TÜV AUSTRIA

TU WIEN

#SafeSecLab

Angriffs- und Verteidigungskonzepte bei OT-Architekturen

Siegfried Hollerer

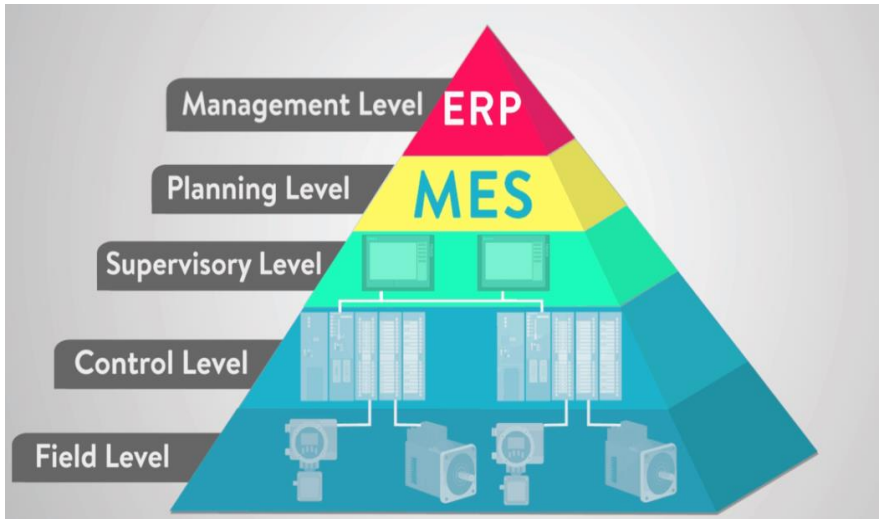
Agenda

#SafeSecLab

- Referenzarchitektur nach ANSI/ISA 95 - Purdue Model
- Herausforderungen
- Beispiele von Security-Vorfällen und deren Auswirkungen
- OT Angriffskonzept (Kill Chain)
- Netz- und Informationssystemsicherheitsgesetz und seine Anforderungen
- Überblick relevanter Sicherheitsnormen und –standards
- Allgemeines techn. Verteidigungskonzept
- Vorstellung #SafeSecLab

Referenzarchitektur nach ANSI/ISA 95 - Purdue Model

#SafeSecLab



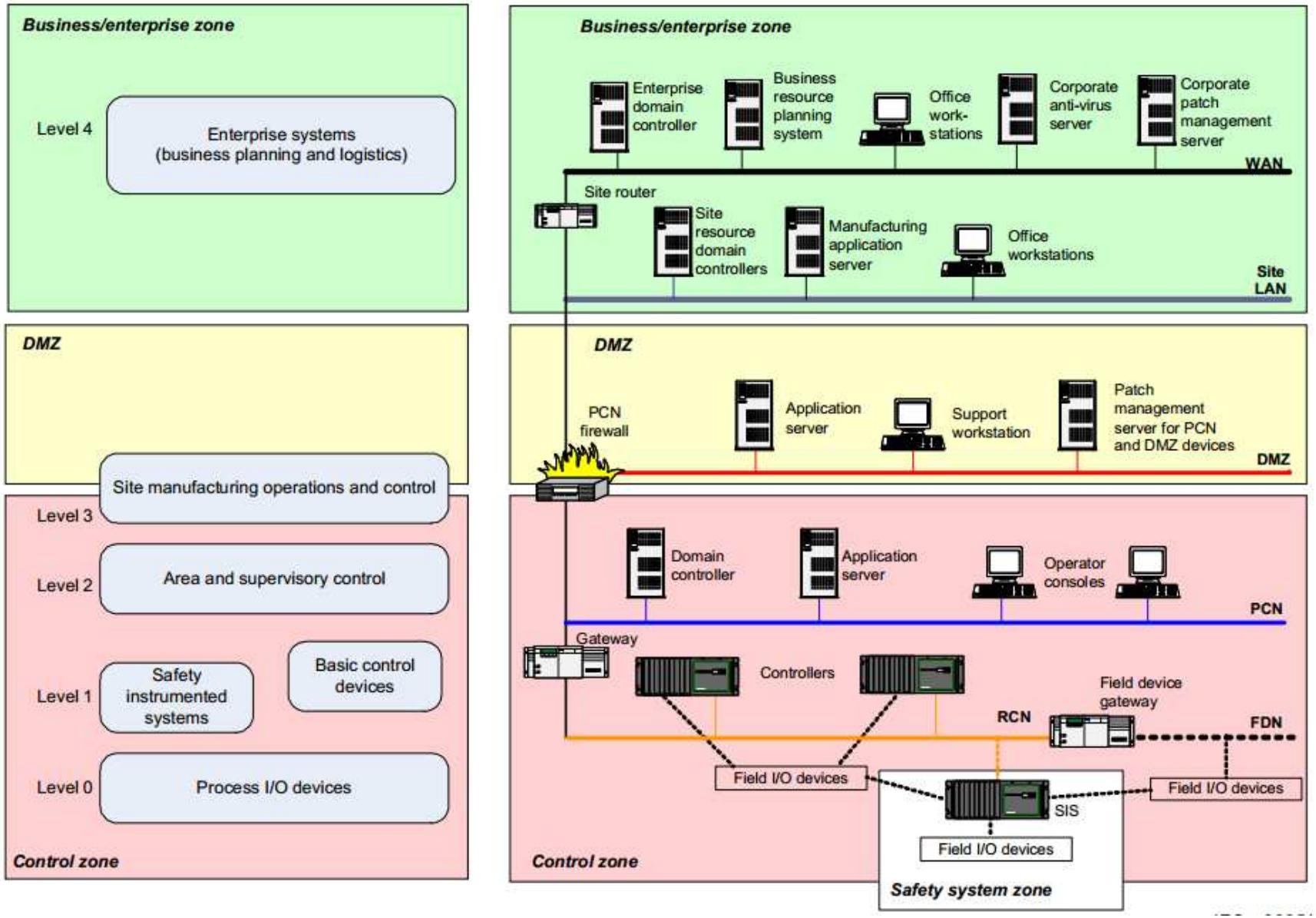
Level 4 *Business Planning*	ERP Work Management, Enterprise Data Systems	IT
Level 3 *Operations Management*	Production, Scheduling, Operations Management, Optimizing Process, Maintenance, Remote Access...	IT
Level 2 *Supervisory Control Applications*	SCADA, DCS, HMI, Industrial Control Systems	OT
Level 1 *Process Control Network (PCN)*	Automation Network (PCN), Safety Instrumented Systems (SIS)	OT
Level 0 *Physical Production Process*	Mechanical Process, Sensors, Actuators, Wiring and Field Devices	OT

Quelle: https://medium.com/world-of-iot/92-what-is-the-five-layer-automation-pyramid-d0ccc1b903c3

- IT
  - Enterprise-Systeme, Office-Netzwerke, Software zur Verarbeitung und Verteilung von Daten bei Produktionsanlagen
- OT
  - Hardware, Industrial Communication Systems (ICS), Software die technische Prozesse überwacht und steuert

Beispiel-Architektur nach Purdue Model

#SafeSecLab



Herausforderungen

#SafeSecLab

- Security-Anforderungen erfüllen
  - Confidentiality, Integrity, Availability (CIA Triade)

- Security-Anforderungen müssen im OT-Umfeld anders erfüllt werden
  - Andere Verfügbarkeits-Anforderungen
    - z.B.: Real-time communication
  - Lebenszyklus
    - 5 Jahre vs. 30 Jahre
  - Physische Interaktion
    - Sensoren und Aktuatoren interagieren mit “realer Welt”
  - Kommunikation
    - Modbus, Profibus, (wireless)HART, Siemens S7, MQTT, OPC(UA), etc.
  - ...

Herausforderungen

#SafeSecLab

- Safety-Anforderungen müssen erfüllt werden
  - Personen müssen vor Verletzungen und Umwelt vor Schaden durch OT-Komponenten geschützt werden
- Security und Safety hängen voneinander ab
  - Ausnutzen einer Schwachstelle kann zu Safety-Auswirkungen führen und umgekehrt!

Beispiele Security-Vorfälle

#SafeSecLab

ANDY GREENBERG SECURITY 09.06.2017 06:00 AM

Hackers Gain Direct Access to US Power Grid Controls

Hackers who hit American utilities this summer had the power to cause blackouts, Symantec says.

eport on the new intrusions details, the cked the Dragonfly 2.0 attacks back to at mber of 2015, but found that they ramped up significantly in the first half of 2017, particularly in the US, Turkey, and Switzerland. Its analysis of those breaches found that they began with spearphishing emails that tricked victims into opening a malicious attachment—the earliest they found was a fake invitation to a New Year's Eve party—or so-called watering hole attacks that compromise a website commonly visited by targets to hack victims'

24 JUN 2014 NEWS

Watering Hole Hackers Sniff Out Industrial Control Systems for Future Attack

Beispiele Security-Vorfälle

Petya-Virus legt Kernkraftwerk Tschernobyl lahm

3 7 41

PANORAMA 20:58 27.06.2017 Zum Kurzlink

Das Kernkraftwerk Tschernobyl ist laut ukrainischen Medien mit der Ransomware Petya, die sich am Dienstag rasant in der Welt verbreitete, angegriffen worden.

Laut einem Vertreter des Kraftwerks wurde der Dokumentendurchlauf nfiziert. Radioaktive Bedrohung bestehe jedoch nicht.

Sobald bekannt geworden sei, dass einige Computer am Kraftwerk nfiziert worden seien, hätten Mitarbeiter diese umgehend ausgeschaltet.

Gleichzeitig sei die offizielle Seite des Kernkraftwerks unverfügbar geworden. Die Radioaktivität werde nun manuell überwacht. heißt es.

© SPUTNIK / ALEKSEJ WITWITZKIJ

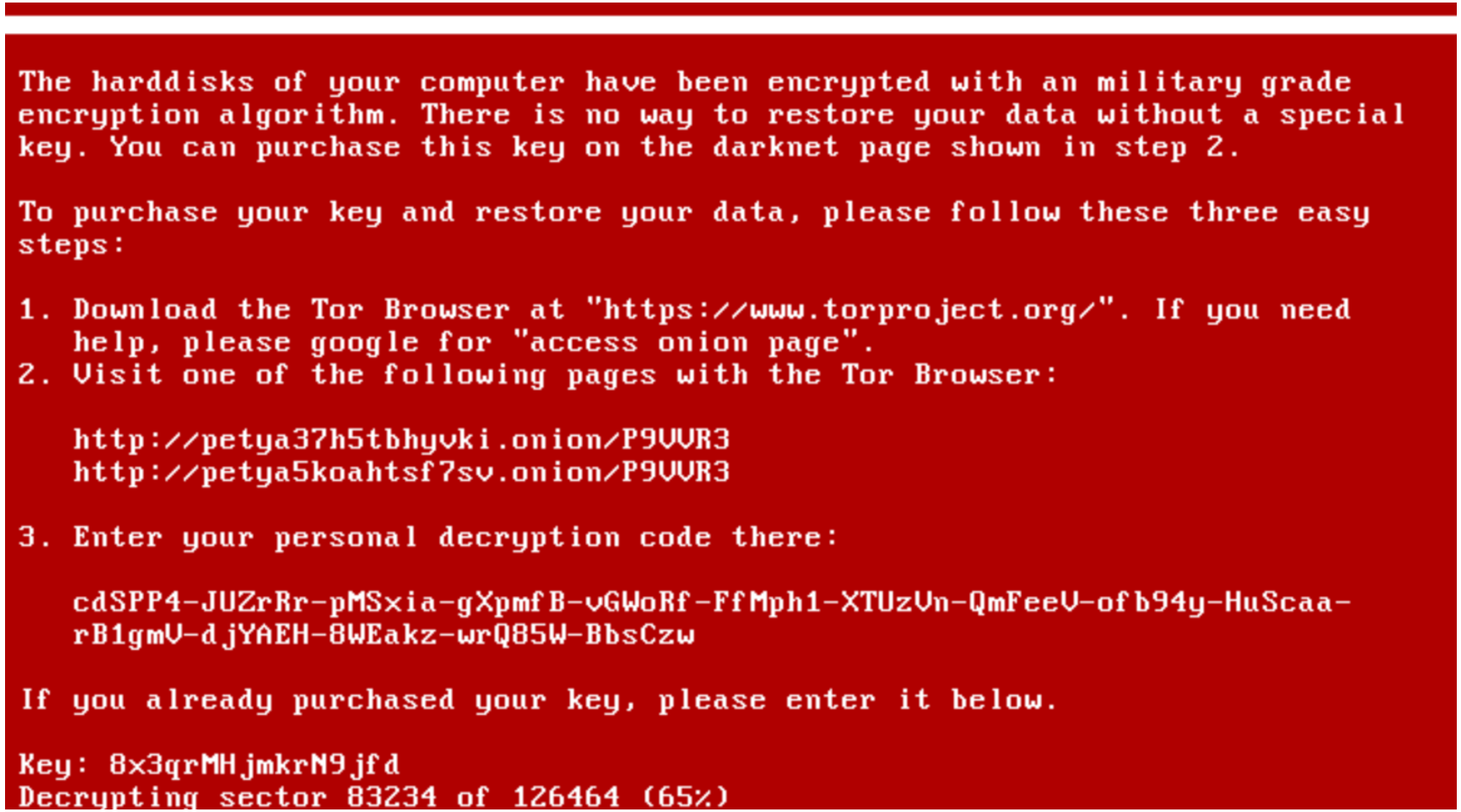
Rückkehr von Petya: Hacker greifen nun Firmen in EU an

Digital Life 15.12.2017

Neuer Cyberangriff zeigt Gefahr für Kraftwerke auf

Bei einem Cyberangriff am Donnerstag wurde Sicherheits-Technologie von Schneider Electric angegriffen. Diese kommt in zahlreichen Kraftwerken und Fabriken zum Einsatz.

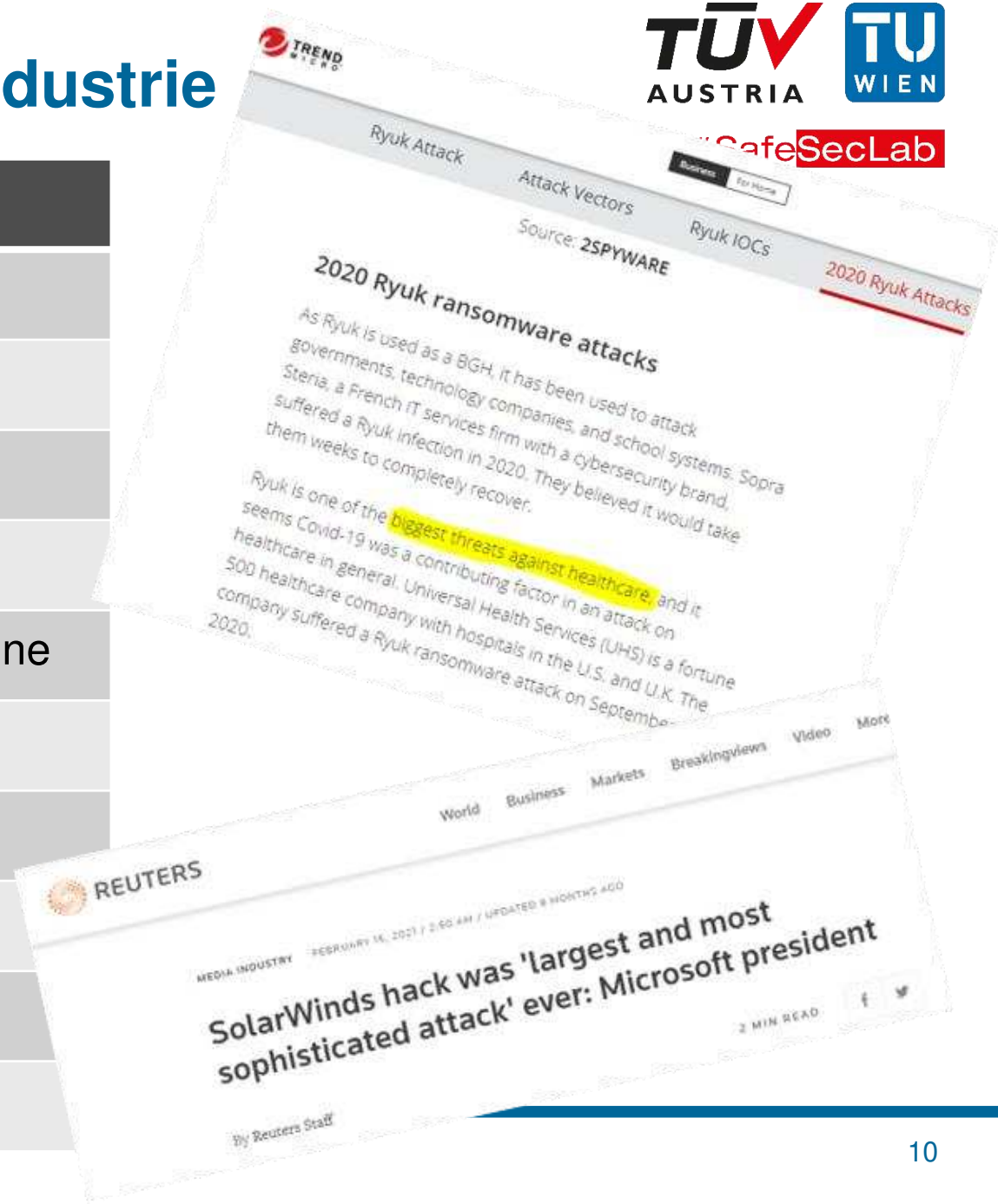
Beispiele Security-Vorfälle in der Industrie



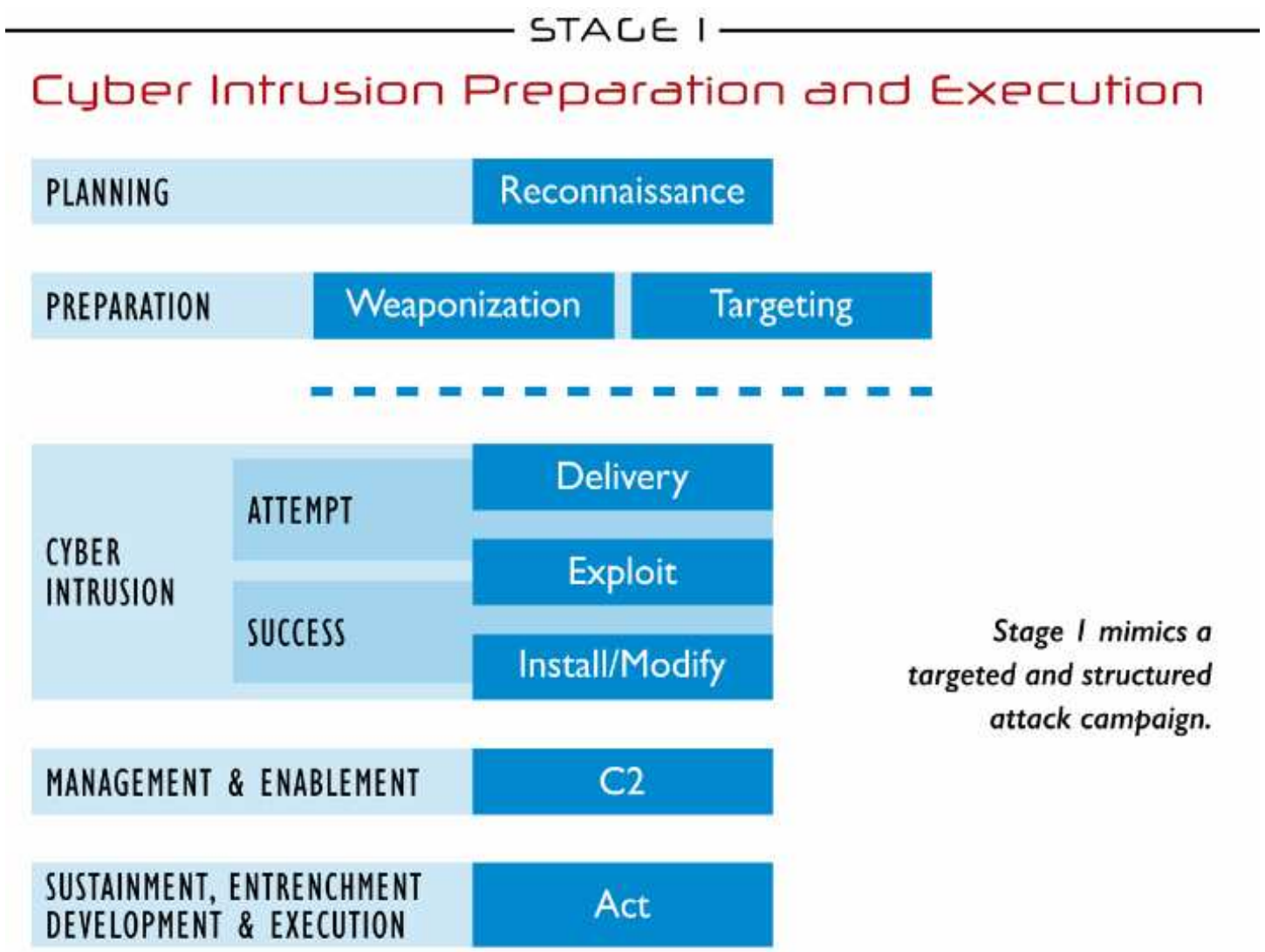
Quelle: https://www.notebookcheck.net/fileadmin/Notebooks/News/_nc3/decrypting_petya.png

Weitere Security-Vorfälle in der Industrie

Jahr	Angriff
2008	Agent.bz
2010	Stuxnet
2011	Night Dragon Attacks
2014	Havex
2015	BlackEnergy stört Stromversorgung der Ukraine
2017	TRITON / TRISIS
2018	Ryuk
2019	LockerGoga
2020	SolarWinds
2021	Cyber-Angriff gegen US Öl- und Gaspipeline



OT Angriffskonzept (Kill Chain) – Stage 1



Stage 1 mimics a targeted and structured attack campaign.

Quelle: https://sansorg.egnyte.com/dl/HHa9fCekmc

OT Angriffskonzept (Kill Chain) – Stage 1

TÜV AUSTRIA TU WIEN
#SafeSecLab

- Planning
  - **Reconnaissance**: Information gathering
    - Aktiv/Passiv (inkl. OSINT)

- Preparation
  - **Weaponization**: Schädliche Dateien generieren
    - z.B.: PDFs, Scripte, Binaries, etc.
  - **Targeting**: Eintrittsvektor aussuchen
    - z.B.: Internet-facing Firewall für VPN-Verbindungen, WebServer, e-Mail Server

OT Angriffskonzept (Kill Chain) – Stage 1

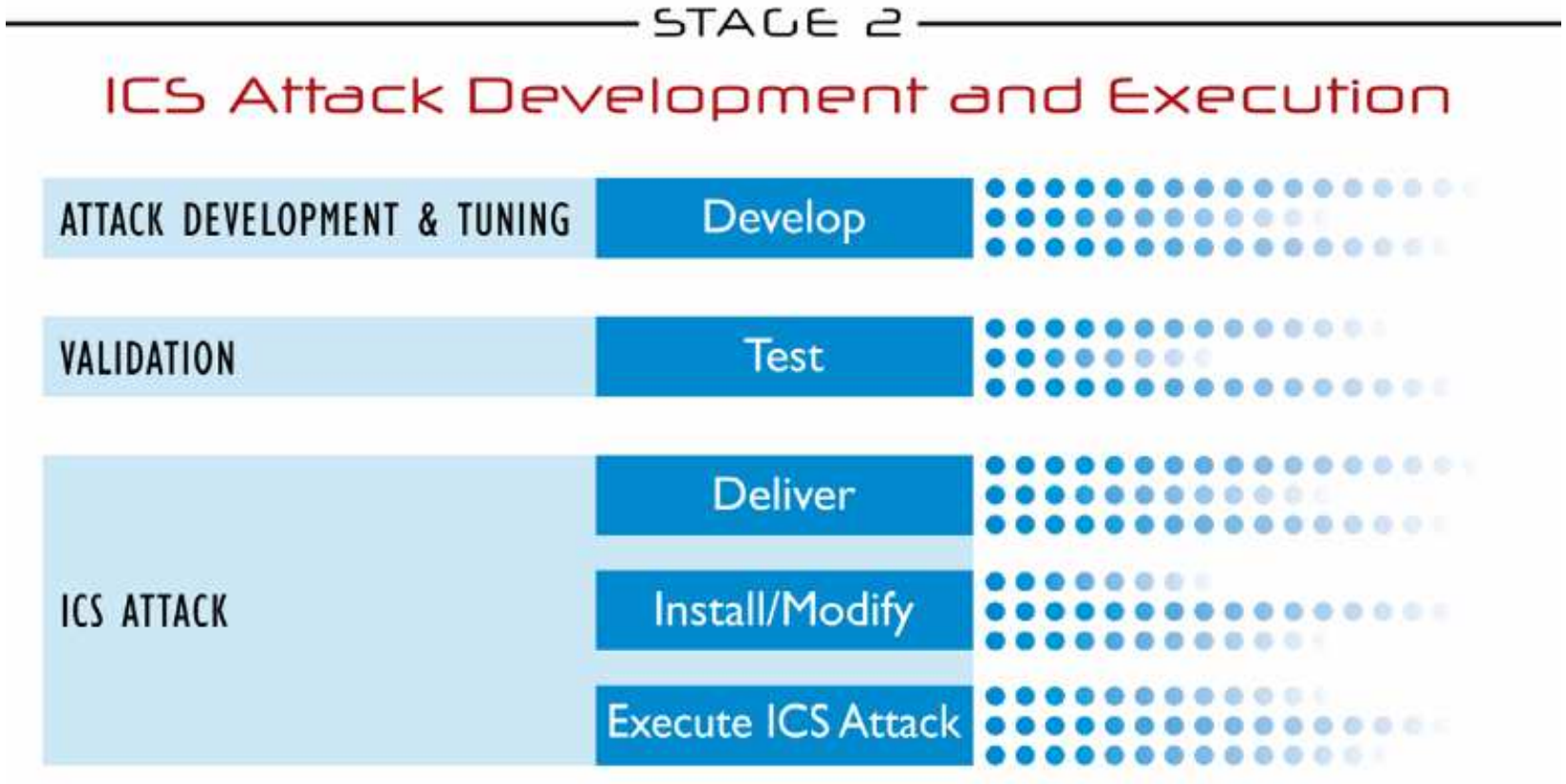
- Cyber Intrusion
  - **Delivery**: Schädliche Dateien (aus Phase *Weaponization*) zum Ziel übertragen
    - Z.B.: Phishing Mail liefert schädliche PDF-Datei
  - **Exploit:** Schwachstelle wird ausgenutzt
    - Z.B.: Öffnen des schädlichen PDFs
  - **Install/Modify:**
    - Privilege Escalation
    - Installation eines Trojaners
    - Vorhandene Boardmittel verwenden
      - PowerShell, cmd, bash, pyhton, ruby, gcc, etc.

OT Angriffskonzept (Kill Chain) – Stage 1

- Management and Enablement Phase
  - **C2 (command and control):** Peristenten Zugriff einrichten
    - Kann in gängiger ein- und ausgehender Kommunikation versteckt, bestehende Verbindungen werden übernommen
    - Einschleusen von Ausrüstung (z.B.: LAN-Turtle)

- Sustainment, Entrenchment, Development & Execution
  - **Act:** Eigentliche Ziele angreifen
    - Neue Systeme/Daten im Netzwerk analysieren
    - Datendiebstahl
    - Verschlüsselung von Daten, Platzierung von Ransomware

OT Angriffskonzept (Kill Chain) – Stage 2



Quelle: https://sansorg.egnyte.com/dl/HHa9fCekmc

OT Angriffskonzept (Kill Chain) – Stage 2

TÜV AUSTRIA TU WIEN
#SafeSecLab

- Attack Development and Tuning
  - Architekturspezifischer, individueller Angriff wird entwickelt
    - Meistens offline, auf Basis der exfiltrierten Daten über die OT-Architektur
    - Schwer zu entdecken
    - Großer zeitlicher Abstand zwischen Stage 1 und hier
- Validation
  - Testen den Angriffs gegen ähnlich oder identisch konfigurierte Systeme bzw. Komponenten

OT Angriffskonzept (Kill Chain) – Stage 2

- ICS Attack
  - Vgl. Stage 1 – Cyber Intrusion
  - Prozessspezifische Auswirkungen
    - Denial / Loss / Manipulation of
      - View
      - Control
      - Safety

NISG – Netz- und Informationssicherheitsgesetz

- Ziel: Steigerung des Sicherheitsniveaus (security)

- Betrifft aktuell Unternehmen, die eine hohe Bedeutung für das Funktionieren des Gemeinwesens haben (kritische Infrastruktur)

Geforderte Sicherheitsvorkehrungen (Auszug)

- Teil 1 - Governance und Ökosystem
  - Risikomanagement
    - Risikoanalyse
    - Sicherheitsrichtlinie
    - Personalwesen
  - Umgang mit Lieferanten und Dritten

- Teil 2 – Schutz
  - Identitäts- und Zugriffsmanagement
  - Systemwartung und Betrieb
  - Physische Sicherheit

Geforderte Sicherheitsvorkehrungen (Auszug)

- Teil 3 – Verteidigung
  - Incident response / Incident management
  - Erkennung von Vorfällen
  - Bewältigung von Vorfällen

- Teil 4 – Resilienz
  - BCM (Betriebskontinuitätsmanagement)
  - Krisenmanagement

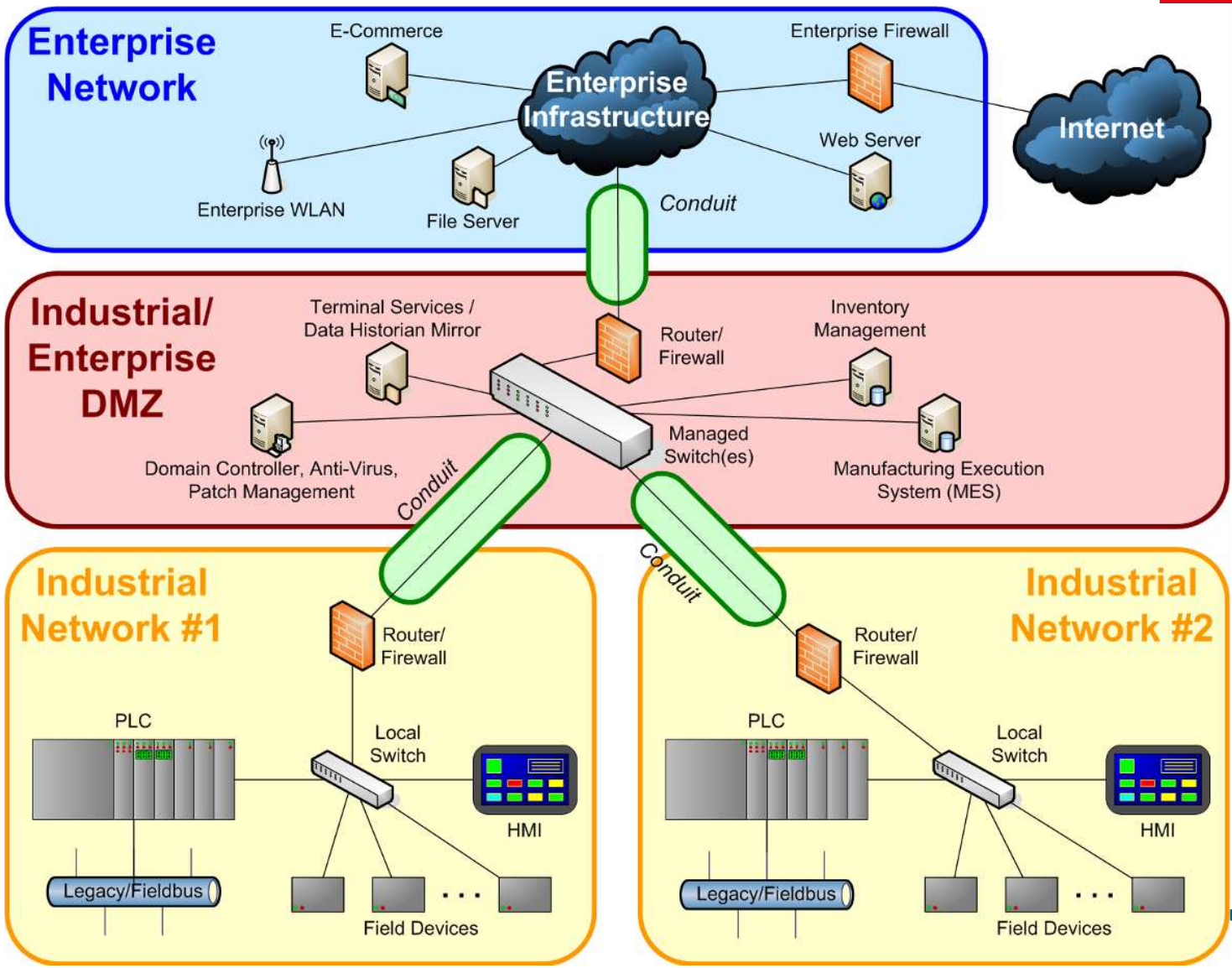
Überblick relevanter Sicherheitsnormen und - standards

- IEC 62443
- NIST Special Publication 800-82 Revision 2
- NIST Cybersecurity Framework
- BSI ICS-Security-Kompendium

Allgemeine Security-Konzepte (laut IEC 62443)

#SafeSecLab

Teilen der Architektur
in Zonen und Conduits



Quelle: https://blogs.cisco.com/security/securing-industrial-networks-what-is-isa-iec-62443

Foundational Requirements nach IEC 62443

TÜV AUSTRIA TU WIEN

#SafeSecLab

FR No.	Abbr.	Title (english)
1	IAC	Identification and Access Control
2	UC	Use Control
3	SI	System Integrity
4	DC	Data Confidentiality
5	RDF	Restricted Data Flow
6	TRE	Timely Response to Events
7	RA	Ressource Availability

Allgemeines techn. Verteidigungskonzept nach IEC 62443

- FR 1 - Identifizierung und Authentifizierung
  - z.B.: Default credentials, shared accounts, Passwortkomplexität, erlaubte Anmeldeversuche
- FR 2 – Autorisierung / Nutzungskontrolle
  - z.B.: Principle of least privilege, Berechtigung von Funk- und Fernzugriffen, Session Management
- FR 3 – Integrität
  - z.B.: Schadsoftwareschutz(z.B.: Anti-Virus, Whitelisting), Input Validation, Error handling
- FR 4 – Vertraulichkeit
  - z.B.: Verschlüsselung, Entsorgung von Datenträgern

Allgemeines techn. Verteidigungskonzept nach IEC 62443

- FR 5 – eingeschränkter Kommunikationsfluss
  - z.B.: Netzwerksegmentierung, Absicherung der Kommunikation (z.B.: durch Firewalls)
- FR 6 - Incident response (techn.)
  - z.B.: Log management, Log accessability, ggf. SIEM
- FR 7 – Availability
  - Z.B.: DoS-Schutz, Backups, Notfall-Stromversorgung, Principle of least functionality

Zusammenfassung

Quelle: https://scontent-vie1-1.xx.fbcdn.net/v/t1.6435-9/219229103_530757591584775_3084930068777890790_n.jpg?_nc_cat=101&_nc_rgb565=1&ccb=1-5&_nc_sid=825194&_nc_ohc=lrW_7lHiL3wAX_c2NTc&tn=YAGqkzFhCSXrqNW2&_nc_ht=scontent-vie1-1.xx&oh=adc4647f1a5c72b60f46fcf6fc31c9ca&oe=614310A8

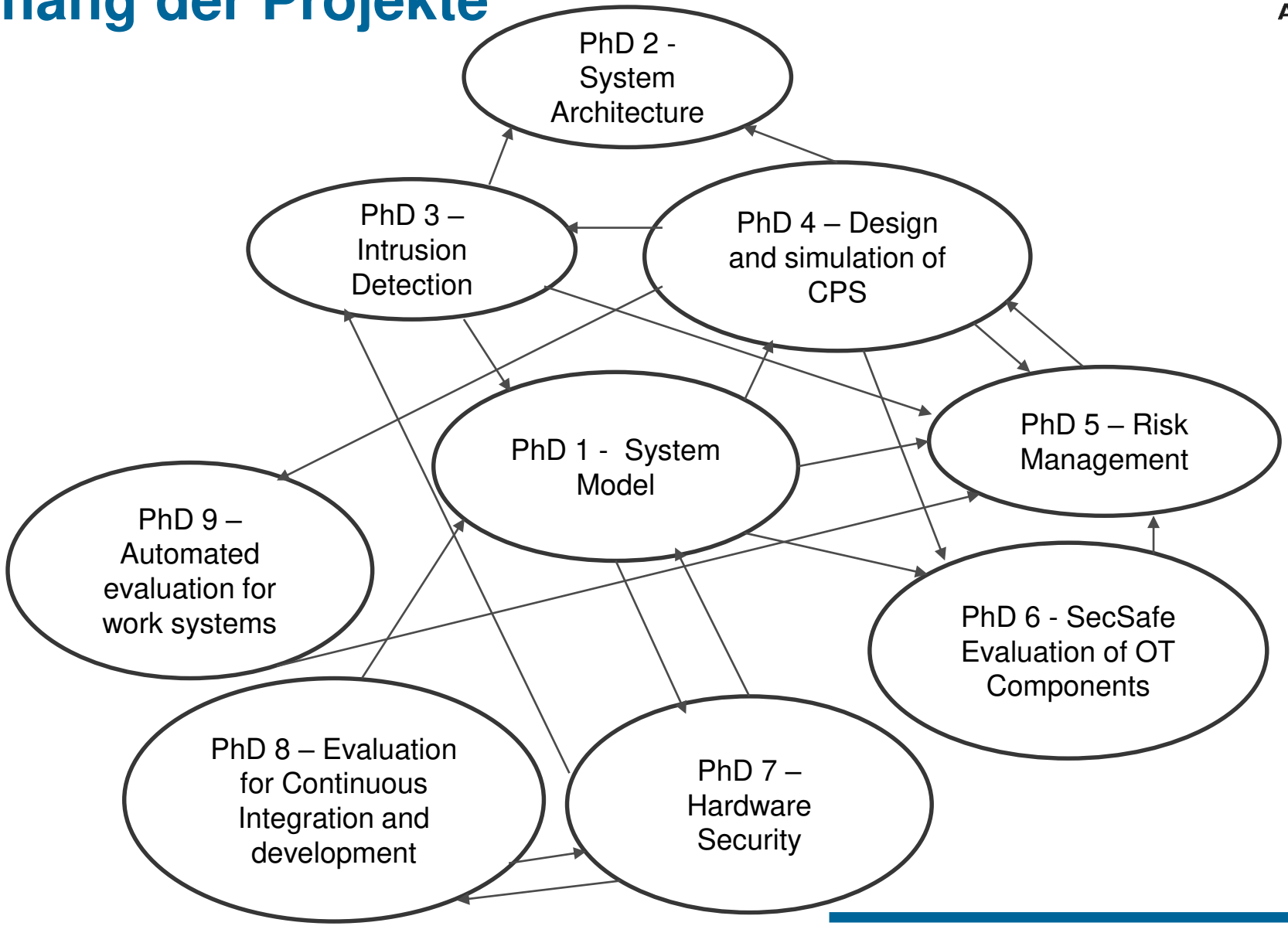
TÜV AUSTRIA #SafeSecLab

Die österreichische Initiative für industrielle Safety & Security

9 PhD Projects

P1: SafeSec System Modeling	Q4 2020 – Q3 2024
P2: SafeSec System Architecture	Q4 2020 – Q3 2024
P3: Multi-Dimensional Intrusion Detection for Industrial Control Systems	Q1 2020 – Q4 2023
P4: Sicherheitsgerichtetes Design und Simulation von cyberphysischen Arbeitssystemen	Q1 2020 – Q4 2023
P5: Automated Risk Management for Industrial Control Systems	Q4 2020 – Q3 2024
P6: Model-based Security & Safety Evaluation of OT Components	Q1 2021 – Q4 2024
P7: Design-Time Hardware-Security Verification	Q4 2020 – Q3 2024
P8: Sicherheitsgerichtete Bewertungsverfahren für Continuous Integration and Deployment	Q1 2021 – Q4 2024
P9: Automatisierte Sicherheitsbewertungsverfahren für dynamisch rekonfigurierbare Arbeitssysteme	Q1 2021 – Q4 2024

Zusammenhang der Projekte



Quellen

- S. Hollerer, W. Kastner and T. Sauter, “Towards a Threat Modeling Approach Addressing Security and Safety in OT Environments,” *2021 17th IEEE International Conference on Factory Communication Systems (WFCS)*, pp. 37-40, doi: 10.1109/WFCS46889.2021.9483591, 2021
- S. Hollerer, W. Kastner and T. Sauter, "Safety und Security – ein Spannungsfeld in der industriellen Praxis", *Elektrotech. Inftech.* 138**,** pp. 449–453 https://link.springer.com/content/pdf/10.1007/s00502-021-00930-0.pdf, 2021
- Hollerer et al. “Cobot attack: a security assessment exemplified by a specific collaborative robot”, Elsevier, ISSN 2351-9789, https://doi.org/10.1016/j.promfg.2021.07.029, 2021
- Thomas Schulz, „Cybersicherheit für vernetzte Anwendungen in der Industrie 4.0“, Volume 1. Vogel Fachbuch, 2020.
- Clint Bodungen et al. „Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions”, ISBN 9781259589713, https://www.mhebooklibrary.com/doi/book/10.1036/9781259589720 , 2016

Quellen: Security-Vorfälle und Kill Chain

- https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/
- https://www.cyber.nj.gov/threat-center/threat-profiles/ics-malware-variants/stuxnet
- https://t3n.de/news/petrwrap-ransomware-833930/
- https://www.nozominetworks.com////downloads/US/Nozomi-Networks-TRITON-The-First-SIS-Cyberattack.pdf
- https://www.ncsc.gov.uk/files/RYUK%20Advisory%20draft%20CP%20June%202019.pdf
- https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware/
- https://www.cisecurity.org/solarwinds/
- https://sansorg.egnyte.com/dl/HHa9fCekmc

Contact Information

Siegfried Hollerer

Senior Consultant
TÜV TRUST IT TÜV AUSTRIA GmbH

Project Assistant
Research Area Automation Systems

TU Wien
Faculty of Informatics
Institute of Computer Engineering

siegfried.hollerer@tuwien.ac.at
siegfried.hollerer@tuv.at

https://at.linkedin.com/in/siegfried-hollerer-1ab397162
https://orcid.org/0000-0002-3814-6019