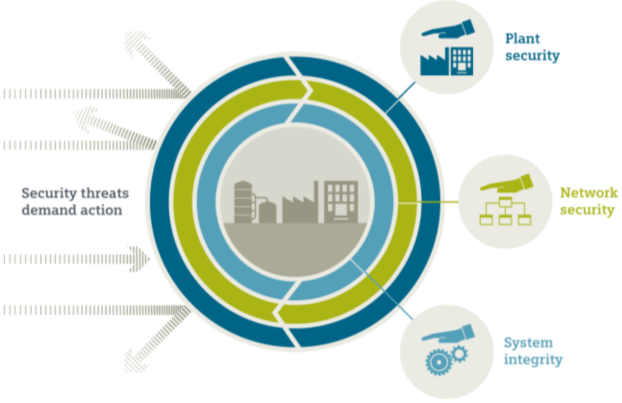
SIEMENS
Ingenuity for life

- Founding member of the charter of trust
  - Holistic concepts
  - Think beyond products and services

- Plant Security Services

- Strong Security competence at DH-Graz
  - Security testing
  - International research projects
    - defense in depth
    - controlled access to production networks
    - certification

Charter of Trust



Your Takeaways

- Air Gapping is not a suitable defense mechanism
- IT and OT environments are converging
  - …to make better use of data
  - …perform data analytics
  - …apply IT techniques
- More attack vectors
- Be proactive in the definition of your security strategy

Contacts

Andreas Reiter

RC-AT DI FA DH-GRAZ SAS

E-mail:
andreasreiter@siemens.com

https://www.linkedin.com/in/anreiter/

siemens.com/industrialsecurity