

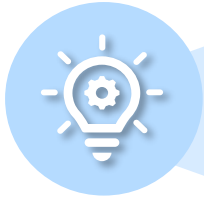
Wie Innovation die Cyber-Resilienz stärkt

Kukovic Christoph
02.10.2025



2020 wurde das VERBUND OT Cyber Security ins Leben gerufen.

Das initiale Ziel von Projekten im OT Cyber Security Lab ist es, durch Innovation die **Sicherheit im Bereich der operativen Technologie (OT)** zu stärken und über die Konzerngrenzen hinaus eine **Leuchtturmfunktion** im Bereich der Sicherung **kritischer Infrastrukturen** einzunehmen.



Das Lab ist ein Kompetenzzentrum unter der Leitung von VERBUND zur Erforschung und Weiterentwicklung neuer Technologien im Bereich der OT, oft in Kollaboration mit Herstellern, Lieferanten und weiteren Partnern



Das Lab ist ein Innovationshub, um die Versorgungssicherheit in Österreich auch in Zukunft weiter gewährleisten zu können



Das Lab ist eine Testumgebung in welcher VERBUND mit Partnern in den Feldern Energiegewinnung, Technologie, Forschung, Software, etc. zusammenarbeitet, um richtungsweisende Innovationen für die Sicherheit von OT-Systemen zu entwickeln

Vision des OT Cyber Security Labs

Unsere Vision ist es, die OT-Sicherheit bei VERBUND kontinuierlich durch **innovative Projekte** zu verbessern. Um dies zu erreichen, gibt es sowohl Kooperationen mit **Herstellern** als auch Innovationsprojekte, in denen wir mit Expert:innen aus den verschiedenen **VERBUND Gesellschaften** zusammenarbeiten.

Die Projekte des OT Cyber Security Labs gliedern sich in mehrere kleinere sowie tiefer gehende und aufwändigere Projekte.

So kann ein ausgeglichenes und flächendeckendes Verhältnis zwischen effizienten **Quick-Wins** und **nachhaltigen Großprojekten** geschaffen werden.





Durch Pentests erkennen wir **reale Risiken** präventiv und können praxisnahe **Schutzmaßnahmen** ableiten.



Reale Risiko-
Validierung statt
Annahmen



Früherkennung
vor Produktions-
ausfall



Regulatorik und
Quality Gates



Praxisrelevanz
stärkt OT
Security

Quantenkryptographie

Grundlagen

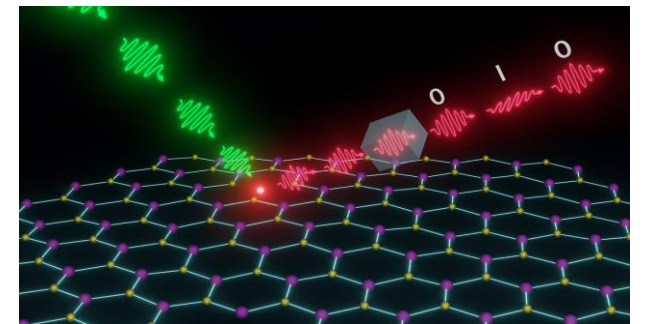
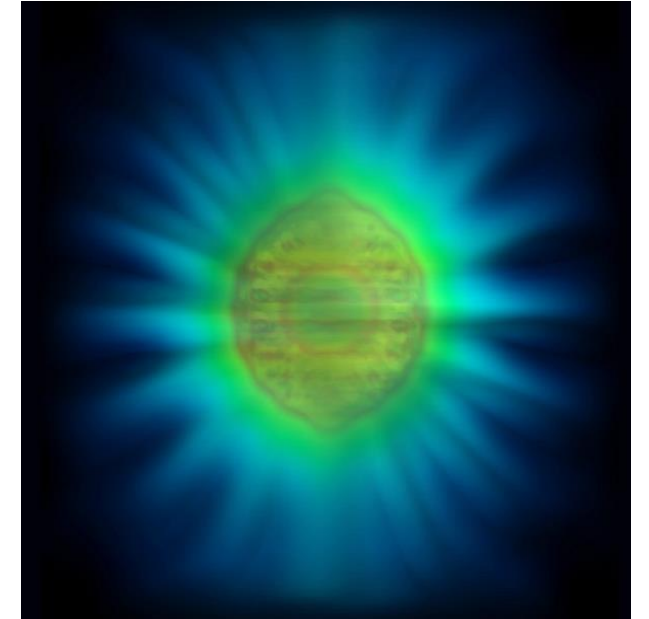
Quantenkryptographie ist ein Verfahren zur sicheren Kommunikation, das auf den Prinzipien der Quantenmechanik basiert – insbesondere dem **Verhalten von Photonen**.

Zentrale Prinzipien der Quantenkryptographie sind dabei:

- **Superposition** – Ein Quantenzustand (z. B. ein Photon) kann gleichzeitig mehrere Zustände einnehmen, bis er gemessen wird.
- **Quantenverschränkung bzw. Quantenüberlagerung** – Zwei Teilchen können so verbunden sein, dass Messungen an einem Teilchen sofort den Zustand des anderen beeinflussen, unabhängig von der Entfernung.
- **No-Cloning-Theorem** – Ein unbekannter Quantenzustand kann nicht exakt kopiert werden, was Abhörsicherheit garantiert.

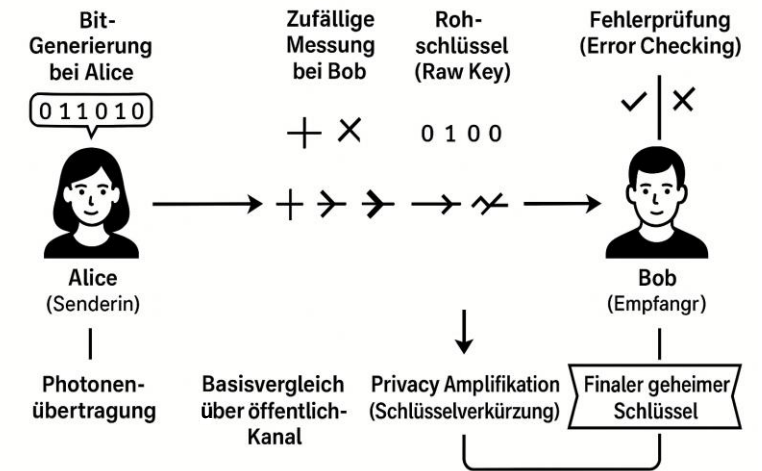
Die **Sicherheit** in der Quantenkryptographie basiert somit nicht auf Rechenleistung, sondern ist durch Naturgesetze **physikalisch garantiert**.

Das erste **Quanten-Verschlüsselungsverfahren** ist das **BB84 Protokoll** (1984).



Quanten-Schlüsselverteilung Ablauf

1. Alice erzeugt eine **zufällige** Bitfolge, **Qubits** genannt (z.B. 011010), wobei jedem Bit eine **bestimmte Polarisationsbasis** zugeordnet wird (z.B. 0 sind 45°, 1 sind 90° usw.) und sendet nacheinander die Photonen an Bob.
2. Bob misst jedes gesendete Photon mit einer **zufällig gewählten Basis** (z.B. 45°).
3. Stimmen die Polarisierung von Alice und die Basis von Bob überein entsteht ein **gültiges Bit**. Stimmen diese nicht überein erhält Bob nur ein **zufälliges Ergebnis**.
4. Alice und Bob teilen die gewählten Basen über einen **öffentlichen Kanal**. Alle Bits, welche keine übereinstimmenden Basen haben werden, **verworfen**.
5. Der **Roh-Schlüssel** besteht aus einer Aneinanderreihung von übereinstimmenden Basen.
6. Der **Roh-Schlüssel** wird im Zuge der Privacy Amplification noch **gekürzt und verdichtet**. So entsteht der **finale geheime Schlüssel** der z.B. für symmetrische Verschlüsselung verwendet werden kann.



Stichprobenartig vergleichen Alice und Bob einige Bits, um Abhörversuche zu prüfen.

Ist die **Fehlerquote** (QBER) zu hoch, wird die **Verbindung unterbrochen**, da dies auf Abhörversuche hinweist.



Quantum Pioneer

Quantenkryptographie im Fokus der Security

VERBUND hat sich als **erster Energieversorger Österreichs** zum Ziel gesetzt, den Bereich der Quantenkryptographie für die sichere Datenübertragung im eigenen Weitverkehrsnetz zu beleuchten, um die Versorgungssicherheit Österreichs auch in Zukunft zu gewährleisten.

Durch den Aufbau einer **hybriden Teststellung** mit Post-Quantum-Algorithmen (**PQC**) und Quantum Key Distribution (**QKD**) kann innerhalb des VERBUND Weitverkehrsnetz die Performance sowie Funktionalität der sicheren Datenübertragung durch die Teststrecke erforscht werden.

Hauptziel ist es erste Schritte in Richtung **Quantenkryptographische Technologien** als **sicheres Übertragungsverfahren** für sensible Daten vorzunehmen.

Digital
Power

Projektpartner

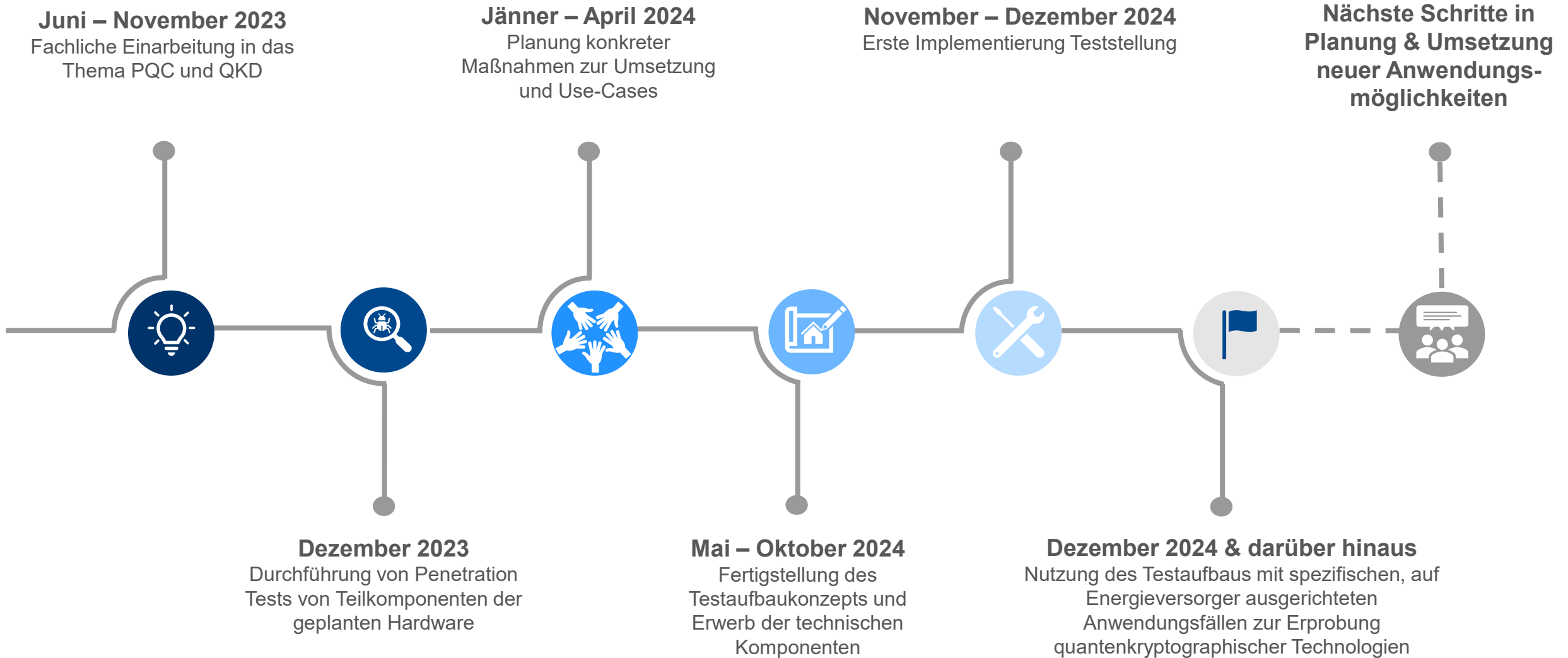


CANCOM

HITACHI



Vision des OT Cyber Security Labs

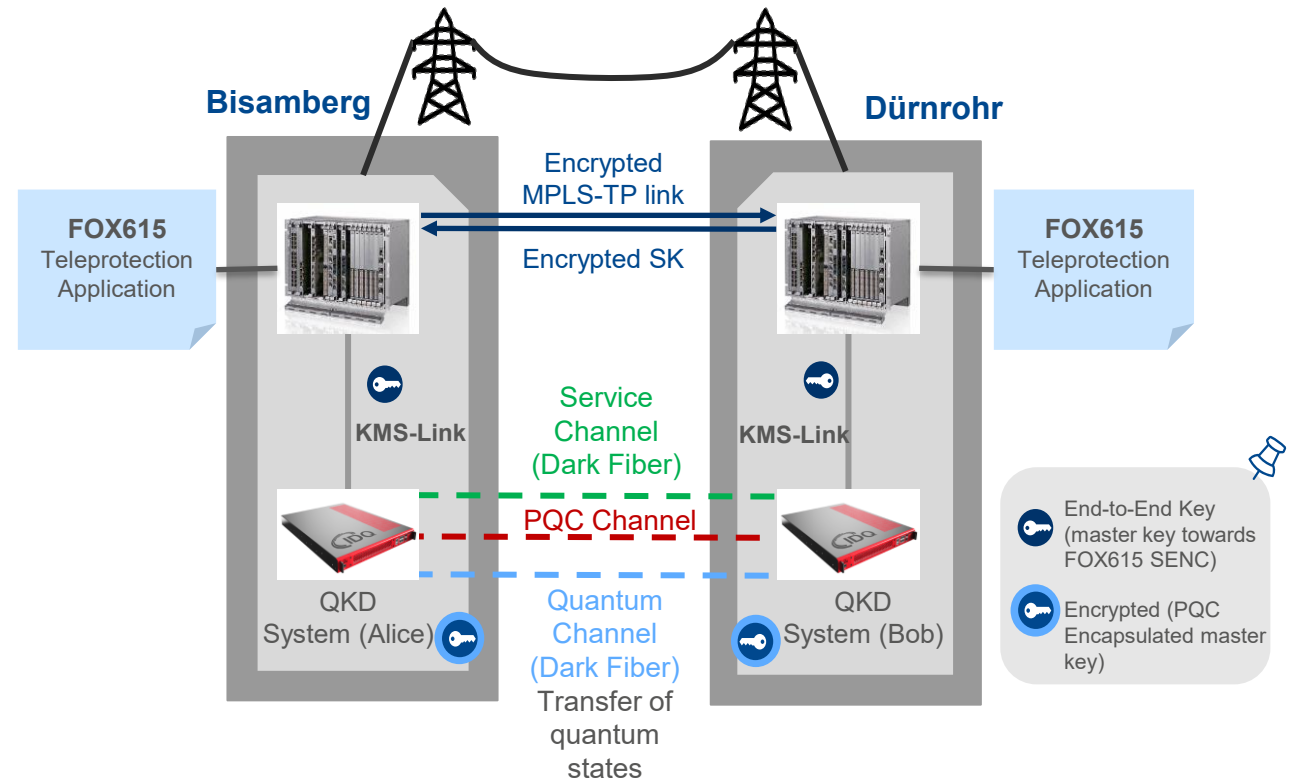


Quantenschlüsselverteilung bei VERBUND

Projekt Quantum Pioneer

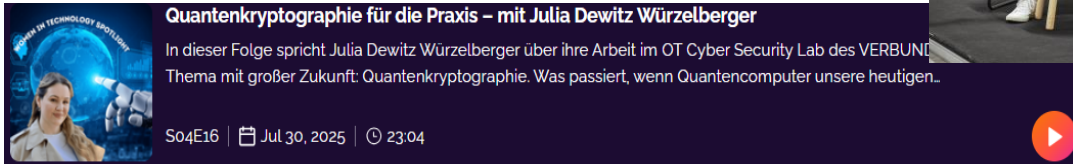
Das **Projekt Quantum Pioneer** beschäftigt sich mit dem **Aufbau einer Teststrecke** in unserem Weitverkehrsnetz mit Quantum-Key-Distribution (QKD) und Post-Quantum-Computing (PQC) Technologie.

- **Testen** quantenkryptographischer Technologie (QKD und PQC) für die **sichere Datenübertragung** im österreichischen Weitverkehrsnetz
- Gewinn **neuer Erkenntnisse** bzgl. Quantenschlüsselaustausch innerhalb eines Weitverkehrsnetzes
- Messung von **Performance** der Technologie in unserem Netz
- Zukünftige Forschung hinsichtlich **Wettereinflüsse** auf die **Funktionalität** der Quantum Key Distribution



Vorträge, Veranstaltungen, Podcasts, Mentoring

- Teilnahme an internationalen Konferenzen
- Aktive Partizipation in cross-nationalen Panels
- Mitwirkung an Mentoring- und Stipendiums-Initiativen, um mehr Frauen für technische Berufslaufbahnen zu begeistern
- Konzeption und Durchführung von OT-Security-Schulungen zur Steigerung von Awareness und Fachwissen an verschiedenen VERBUND-Standorten



VERBUND X Ventures

seeks to invest in early-stage startups
all over Europe that accelerate the energy transition



Investment stage & ticket size

- Late Seed and Series A
- Ticket size: Up to €2.5mn for initial investments
- Role: (Co-)Lead Investor, Co-Investor



Focus areas

- Sustainable energy production
- Flexibility & energy transport
- Green mobility



Geographical focus

- Based in Europe

Our ambition

15

Investments

2024-
2026

Between 2024-2026

30mn

With a fund volume
of €30mn

Since the launch in 2022, VERBUND X Ventures has invested in ten outstanding startups and one venture capital fund in the energy sector



Romania



Sweden



Austria



HYBRID ENERGY STORAGE SOLUTIONS

Spain

EOLOGIX-PING

Austria/Australia

e⁺friends

Austria



Slovenia



Germany



Austria



Austria

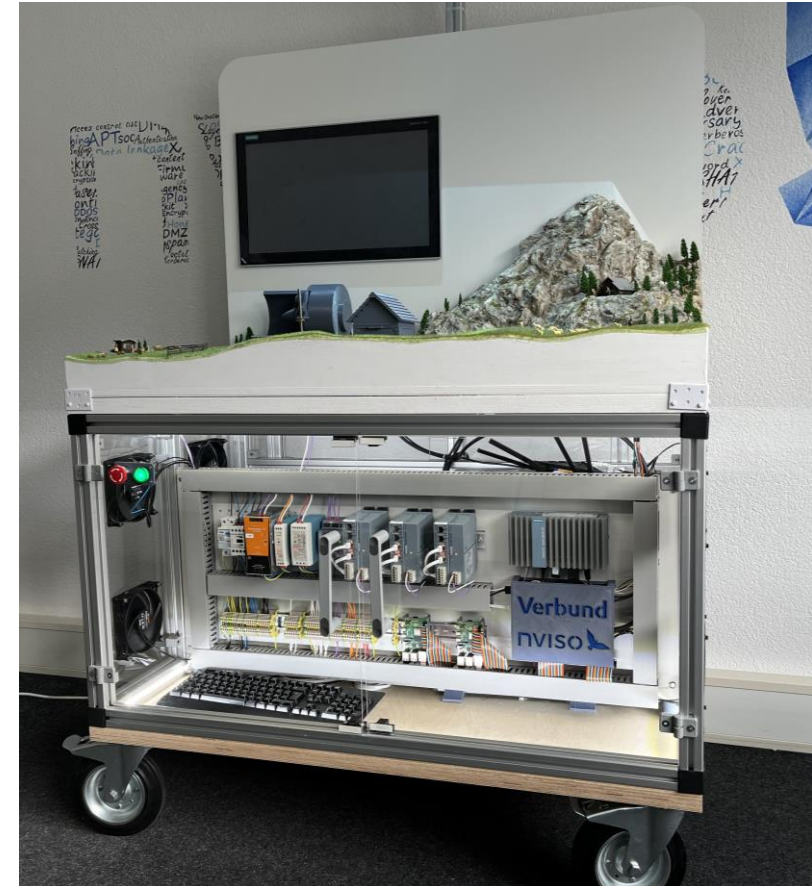


Germany

OT-Security braucht reales Training

ICS Firing Range Prototype

- **Simulation** eines **Angriffsszenario** auf ein **Laufkraftwerk**
- Soll die Dynamik und die Auswirkungen eines **Cyber Incidents** greifbar machen
- Es kann ein **programmiertes Angriffsszenario** abgespielt werden, bei welchem von einem Hacker **manipulierte Werte** zu einer **Überflutung** des Landschaftsmodells führen
- Über den **Touchscreen** können Anweisungen an die Steuerung gegeben werden
- Je nach gewähltem **Zufluss** schließen oder öffnen sich die simulierten **Wehre**. Ist der Pegelstand zu hoch, öffnet der **Notablass** um das **Wasser** schnell **abzuführen**
- Funktion als **interaktive Trainingskomponente**



In unserer OT Cyber Security Range bereiten wir uns mit Cyber-Krisenübungen in einer gesicherten und realitätsnahen Umgebung auf den Ernstfall vor



Unser Trainingskonzept

Unser innovatives Trainingskonzept bietet eine breite Palette von Cyber Security-Maßnahmen.

Diese einzigartige Mischung aus bewährten und fortschrittlichen Lehrmethoden macht nicht nur Wissen zugänglich, sondern fördert auch praktische Fähigkeiten.

Unser Trainingskonzept ist nicht nur eine Aufgabe, sondern eine Reise voller Erkenntnisse!



Schulungen



Vorträge



Analyse von
Fallbeispielen



Praxisnahe
Übungen



Simulationen von
"live" Angriffen



Wissens- &
Erfahrungsaustausch



Lessons
learned



und vieles mehr
...

Vielen Dank für Ihre Aufmerksamkeit!

V