DCNA Austria

Disaster Competence Network Austria

Austrian Disaster Research Days 2019

14.-15.Oktober 2019, Technische Universität Graz

Industrieanlagen im Visier von Hackern

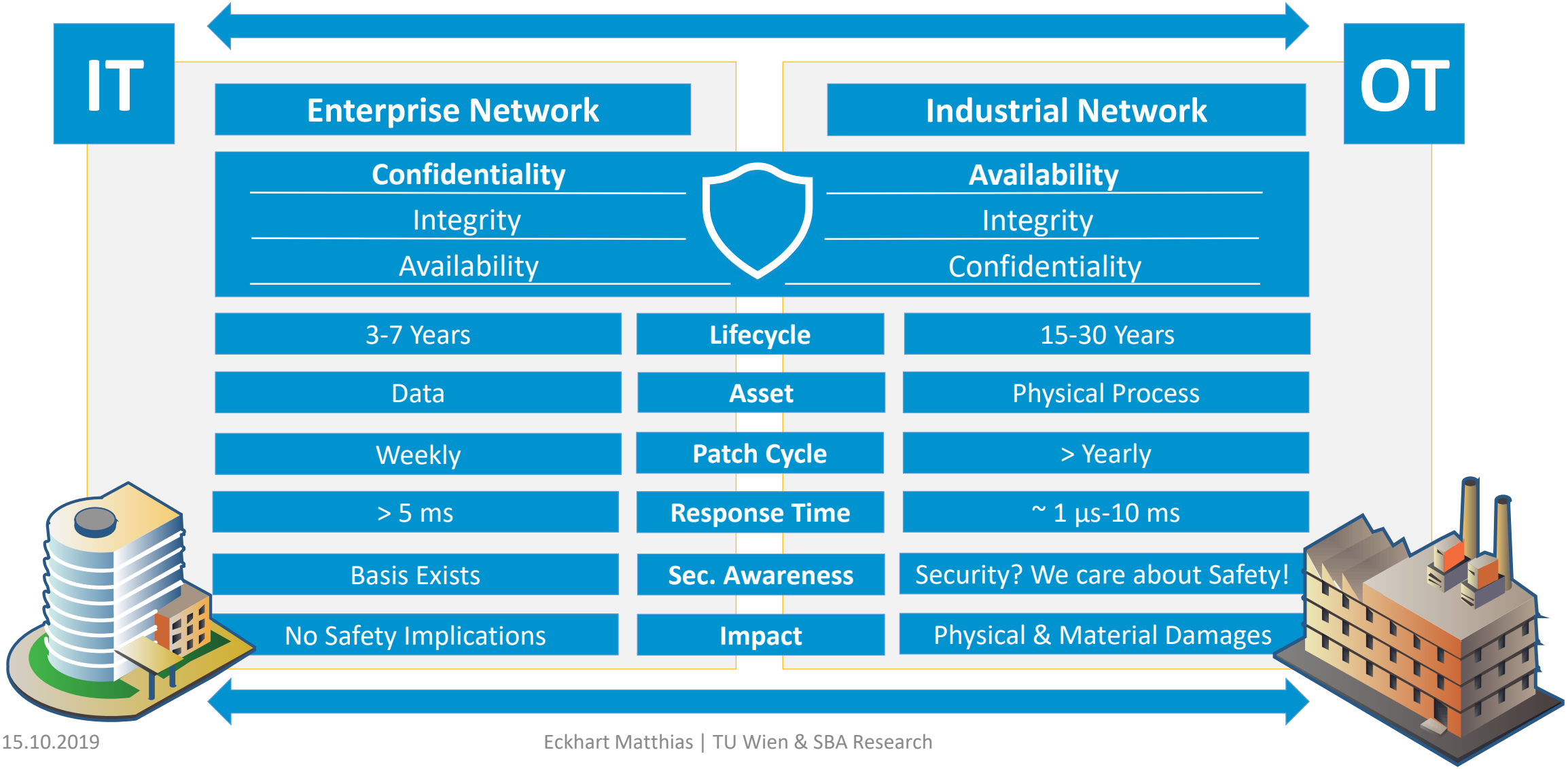
Matthias A. Eckhart

TU Wien (CDL-SQI) & SBA Research

Maroochy Water Breach

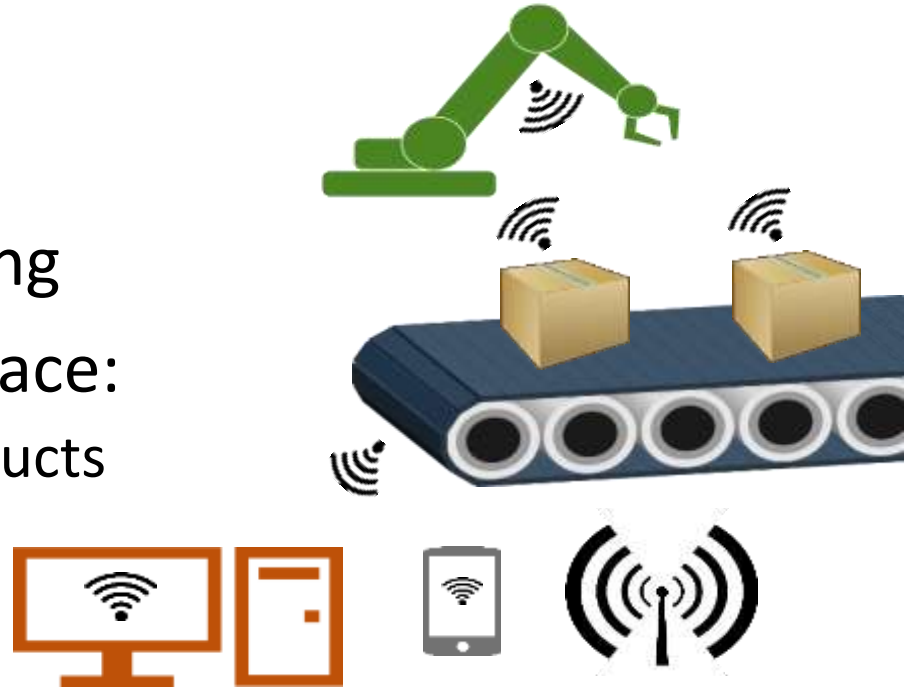
Image Source
(Wikimedia, 2006)

IT vs. OT (Industrial Control Systems, ICSs)

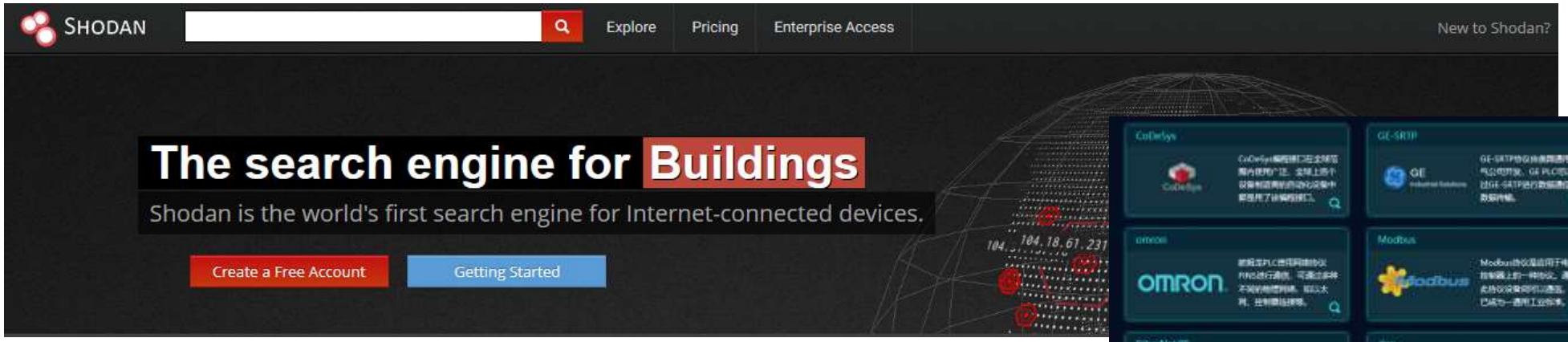


A Changing Threat Landscape

- The myth of “air gaps”
- New trends: Industry 4.0 & Smart Manufacturing
- Increasing connectivity expands the attack surface:
  - Interconnectivity of resources, processes, and products
  - Remote maintenance
  - Cloud & edge computing
- IT/OT convergence
- Legacy systems still in operation

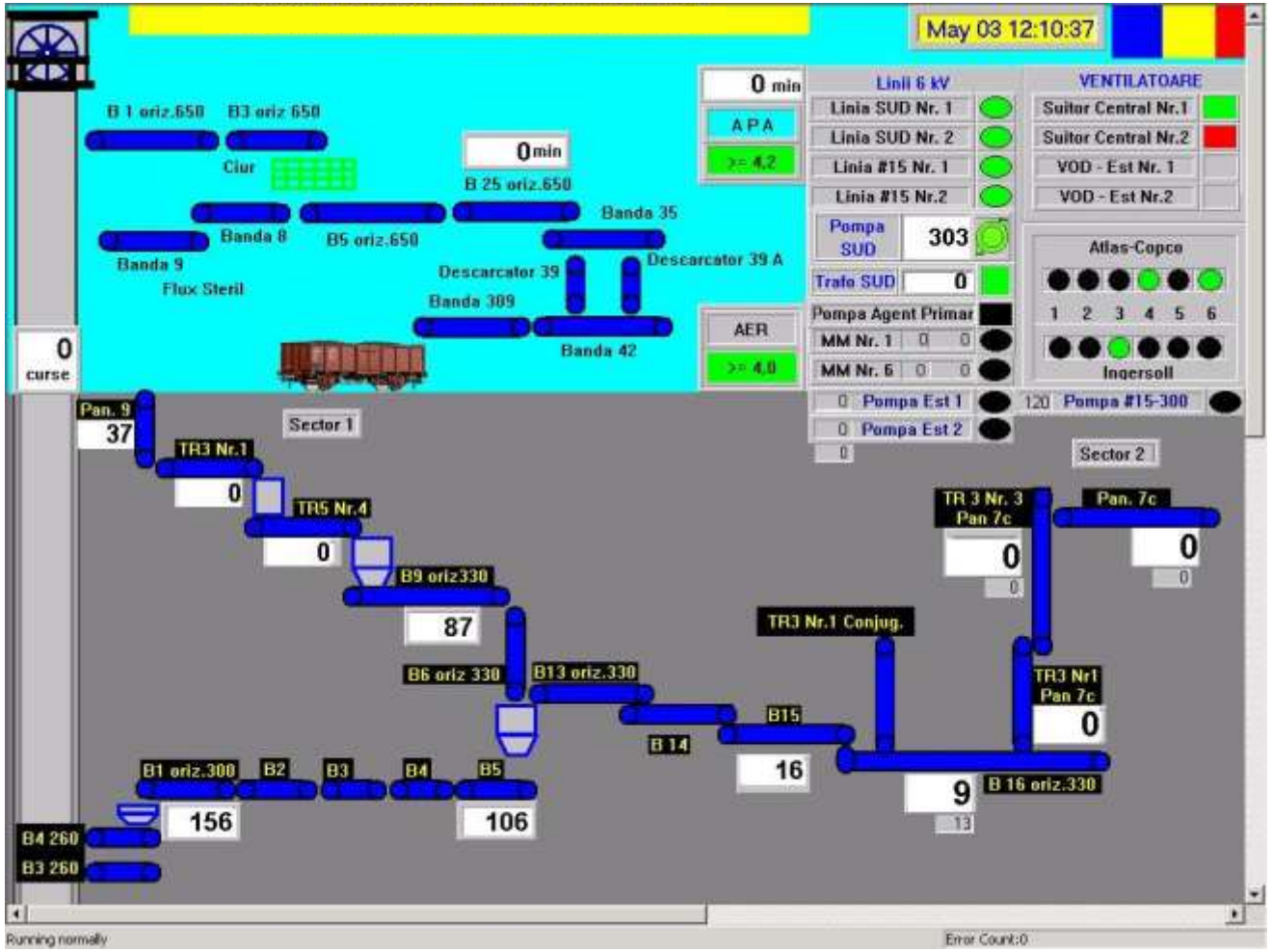


Internet-Exposed ICSs



- Search engines for Internet-connected devices
  - Shodan.io, FOFA.so, …
- Regularly scan the entire IP range
- Find:
  - ICSs, Traffic Lights, Webcams, Databases, IoT devices, …

Finding Interesting Things with Shodan



- Mine in Romania
  - VNC
  - Authentication disabled
  - Control:
    - Air supply
    - Pumps
    - …

Insecure by Design

> "64% of 2017 ICS-related vulnerability patches don't fully eliminate the risk because the components were insecure by design." – Dragos, 2018

- Security weakness discovered (and patched):
  - Still exploitable until end of life?
- Proprietary protocols & inherently insecure protocols often used
- Vulnerability management is difficult
- Time to rethink engineering (process)
- **Objective:** Establish security as a `first-class citizen` in the engineering process

Securing the Engineering Process

Engineering process is highly complex

Artifacts are created, managed, edited

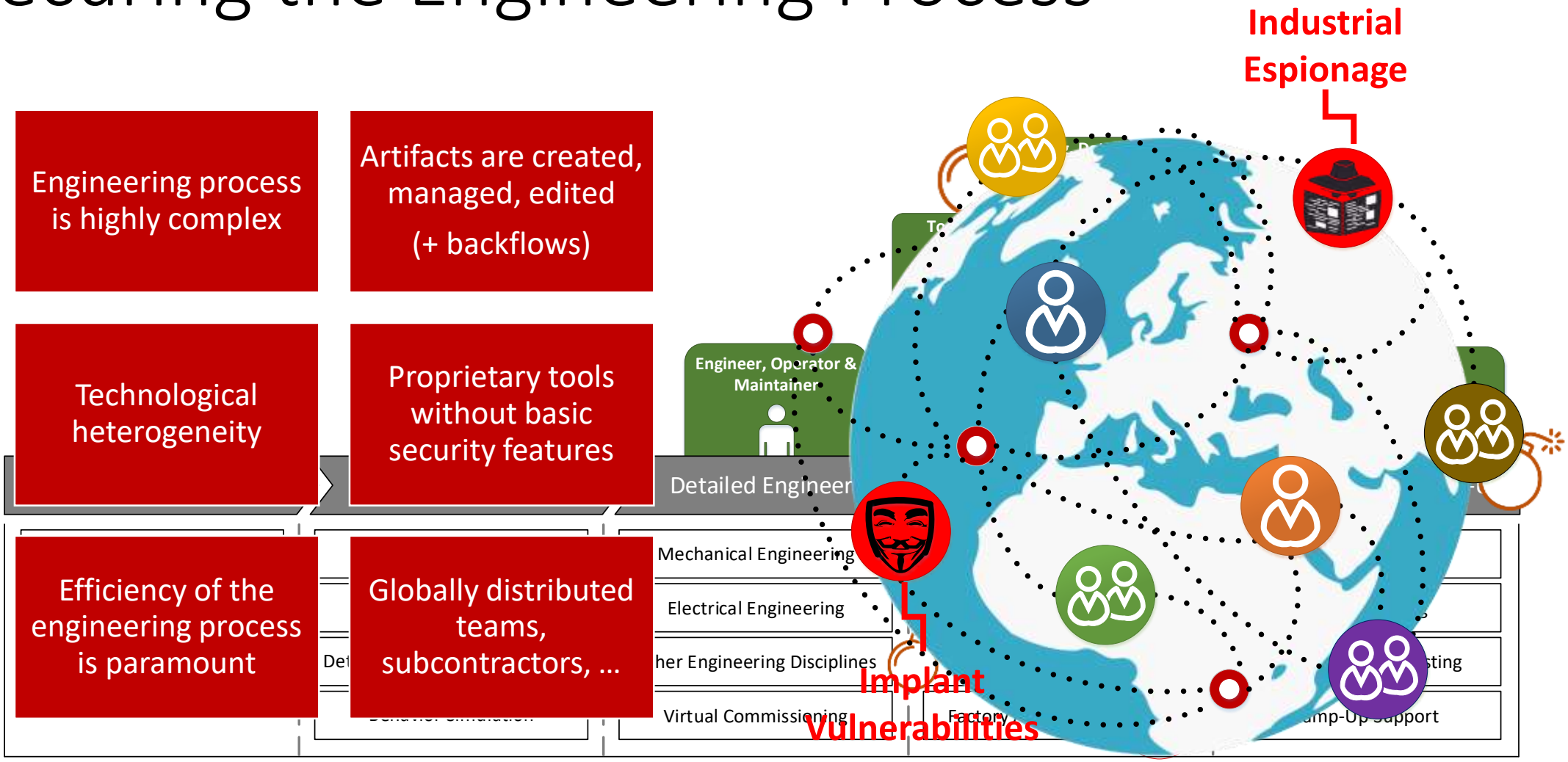
(+ backflows)

Technological heterogeneity

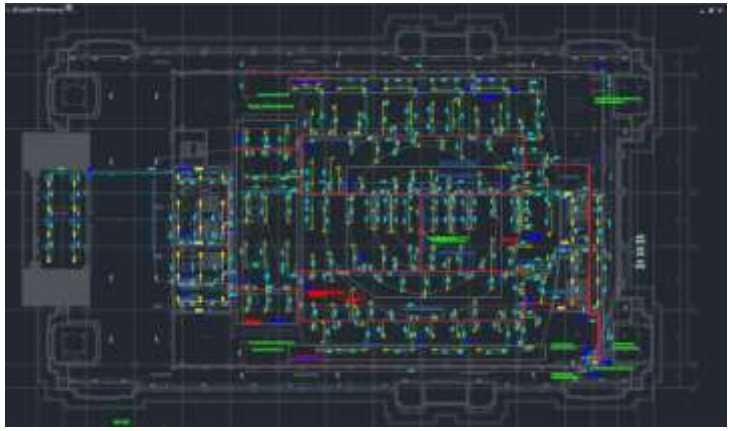
Proprietary tools without basic security features

Efficiency of the engineering process is paramount

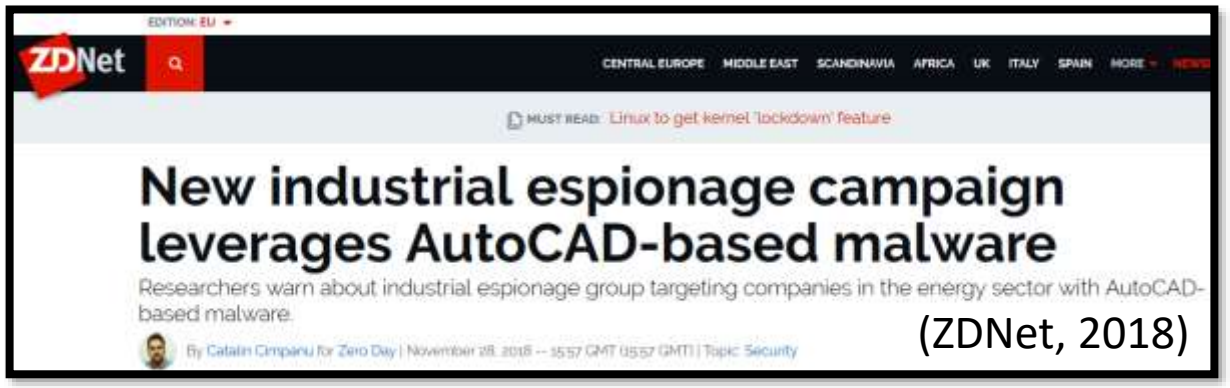
Globally distributed teams, subcontractors, …



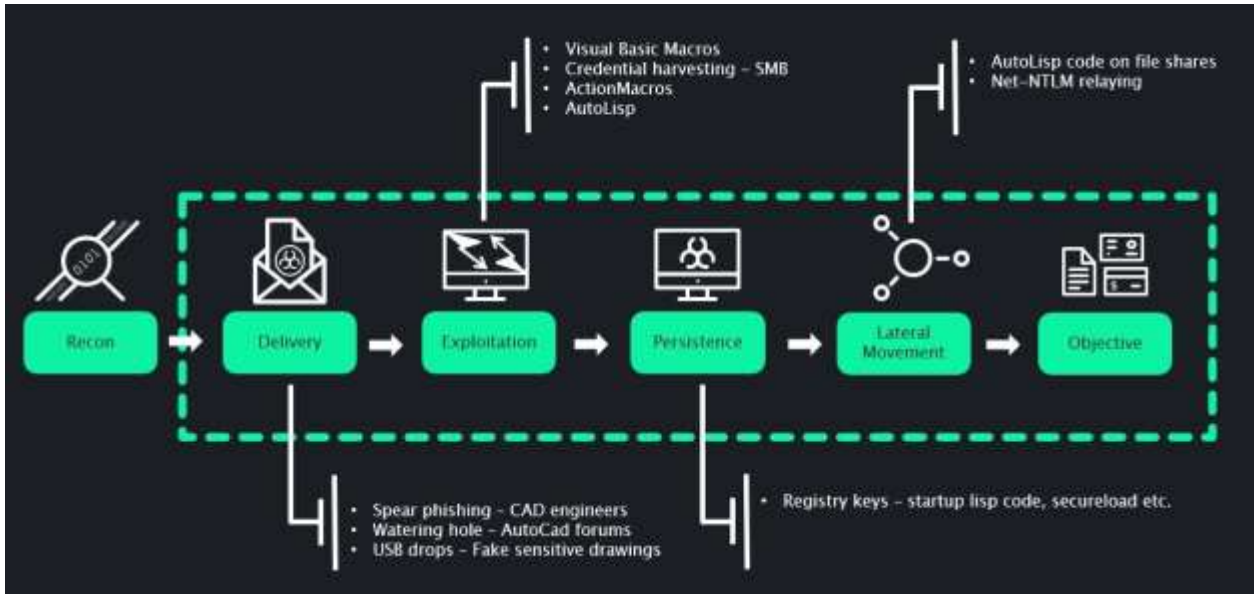
Malware in Engineering Artifacts – In the Wild



(Forcepoint, 2018)



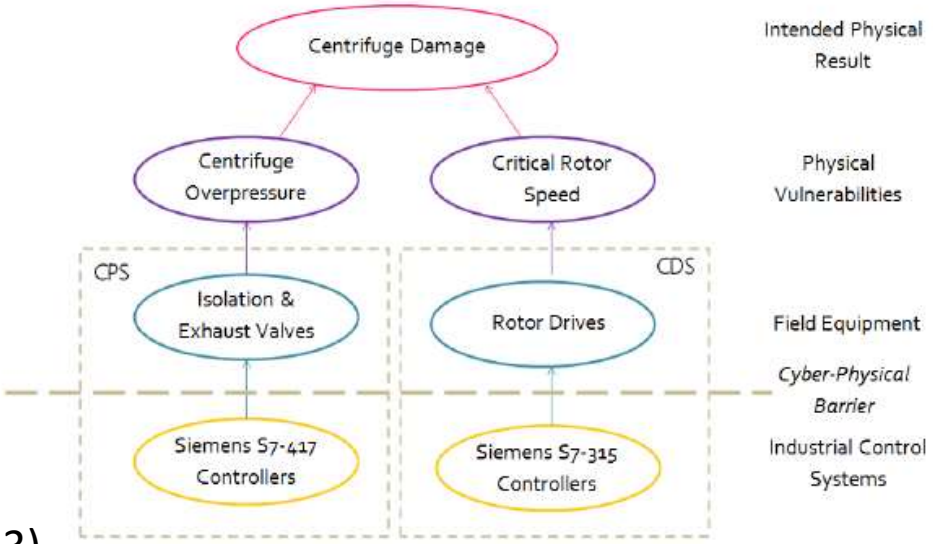
(ZDNet, 2018)



(F-Secure Labs, 2019)

Stuxnet

- Target: Iran's nuclear enrichment facility at Natanz
- 2 attacks executed periodically:
  - Overpressure attack:
    - Interfere with the Cascade Protection System (CPS) that is used for isolating unreliable centrifuges
    - Manipulation of exhaust valve to relieve overpressure
    - Record & replay 21 seconds of normal operation during attack
  - Rotor speed attack:
    - Interfere with Centrifuge Drive System (CDS) that controls motor speed
    - Overspeed rotors (normal: 63k rpm, Stuxnet: 84.6k rpm) for ~15 minutes
- Utilized multiple 0-days
- Attackers *tried* to avoid catastrophic damage
- Creators: NSA & Israel's Unit 8200?

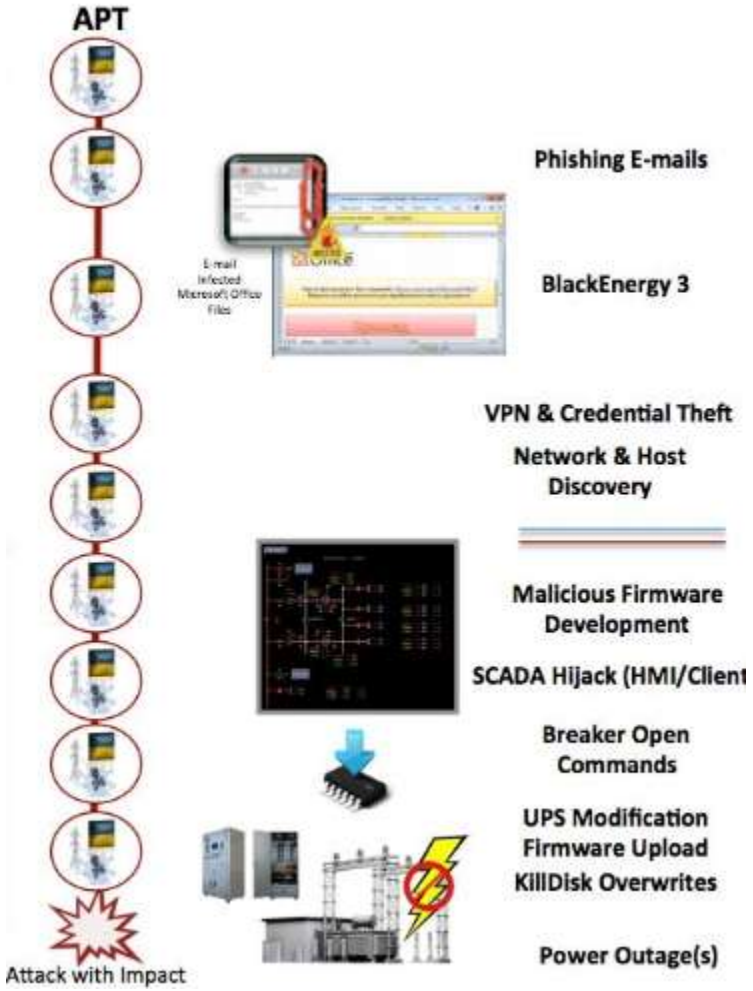


(Langner, 2013)

Cyber Attack against the Ukrainian Power Grid

- Attack on SCADA distribution management system
- Caused power outage in December 2015
  - Lasted several hours
  - Affected 225,000+ customers
- Malware enabled the attack and caused restoration delays
- Involved direct interaction with ICSs by adversaries

(Lee et al., 2016)



Cyber Insurance

(Financial Times, 2019)

- Growing importance of risk transfer
- Mondelez vs Zurich case:
  - NotPetya attack (2017)
  - Mondelez had an all-risk property insurance policy
  - $100MM claim
  - Policy exclusion: *"a hostile or warlike action"* by a "government or sovereign power"
- Attribution of cyber attacks is difficult
- Silent cyber exposure:
  - Non-affirmative cyber risks: risks implicitly included in policies
  - Claims for cyber attacks on non-cyber policies
- cf. Prudential Regulation Authority SS4/17
- Reducing silent cyber: cyber insurance for ICSs
- Opportunity: Incentivizing security

(PRA, 2017)

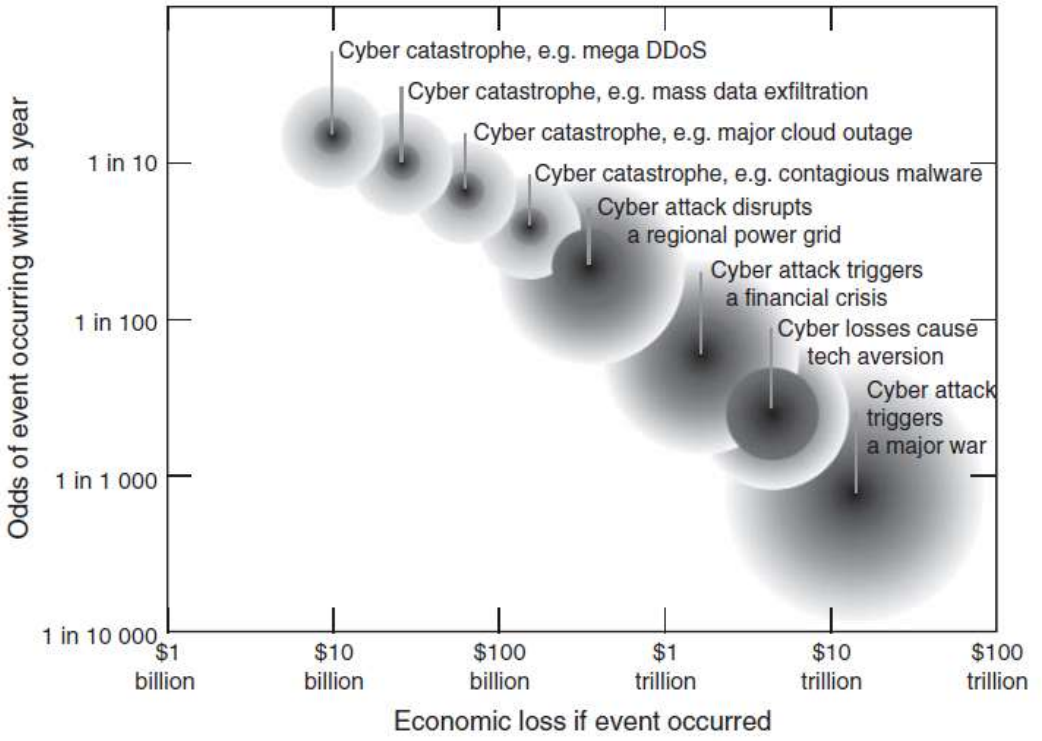
(JLT, 2019)

Managing the Cyber Black Swan

Image Source
(Wikipedia, 2009)

Cyber Accumulation

- Global spreading could lead to a <u>cyber catastrophe</u>
  - Cyber risk not geographically bound
  - Interdependencies among vulnerabilities, services, companies, …
  - Attackers & vulnerabilities are highly dynamic variables
- Cyber losses can cascade
- $3bn (re)insurance industry loss caused by NotPetya
  - Direct and consequential business loss: > $10bn (Coburn et al., 2019)
- Multiple reinsurers cannot deal with accumulated events
- Collapse of the insurance industry?
  - Devastating impact on economy
- Pressing research issues: quantification methods, cyber risk models, accumulation control strategies



(Coburn et al., 2019)

Ongoing Research Efforts in ICS Security @ CDL-SQI & SBA Research

Quant. Security Risk Assessments	Security of Engineering Data Exchange	Security by Design for Industry 4.0	Digital Twins	Blockchain

• Security Modeling in Production Systems Engineering
• Automated Risk Identification based on Engineering Artifacts
• Cyber Risk Quantification
• Cyber Insurance
	• Protecting Engineering Data in Transit and at Rest
	• Focus: AutomationML
	• Secure Interfaces for Engineering Tools
	• Security Technical Debt Analysis
		• Security Development Lifecycle for Cyber-Physical Production Systems
		• Designing ICSs with Security in Mind
		• Strongly Connected to Risk Assessment Research
			• Generation of Virtual Replicas
			• State Replication
			• Security-enhancing Use Cases
			  • Intrusion Detection
			  • Secure Design
			  • Attack Simulation
				• Analysis of Risky Design Decisions
				• Blockchain-based Engineering Data Logistics
				• Distributed Randomness
				• More details: https://blockchain.sba-research.org/

Conclusion

- Time to change our attacker model:
  - Attackers know everything about the physical process under control (or at least enough to cause disastrous consequences)
- Past has shown:
  - Attacks against ICSs are high-impact, low-frequency (HILF) events
  - However, frequency continuous to increase
- Time to rethink our engineering approach:
  - “Security by Design” & securing the engineering process
- Emerging cyber insurance market, but many open challenges
- Multidisciplinary research approach required

References

(Dragos, 2018) Dragos, Inc., “Industrial control vulnerabilities: 2017 in review,” Dragos, Inc., techreport, Mar. 2018.

(Eckhart et al., 2019) Eckhart, Matthias and Ekelhart, Andreas and Lüder, Arndt and Biffl, Stefan and Weippl, Edgar, “Security Development Lifecycle for Cyber-Physical Production Systems“. In Proc. of the 45th Annual Conference of the IEEE Industrial Electronics Society (IECON’19), Lisbon, Portugal. IEEE, October 2019.

(Forcepoint, 2018) Forcepoint, “AutoCAD Malware - Computer Aided Theft”, Nov. 2018: https://www.forcepoint.com/blog/x-labs/autocad-malware-computer-aided-theft

(ZDNet, 2018) ZDNet, “New industrial espionage campaign leverages AutoCAD-based malware”, Nov. 2018: https://www.zdnet.com/article/new-industrial-espionage-campaign-leverages-autocad-based-malware/

(F-Secure Labs, 2019) F-Secure Labs, “AutoCAD - Designing a Kill Chain”, Feb. 2019: https://labs.f-secure.com/blog/autocad-designing-a-kill-chain/

(Assante & Lee, 2015) Assante, Michael J. and Lee, Robert M. “The Industrial Control System Cyber Kill Chain”, SANS Institute, Oct. 2015.

(Langner, 2013) Langner, Ralph “To kill a Centrifuge: A Technical Analysis of What Stuxnet’s Creators Tried to Achieve”, Nov. 2013.

(Lee et al., 2016) Lee, Robert M. and Assante, Michael J. and Conway, Tim “Analysis of the Cyber Attack on the Ukrainian Power Grid”, SANS Institute, Mar. 2016.

(Dragos, 2017) Dragos, Inc., “CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations”, Dragos, Inc., techreport, June 2017.

(Dragos, 2019) Dragos, Inc., “CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack”, Dragos, Inc., techreport, Aug. 2019.

(Dragos, 2017a) Dragos, Inc., “TRISIS Malware: Analysis of Safety System Targeted Maware”, Dragos, Inc., techreport, Dec. 2017.

(Financial Times, 2019) Financial Times, “Mondelez sues Zurich in test for cyber hack insurance”, Jan. 2019: https://www.ft.com/content/8db7251c-1411-11e9-a581-4ff78404524e

(Wikipedia, 2009) Wikipedia, Black swan, 2009: https://en.wikipedia.org/wiki/File:Black_swan_jan09.jpg

(JLT, 2019) JLT, “Cyber Insurance for the Manufacturing sector”, 2019: https://www.jlt.com/insurance-risk/cyber-insurance/manufacturing

(PRA, 2017) Prudential Regulation Authority. Cyber insurance underwriting risk. Technical Report Supervisory Statement 4/17, Prudential Regulation Authority, July 2017.

(Coburn et al., 2019) Coburn, A. and Leverett, E. and Woo, G. “Solving Cyber Risk: Protecting Your Company and Society”. John Wiley & Sons, December 2018.

(Wikimedia, 2006) Wikimedia, Discharge pipe, 2006: https://commons.wikimedia.org/wiki/File:Discharge_pipe.jpg

DCNAustria

Disaster Competence Network Austria

Austrian Disaster Research Days 2019

14.-15.Oktober 2019, Technische Universität Graz

TU Wien (CDL-SQI) & SBA Research

Matthias A. Eckhart

Floragasse 7, A-1040 Wien

Tel.: +43 664 448 34 35

matthias.eckhart@tuwien.ac.at , https://sqi.at/, https://www.sba-research.org/