Know-how Vorsprung durch Wissenstransfer: Projekte und Forschung zur IT-Sicherheit in der Produktion

27.10.2021

Bayern Innovativ Cluster Workshop
IT-Sicherheit in der Produktion - Einblicke für das Management

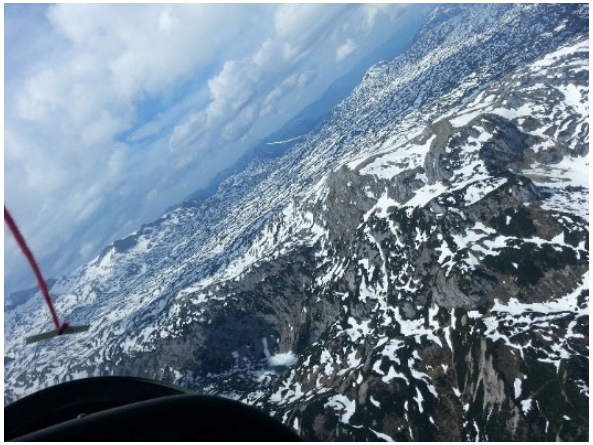
Prof. Dr.-Ing. Andreas Grzemba

Vizepräsident

Leiter des Instituts ProtectIT

Prof. Dr.-Ing. Andreas Grzemba

- Studium: Technische Kybernetik und Automatisierungstechnik
- Vizepräsident F&E der TH Deggendorf
- Lehre: Digitaltechnik, Sensor-Aktor-Netzwerke, Echtzeitsysteme, Systemprogrammierung
- Forschung: In-Car Kommunikationssysteme, Embedded Security
- Leiter des Instituts ProtectIT
- Zweiter Vorstand des Verein Technik für Kinder (www.tfk-ev.de)
- Hobby: Segelflug

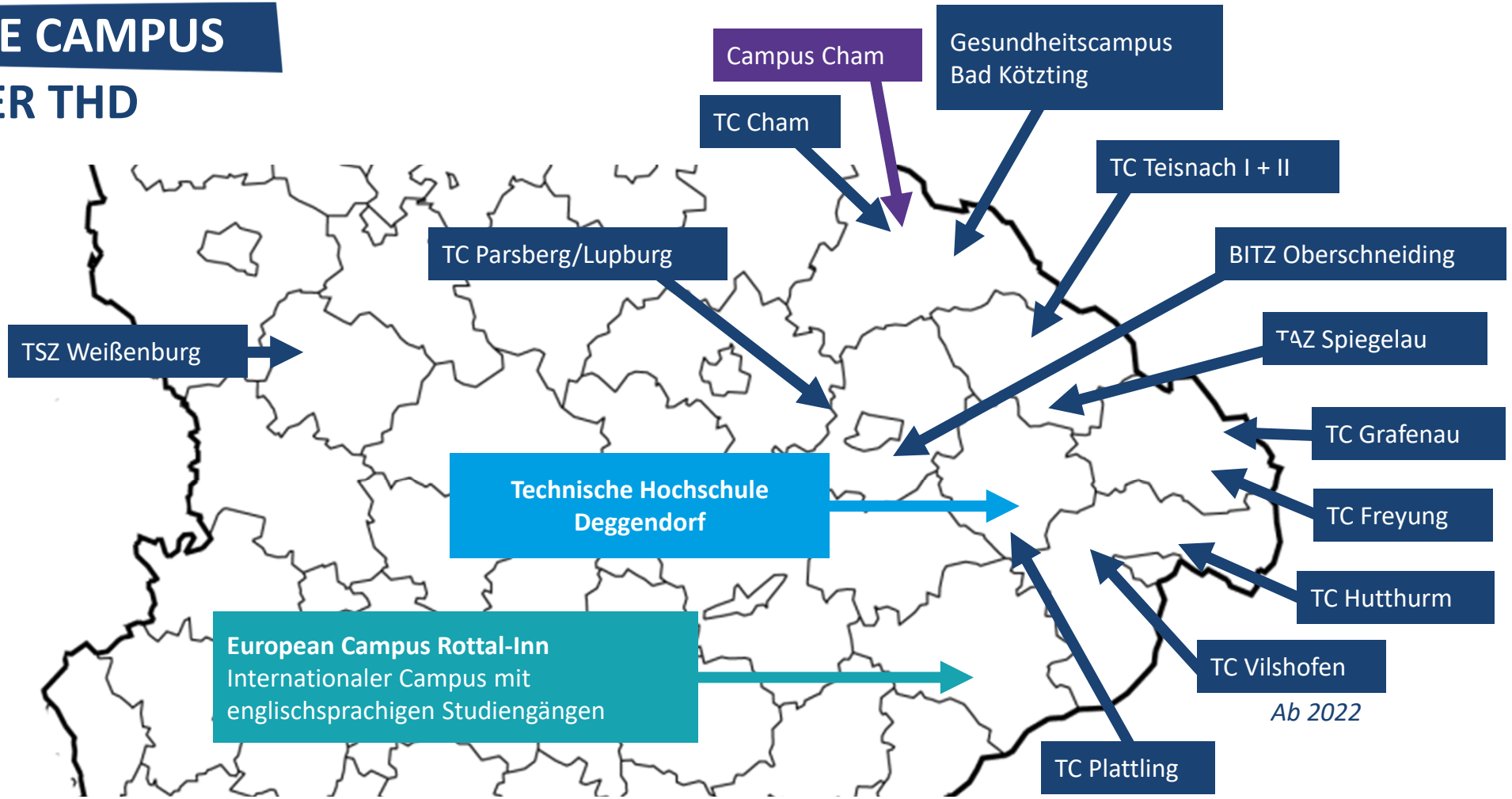


DIE THD IN ZAHLEN

- 8 Fakultäten
- 35 Bachelorstudiengänge
- 20 Masterstudiengänge
- 6 Weiterbildungs-Bachelor
- 7 Weiterbildungs-Master (inklusive 2 MBA)
- 12 Innovations- und Technologiecampus

- 7850 Studierende
- 159 Professor:innen
- 335 Dozierende und Lehrbeauftragte
- 776 Mitarbeiter:innen

DIE CAMPUS DER THD



TC VILSHOFEN

CAMPUS FÜR CYBER SECUIRTY

Technische Hochschule Deggendorf

Lehre:	Bachelor Cyber Security
	Weiterbildungs-Master Cyber Security (Schwerpunkte Industrie & Automotive)
Angewandte Forschung:	Institut ProtectIT
Start-up:	ProtectEM →TG alpha

Fields of Research

ProtectIT

DIGITAL:

Digital Business and Society

- Industrie 4.0
- Big data / data analytics
- Industrial & IT security
- Embedded systems, communication and software
- Digital living environments / eVillage
- Environment, spacial planning, information & society

SUSTAINABILITY:

Sustainable Business, Innovative Materials & Energy

- Renewable resources and resource efficiency
- Applied energy research & electro mobility
- Bionics
- Nano technology & new materials
- Construction and sustainability
- Sustainable plastics
- Regional sustainability

MOBILE:

Intelligent Mobility

- Mobility concepts for the future
- Autonomous driving
- E-mobility
- Geo information technology
- Traffic management
- Tourism

HEALTH:

Innovative Working Environments & Well Being

- Ethics and health sciences
- Health management
- Demographic change
- Health and nursing sciences
- DIT Vitality

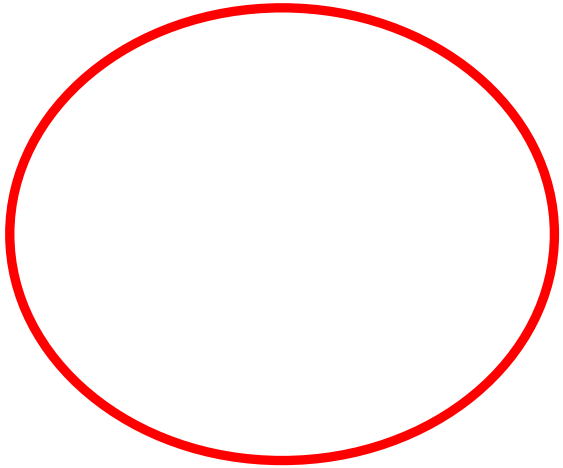
Herausforderungen

NHTSA Cybersecurity Framework : Identify, Protect, Detect, Respond, and Recover

Identifizieren von Security Risken

Schutz gegen Eindringen - Härten

Datenschutz
Löschen von nicht benötigten Daten



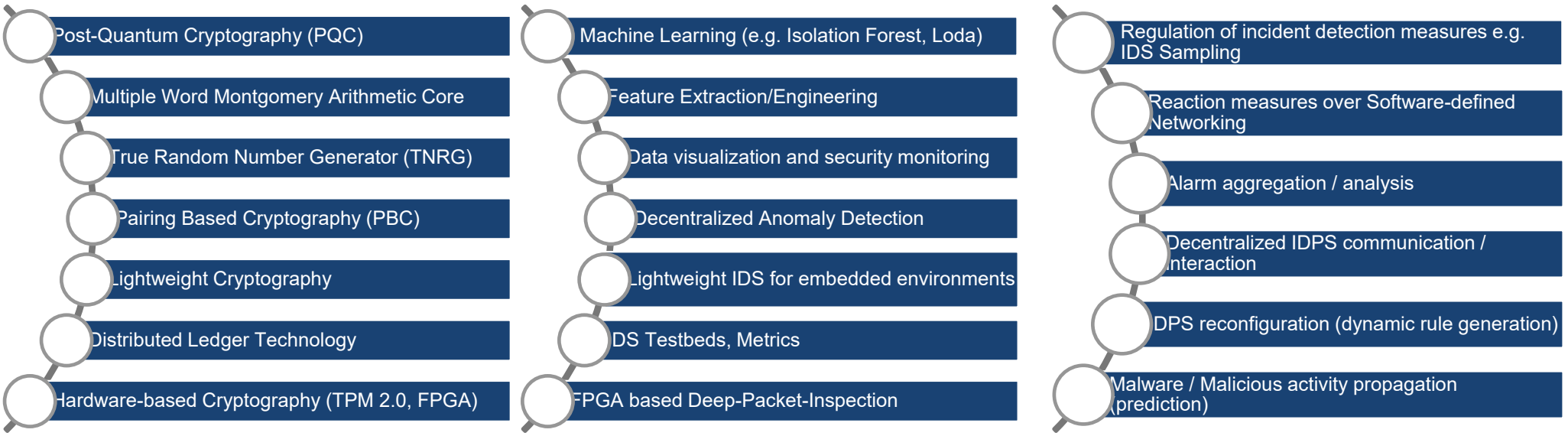
Erkennen von Angriffen - Intrusion Detection Systems (IDS)

Analyse von Angriffen - Forensik

Reaktion – Wiederaufsetzen des Systems
Security Information and Event Management (SIEM)

Organisation

- TCV & ProtectIT



INSITUTE PROTECTIT

ProtectIT

Erfolgreich Abgeschlossen F&E Projects

- **ANSII** - Anomalieerkennung und eingebettete Sicherheit in industriellen Informationssystemen
- **SiNeMA** - Sicherheit in industriellen Netzwerken durch intelligente Methoden zur Anomalieerkennung und Integritätsprüfung
- **KoDaK** - Koexistenz verschiedener Datenverkehrs-Klassen im Fahrzeug und Flugzeug
- **HiS_Switch** - High Safety and Security for Onboard Switches
- **SURF** - Systemic Security for Critical Infrastructures
- **Sec-BIT** - Secure Cloud-based Smart Building and Infrastructure Technology
- **DecADe** - Decentralized Anomaly Detection
- **PCN-Sec** - Process Control Network Security
- **SeSaRe** - Security in Safety-Critical Environments of Real-Time Automotive Domains
- **SmartDefense** - Anomalieerkennung in Energienetzen

Aktuelle Projekte

- **MLPaSSAD** - New Multi-Layer Platforms for Security and Safety-Relevant Automated Driving Functions
- **VITAF** - Vertrauenswürdige IT für autonomes Fahren
- **SKINET** - Proaktive Sicherheit durch Künstliche Intelligenz in automobilen und industriellen IT-Netzwerken
- **SHORT** - Security-Centered HiL-Platform Offering Risk-aware Testing
- **iAATG** - innovative Absicherungskonzepte für die Anlauftauglichkeit Gesamtfahrzeug
- **SISSeC** - Secure Industrial Semantic Sensor Cloud
- **IIOT BMC** – Industrieller IoT Board Management Controller als Erweiterungsmodul für zukünftige COMs

Projekte in Vorbereitung

- SecCONDIS
- FORDaySec
- (APOLO, SmartEnergy, …)

AKTUELLE FORSCHUNGSARBEITEN

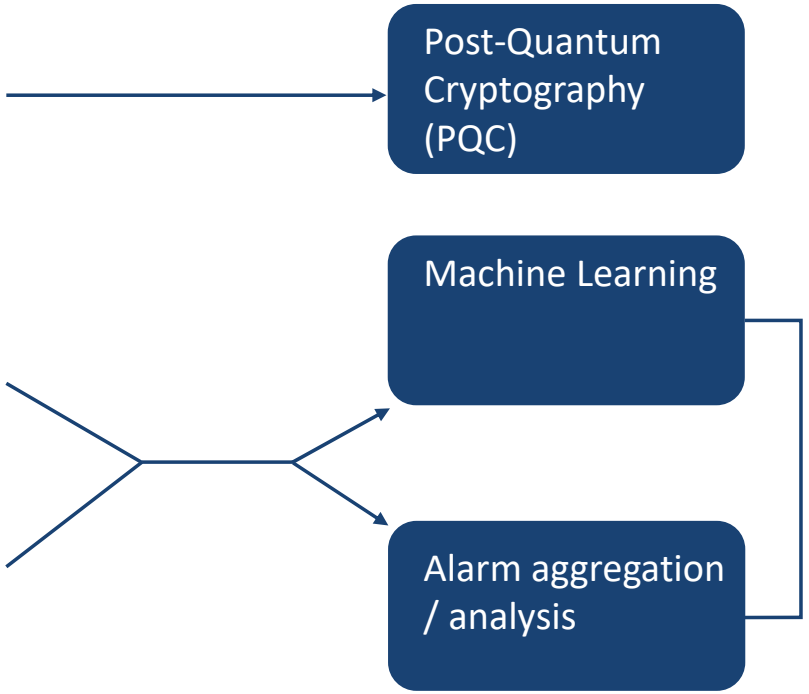
TCV & PROTECTIT

Veröffentlichung:

“On the Energy Consumption of Quantum-resistant Cryptographic Software Implementations Suitable for Wireless Sensor Networks “ [1]

“On the Improvement of the Isolation Forest Algorithm for Outlier Detection with Streaming Data” [2]

“Exploiting the Outcome of Outlier Detection for Novel Attack Pattern Recognition on Streaming Data” [3]

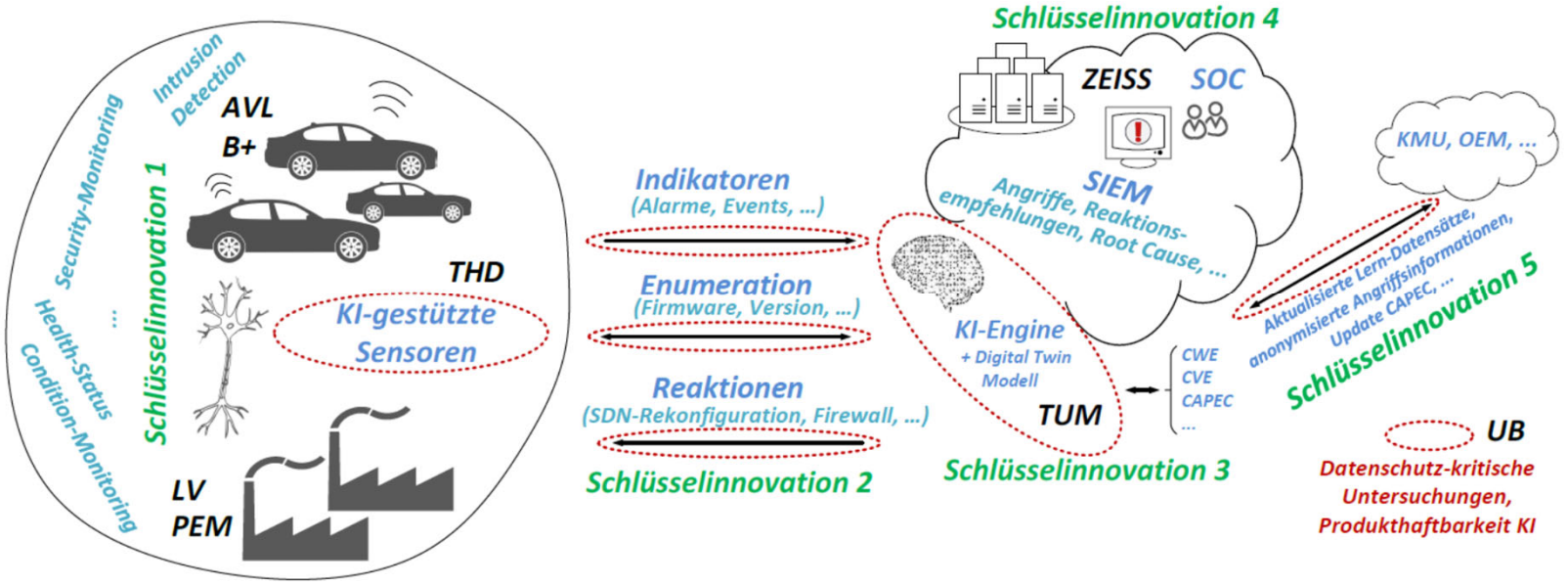


1 Quelle: https://www.scitepress.org/Papers/2019/78356/78356.pdf
2 Quelle: https://www.mdpi.com/2079-9292/10/13/1534
3 Quelle: https://www.mdpi.com/2079-9292/10/17/2160

SKINET

Proaktive Sicherheit durch Künstliche Intelligenz in automobilen und industriellen IT-Netzwerken

Gefördert aus dem BMBF-Call: Gebiet „Künstliche Intelligenz für IT-Sicherheit“ im Rahmen des Förderprogramms „Selbstbestimmt und sicher in der digitalen Welt 2015 bis 2020“



- Erkennung und Verarbeitung von Anomalien auf verschiedenen Ebenen
- Anwendung von Prinzipen aus dem Edge-Computing: Autarke Erkennung und Behandlung von Vorfällen möglichst Nahe an der Datenquelle
- Weiterleitung der Anomalien an höhere Instanz

- Entwicklung von KI-gestützten Systemen zur proaktiven Erfassung, Behandlung und Aufklärung von IT-Sicherheitsvorfällen
- Bildung eines hierarchischen Anomaliedetektionsnetzwerks

SKINET

Automotiveusecase

- Behandlung der Anomalien auf Sensorebene (Zusammenarbeit THD mit AVL)
  → Verarbeitung von Adversarials
- Adversarials: Negative Beeinflussung der Objekterkennung durch böswillige Veränderung der Umgebung (→ Bösartiges Auslösen von Reaktionsmechanismen)
  - Verkleben von Stopschildern
  - Projektion von Schildern
  - Injektion von falschen Lidarpunkten
  - Etc.
- Detektion durch Convolutional Neural Networks (CNN)
- Testung der Anomalieerkennung mithilfe eines Demonstrators (AVL-Rooftopbox)

SKINET

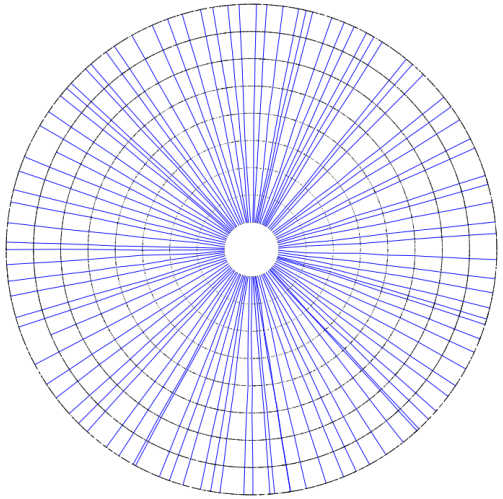
Industrialcase

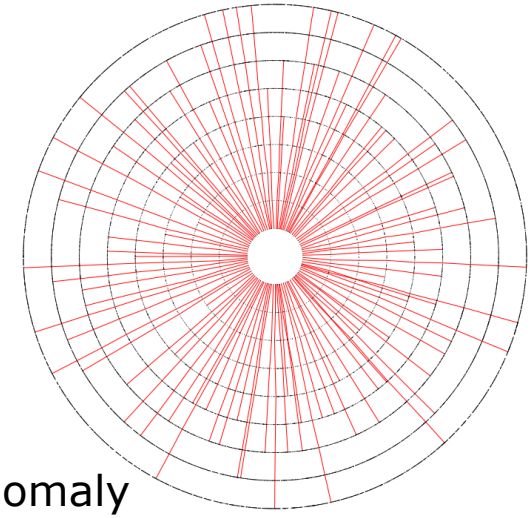
- Behandlung der Anomalien auf Kommunikationsebene (Zusammenarbeit THD mit TG-Alpha)
  → Verarbeitung auf Netzwerkpaketen
- Erkennung von maliziösem Informationsaustausch
  - Aufzeichnung, Vorverarbeitung und Behandlung des Traffics durch KI gestützte Sensorik (Autarkes System)
  - Anomaliedetektion basierend auf IP-5-Tuple
  - Verwendung eines selbstoptimierenden Isolation Forests (PCB-iForest) für Streaming Data
- Integration und Testung der Strukturen in Industrie 4.0 Demonstrator
  → Ausführung von Angriffsszenarien auf Ebene der Speicherprogrammierbaren Steuerungen

Proof of Concept: Isolation Forest

- Testing the model
  - Path length provides information about normality / abnormality
  - A anomaly score is calculated for a data set, that runs through all iTrees
- Test run of normal and abnormal data set reveals the connection with the path length

normal

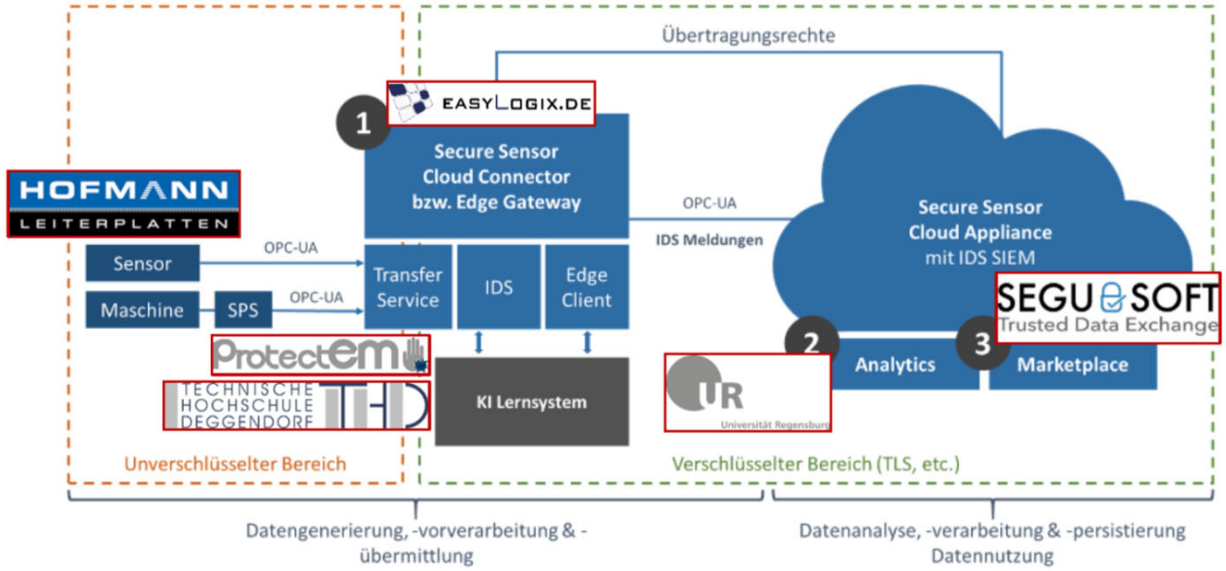




anomaly

SISSEC

Secure Industrial Semantic Sensor Cloud



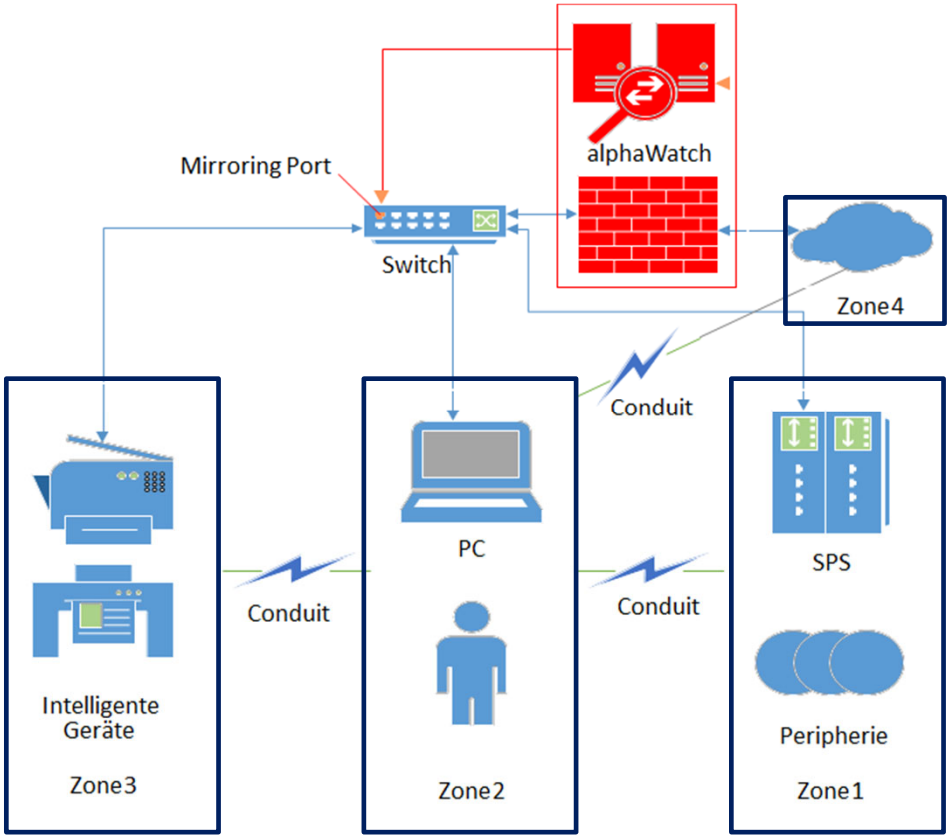
ZIM-Projekt im Rahmen der ZIM-Netzwerks des Clusters Mobility & Logistics an der TechBase Regensburg:
SeDiPeT - Secure Digital Performance Twin

- Hofmann Leiterplatten: Bereitstellung der Daten & Echtzeit-Fehlererkennung
- TG alpha (ProtectEM): Erfassung der Rohdaten, IDS im Maschinenbereich, Metadaten als Footprint, sichere Abholung und Authentifizierung der Daten
- THD: Verschlüsselung mit Hilfe leichtgewichtiger Algorithmen
- Schindler & Schill: Einbindung der Daten aus ERP-System in die Cloud, Real-Time-Korrelationen
- UR: Architektur & Systeme in der Cloud, Analytics im Sicherheitsbereich (IDS), Metamodell für Prozesssicht
- Segusoft: Ablage, Speicherung der Daten in der „Secure Sensor Cloud Appliance“, Lieferung der Datenpakete (z.B. an Maschinenhersteller) im „Marketplace“

alphaWatch Security - Feldwächter

- Überwachung der Kommunikation im Feld (Maschine, Zelle)
- Erkennung von Anomalien
  - Regelbasiert
  - KI-basiert
- Firewall zum Eingriff

alphaWatch PREDIX Edge Controller



Kontakt

Deggendorf Institute of Technology

Institute ProtectIT

Fakultät für Angewandte Informatik

Dieter-Görlitz-Platz 1, 94469 Deggendorf

andreas.grzemba@th-deg.de

Phone: +49 (0) 991 3615-512

https://www.th-deg.de/en/protectit