it-sa Expo&Congress, October 10-12, 2023

MODERN TRAINING FOR OPERATING CYBER-RESILIENT CRITICAL INFRASTRUCTURES

Helmut Leopold
Head of Center for Digital Safety & Security
AIT Austrian Institute of Technology

Nürnberg, October 11th, 2023

(v1.0)

The availability & resilience of our digital and globally interconnected infrastructures are no longer guaranteed

Social media

eHealth

Industry 4.0

Smart City

Connected Cars

Digital Transport

Smart grid

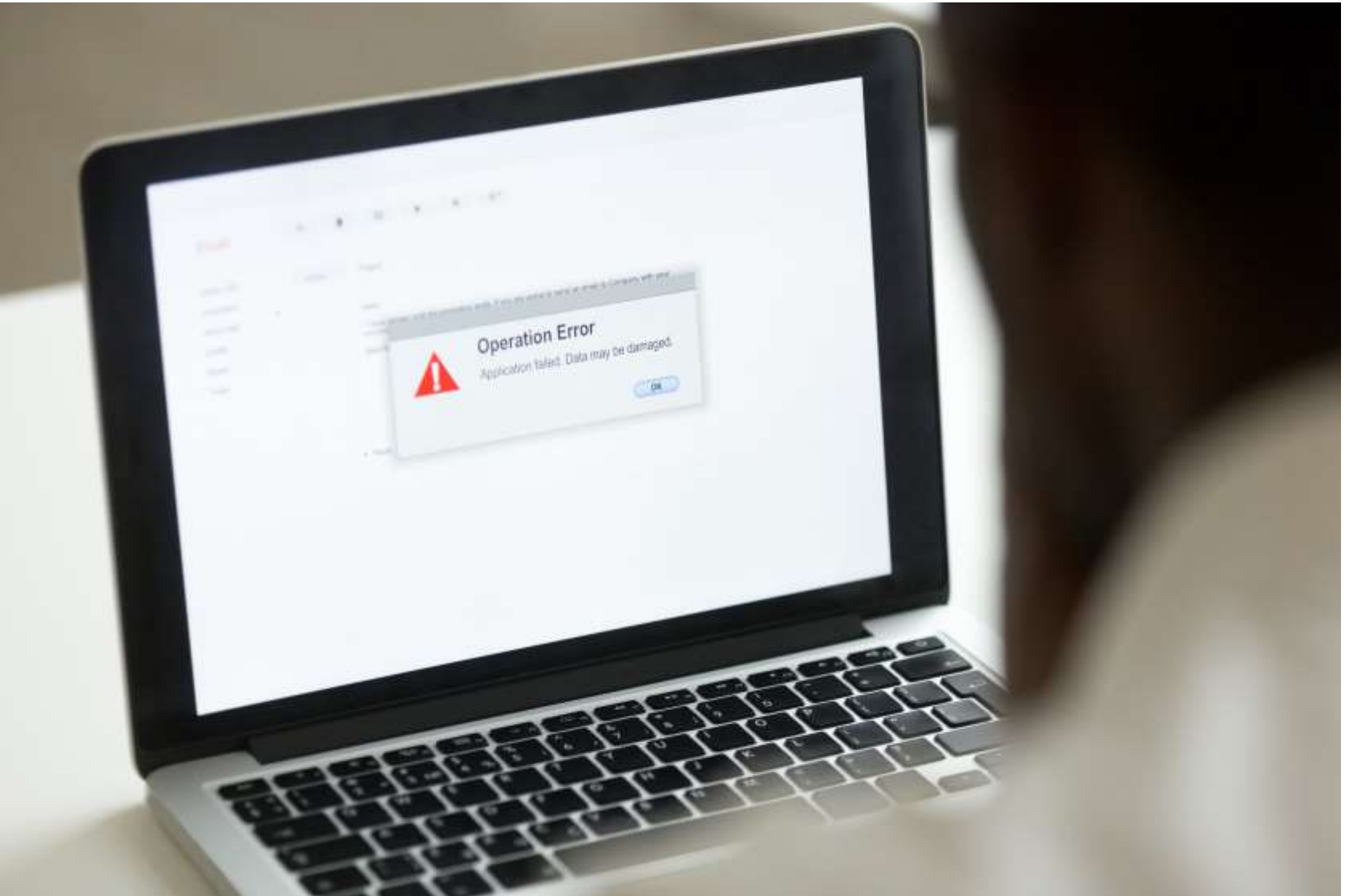
New attack scenarios
Crime as a Service

Increased complexity
System of Systems (IIoT)

Safety & Security
IT/OT

(Many) new regulations

THREAT 1: EACH SOFTWARE HAS FLAWS - "ZERO DAY VULNERABILITIES"



- **200k+ known vulnerabilities**
- **70 new vulnerabilities per day**

7 days to exploit vulnerabilities

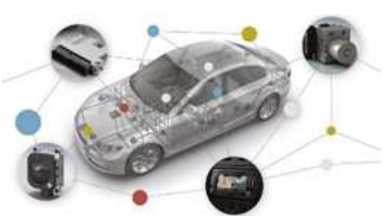
176 days to close vulnerabilities – up to never…

Side Channels - secure implementation?

heartbleed

THREAT 2: "CYBER SECURITY IS NO LONGER MANUALLY CONTROLLABLE – SYSTEM OF SYSTEMS"

- Comprehensive digitalization & networking
- Cloud Shift
- Service Shift – from products to services
- IT & OT integration
- Users of digital systems have to deal with “complex systems”



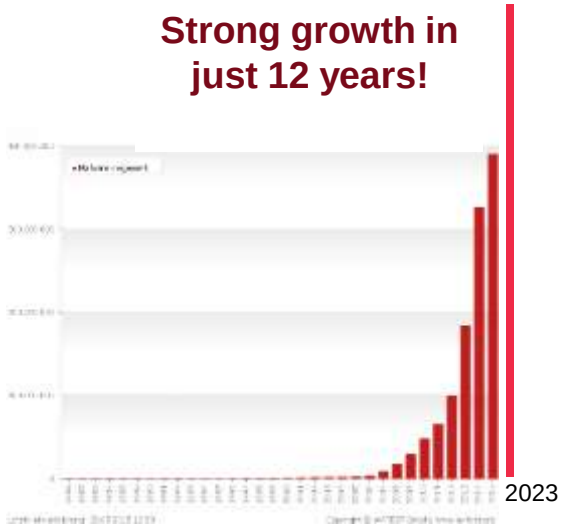
- 100 Mio Lines of Code
- 150 control systems
- 4 bus systems
- Interaction with internet & apps

THREAT 3: “INDUSTRIALISATION OF ATTACK METHODS"

THE ATTACKER KNOWS YOUR VULNERABILITY BEFORE YOU KNOW IT

1 billion malware types
100-200k new types per day

Strong growth in just 12 years!

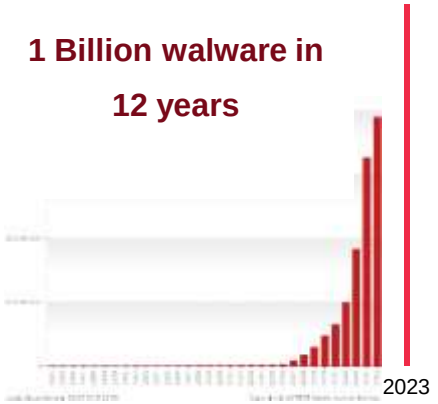


Source: https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Sicherheitsreport_2018-2019.pdf

THE NEW CYBER SECURITY LANDSCAPE

Increasing threat complexity

- Every SW System has vulnerabilities
- Attack industry – democratisation of attack tools & technologies
- The threat scenario is constantly changing



Sustainable Cyber resilient systems need …

- new tools for system development: safety & security by design
- a permanent revision of the protection concepts - continuous updating of the threat model for vulnerabilities and threats – permanent certification of systems
- Identification of the unknown unknown attack – AI based protection systems
- Capabilities for infrastructure operation and security management
- Incident information exchange & management between organization as well as with public administration

New regulations & laws

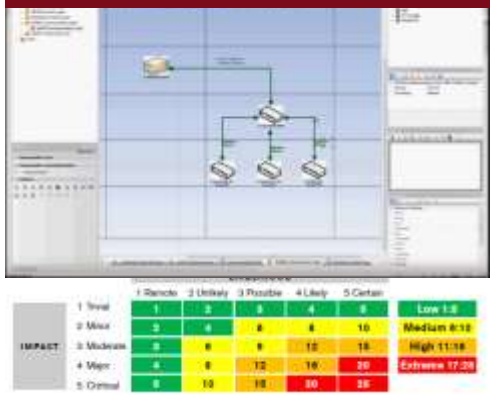
- EU NIS-2 Regulation
- EU Cyber Resilience Act
- EU Data Act
- EU Data Governance Act
- DORA for finance
- WP29 - UNECE 155 Regulation for automotive cyber security
- …

RECOMMENDATIONS

1. Positioning cybersecurity as a strategic issue → CEO priority
2. Increase awareness of threats in the enterprise & establish a tool supported risk management
3. Implement basic protection concepts: business processes, IT architecture, firewalls, virus protection, smart back-up systems (!), penetration tests, access protection, etc. → *"IT security hygiene"*
4. Apply security standards & certifications → product development & business processes
5. **Implement modern cyber security protection mechanisms**

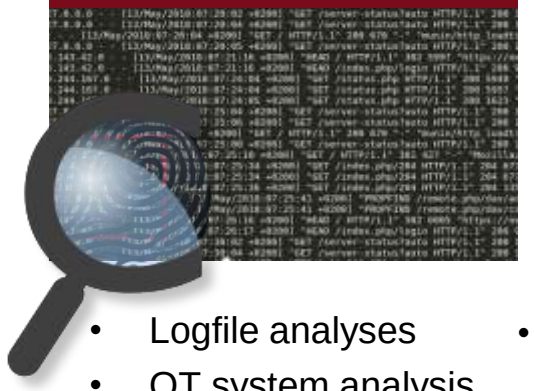
THREATGET
www.threatget.com

Security by Design



AECID
www.aecid.ait.ac.at

Artificial Intelligence attack/anomaly detection online monitoring



- Logfile analyses
- OT system analysis
- Run-time verification

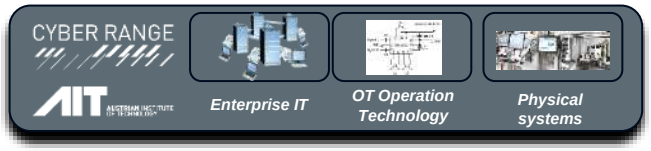
fragmentiX QUANTUM SAFE STORAGE SOLUTIONS
CATCH DIRECT
www.fragmentix.com
www.catch.direct

Smart Encryption

CYBER RANGE
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
www.cyberrange.at

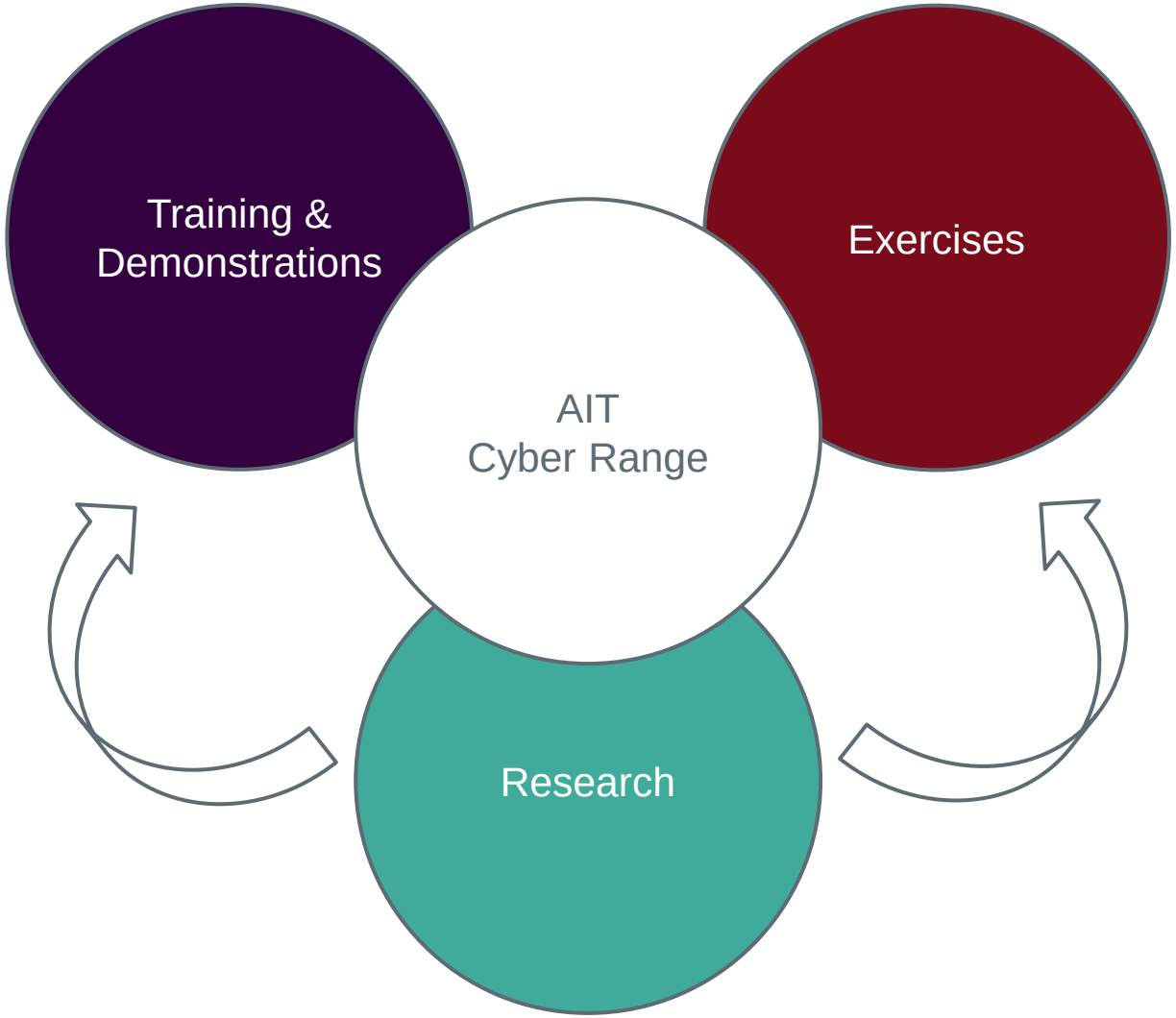
Education, training, qualification, practice

- Highly secure cloud storage systems - Post Quantum safe
- Secure distributed market places



LieberLieber
AVL
msg PLAUT

AIT CYBER RANGE PROGRAMME PORTFOLIO



AIT CYBER RANGE - DIGITAL TWIN FOR IT/OT CYBER SECURITY MANAGEMENT

» **Learners** »

Education and training, and certification (skills) for various expert levels

« **Exercises** »

ICT, Processes, Structures, Policies

Training of usage of dedicated tools: detection, analysis and countermeasures of cyber attacks

Testbed for Cyber Physical Systems

Training & certification: Skill, capability development for specific tasks; coping with scenarios – IT experts, crisis teams & management

Testing of protection concepts and processes
- contingency plans & processes
- communication channels

AIT CYBER RANGE - DIGITAL TWIN FOR IT/OT CYBER SECURITY MANAGEMENT

AUSTRIAN INSTITUTE OF TECHNOLOGY

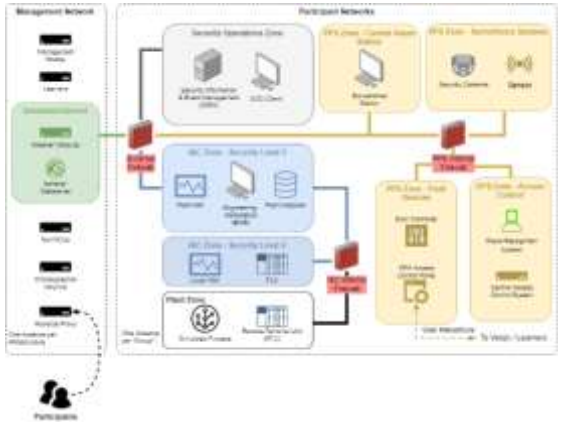
» **Learners** «

Web-based learning management system with Cyber Range access

- Training provides theoretical background & hands on experiences with virtualized and real equipment (ICS and PPS equipment) to support learning outcomes
- Simultaneous delivery of training in multiple languages
- Self-paced exercise control
- Virtual Desktop for hands-on experiences
- Templating of exercise workbooks - easy customization.
- Clicker-style quizzes for presentations
- Instructors can monitor progress in real-time
- All content delivered through a web browser

« Multi-Stake-holder Exercises »

ICT, processes, structures, policies & guidelines



Recognising Cyber Security Attacks	Managing Computer Security Risks	Perform Risk-management	Identify IoC for critical Infrastructure Operators	Development of a resilient Computer Architecture	Incident management according to regulations and laws

Red/Blue/White Team scenarios

CYBER RANGE

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Enterprise IT

OT Operation Technology

5G

5G network infrastructure

Physical systems

Training & Capacity Building
Technology, Processes & People
for designers, operators, policy makers & users

CYBER SECURITY CAPACITY BUILDING

AUSTRIAN INSTITUTE OF TECHNOLOGY

Recognising the Significance of Sensitive Information

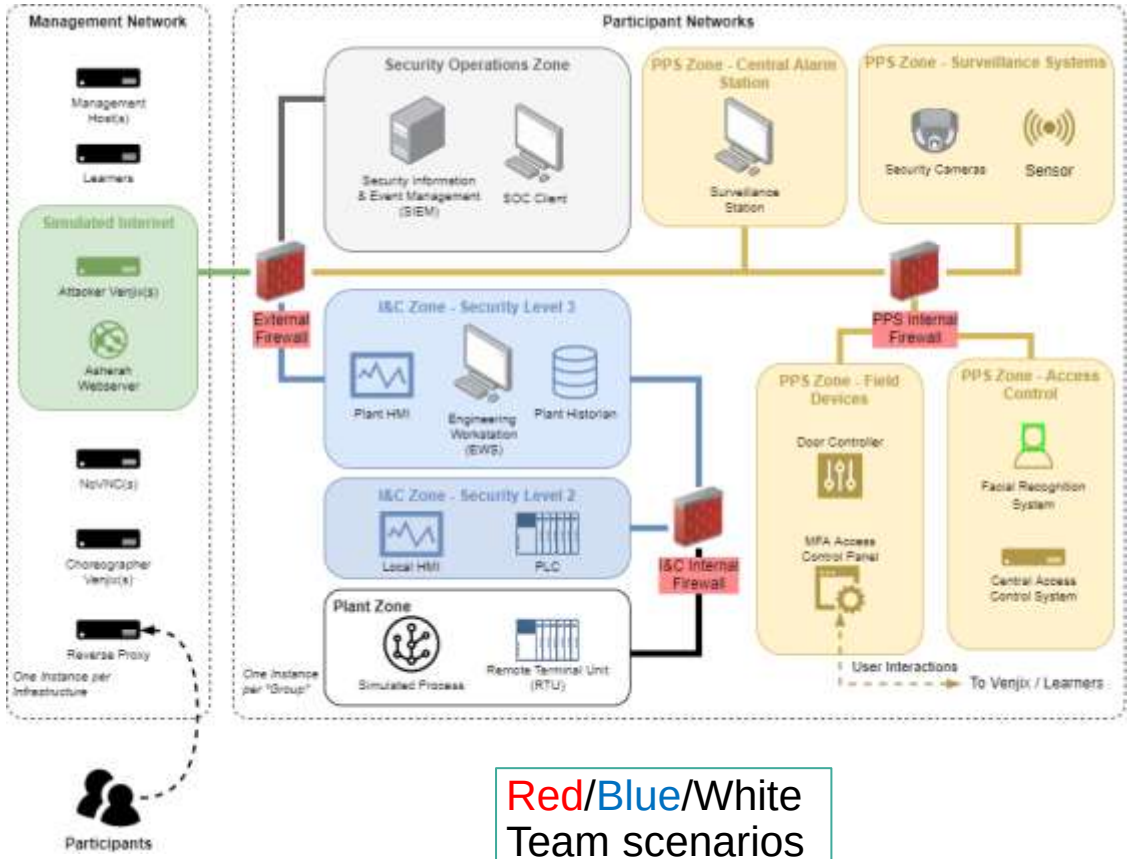
Appreciating the Nature of I&C Systems for Nuclear Facilities and those Associated with Radioactive Material

Recognizing the Impact of Cyber-attacks on I&C Systems and their Ability to Perform their Function

Exploring the Benefits and Importance of Applying a Risk-informed Graded Approach to Computer Security

Managing Computer Security Risk with Technical Vulnerability Management

Understanding the Need to Apply Defence in Depth as part of a Defensive Computer Security Architecture



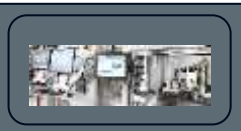
Red/Blue/White Team scenarios

CYBER RANGE

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Enterprise IT

OT Operation Technology



Physical systems

Training & Capacity Building - technology, processes & people - for designers, operators, policy makers & users

AIT CYBER SECURITY TRAININGS FOR IMPROVING THE CYBER SECURITY GLOBALLY

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

IAEA
AIT Austrian Institute of Technology GmbH
IAEA Collaborating Centre
for
Information and Computer Security for Nuclear Security

AIT supports and delivers the hands-on training courses for the IAEA globally

IAEA

WINS WORLD INSTITUTE FOR NUCLEAR SECURITY

COLTRANE
COLLABORATIVE CYBERSECURITY AWARENESS LEARNING

Erasmus+

KSÖ Kompetenzzentrum Sicheres Österreich
CERT.at
Federal Chancellery Republic of Austria
Federal Ministry Interior
Federal Ministry Republic of Austria Defence

https://kompetenzzentrum-sicheres-oesterreich.at/wp-content/uploads/2021/09/KSOe-PLANSPIEL-2021-v2.mp4.mp4

Digital Factory Vorarlberg
Verbund
AT&S
WIEN IT
EVN
SALZBURG AG




CYBER RANGE
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY


Enterprise IT


OT Operation Technology


Physical systems

Training & Capacity Building
Technology, Processes & People
for developer, operator, policy maker, user

https://cyberrange.at

We have to rethink our approach how o build and operate digital systems –

for system designers, developers and operators –

otherwise are the availability & resilience of our digital and globally interconnected infrastructures no longer guaranteed!

Capacity building will be key for an EU digital and data sovereignty

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

Thank You!

Helmut LEOPOLD

Head of Center for Digital Safety & Security

AIT Austrian Institute of Technology

LITERATURE – FURTHER INFORMATION

http://www.czernin-verlag.com/buch/30-ideen-fur-europa

https://link.springer.com/book/10.1007/978-3-662-44306-4

https://vogel-fachbuch.de/maschinenbau/automatisierung/672-cybersicherhe

https://plattformindustrie40.at/wp-content/uploads/2020/05/WEB_Industrie4.0_Ergebnispapier_CyberSecurity_2019.pdf

https://thertoinnovationsummit.eu/sites/default/files/inline-files/Cybersecurity_Discussion_Paper_Final_Layout_20201023%20%281%29_0.pdf