

visIT

Industrial Cybersecurity

Technologies for the cybersecurity of
industrial automation and control systems

Imprint

visIT is published about three times a year and informs about selected research topics of Fraunhofer IOSB. To order single issues, for a free visIT subscription, and for address changes and cancellations, please send an e-mail to publikationen@iosb.fraunhofer.de

Publisher

Prof. Dr.-Ing. habil.
Jürgen Beyerer

Editor

Dipl.-Phys. Ulrich Pontes
Lena Kaul, M.A.

Layout

Anja Wollfarth, M.A.

Printing

Ganz GmbH
Ooser Bahnhofstraße 36
76532 Baden-Baden

Editorial Address

Fraunhofer Institute of
Optronics, System Technologies
and Image Exploitation IOSB
Fraunhoferstr. 1, 76131 Karlsruhe
Phone +49 721 6091-300
Fax +49 721 6091-413
presse@iosb.fraunhofer.de

© Fraunhofer IOSB
Karlsruhe 2025

Institute of the
Fraunhofer-Gesellschaft,
Munich

26th Year
ISSN 1616-8240

Image sources

Cover picture: indigo, stock.
adobe / Icons-Studio
Page 6: stock.adobe / Andrii

All other images
© Fraunhofer IOSB,
Exceptions are marked.

Themen

Editorial	3
Jürgen Beyerer, Christian Haas	
ISuTest®: Automated vulnerability detection in accordance with the Cyber Resilience Act and IEC 62443	4
Steffen Pfrang	
Assistance systems to improve OT security in energy supply	6
Dennis Rösch, Nicolai Steffen	
Cybersecurity Training Lab: Research and continuing education programs for cybersecurity in the context of production and critical infrastructures	8
Christian Haas	
“Engineering Security for Production Systems”: The Industrial Cybersecurity Lab within the KASTEL Security Research Labs	10
Pascal Birnstill	
Cyber resilience monitoring in industrial automation and control systems	12
Christian Haas	
Classification of cyberattacks on industrial control systems in encrypted network traffic	14
Felix Specht, Jens Otto	

Editorial

Dear friends of Fraunhofer IOSB,

Industrial automation and control systems (IACS) are crucial for the effective functioning of various industries such as energy, transportation, healthcare and manufacturing. IACS consist of complex networks of machines, devices and software applications that control, monitor and automate critical processes. Compromises or data breaches in these systems can result in significant economic losses, risks to public safety and security, and potential threats to national security. Protecting critical infrastructure, manufacturing processes and sensitive data is therefore a top priority for companies worldwide. Industrial cybersecurity is therefore a research topic that requires extensive attention.

Cybersecurity for industrial automation and control systems must take into account industry-specific requirements such as real-time communication, system longevity and functional safety. In these respects, it differs significantly from cybersecurity in office environments or when operating internet servers in data centers. In an industrial context, traditional cybersecurity measures such as software updates, antivirus programs or firewalls cannot therefore be used without restriction. For this reason, new strategies and methods must be developed to protect industrial automation and control systems.

Fraunhofer IOSB plays a leading role in research on IACS. One of the central topics is the Cybersecurity Training Lab with the consortia "Industrial Production" and "Security for the Energy and Water Industry". Practical scenarios and laboratories are created here to test innovative approaches and offer practical training courses. As part of the Competence Center for Applied Security Technology (KASTEL), Fraunhofer IOSB, in collaboration with the Karlsruhe Institute of Technology, focuses on the research and development of security solutions for industrial systems with the aim of strengthening the security and resilience of IACS against cyber threats. In addition, the self-financed project CyReM-ICS (cyber resilience monitoring in industrial automation and control systems) focuses on the development of methods and tools for the presentation and improvement of cyber resilience in industrial control systems. It is pursuing a holistic approach that includes preventive and reactive measures.

Through these initiatives, Fraunhofer IOSB makes a decisive contribution to the further development of security standards and innovative solutions in industry and research.

Fraunhofer IOSB, March 2025



Prof. Dr.-Ing. habil. Jürgen Beyerer



Dr. Ing. Christian Haas



Prof. Dr.-Ing. habil. Jürgen Beyerer



Dr.-Ing. Christian Haas

ISuTest®

Automated vulnerability detection in accordance with the Cyber Resilience Act and IEC 62443

Industrial components are often used behind the scenes: modern traffic light control systems at junctions, trains, power stations and hospitals cannot function without them. They also control and monitor entire factory halls, read sensor data and process it, sometimes with real-time requirements.

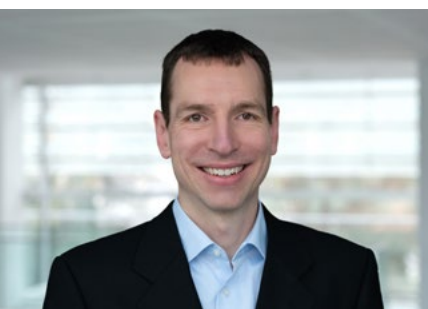
But what do all industrial components have in common? A network connection, a “digital element” according to the Cyber Resilience Act (CRA) of the European Union (EU). Through this connection, they are accessible via the network – and therefore in principle also vulnerable to attack. What happens in the event of an attack? Sometimes railway display boards fail, sometimes hospitals shut down, or a workpiece in production does not meet the required quality.

Against this background, the EU has issued the CRA, which obliges manufacturers of com-

ponents with digital elements to develop and test them safely. Otherwise, they may no longer be placed on the market within the EU from December 2027. The IEC 62443 standard for the protection of industrial communication networks describes such a secure development life cycle for manufacturers of industrial components. Automated vulnerability scanning via the network interface is an essential part of this. This means that all protocols that could impair the robustness of the components must be extensively tested for vulnerabilities.

Testing like an attacker

The Industrial Security Testing Framework ISuTest® is a tool for finding vulnerabilities in the implementations of automation components. It has been developed at Fraunhofer IOSB in Karlsruhe in the Industrial Cybersecurity group since 2016. ISuTest® is designed as an open,



Dipl.-Inform.
Steffen Pfrang

Information Management
and Production Control (ILT)

Phone +49 721 6091 357
steffen.pfrang
@iosb.fraunhofer.de

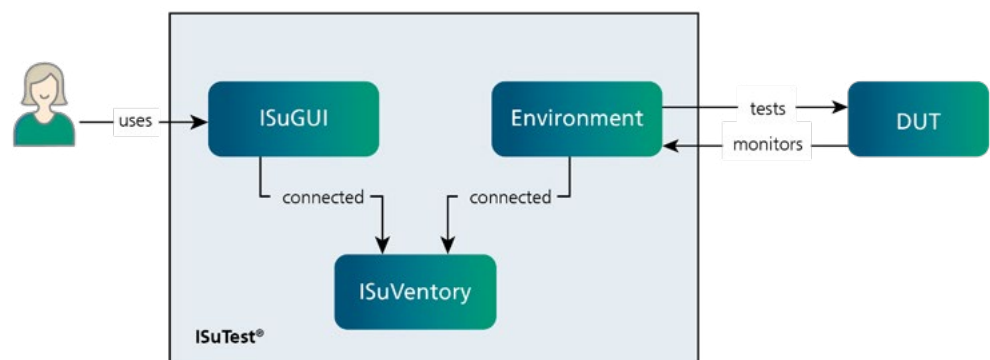


Fig. 1: The flexible, distributed architecture of ISuTest®.



Fig. 2: Test setup of ISuTest® in the Fraunhofer IOSB laboratory in Karlsruhe.

extensible framework. It supports manufacturers in setting up and performing a test as well as in isolating vulnerabilities in order to reproduce the error with the developer. An exemplary test setup of ISuTest® as used in the Fraunhofer IOSB laboratory is shown in Figure 2.

The vulnerability test by ISuTest® is carried out using fuzzing techniques. Network packets are slightly modified and sent to the component in the same way as an attacker would. ISuTest® does not require any insight into the internal workings of the device; the specification of the communication protocols is sufficient. This means that any device with a network interface can be tested; it is a so-called black box test. In addition, further protocols can easily be added to ISuTest® to fulfil the IEC 62443 requirement for testing all offered protocols.

The architecture of ISuTest® is shown in Fig. 1. It is a distributed client-server infrastructure. The actual test is carried out by the Environment. Using the ISuGUI graphical user interface, the user configures components to be tested, starts tests and conveniently evaluates completed tests. The ISuVentory is the central database, file repository and communicator. At the smallest configuration level, all components are installed on a local PC. At the largest expansion stage, many users work with ISuGUIs via VPN with an ISuVentory in a Kubernetes cluster and several Environments.

Monitoring like in the functional tests

ISuTest® uses monitoring to recognize whether a component is still working as intended during and after a test. Classic IT monitoring is used, for example, to test whether the device

can still be pinged or whether the web server is still delivering data. ISuTest® can also monitor any process parameters. In the simplest case, these are the digital output values of an actuator. The process of a switch, however, is its switching functionality, which is evaluated. Basically, the same procedures can be used here that are already used in the functional tests.

Just as ISuTest® can control other test tools and enrich them with process monitoring, for example, it can also be controlled remotely itself. The REST API specified in OpenAPI allowstests to be started at selected times and the test results to be returned in machine-readable form. This means that security tests can be triggered by existing CI/CD systems and tickets can be created in return if ISuTest® has discovered a potential vulnerability.

Successful in daily use

ISuTest® is aimed at manufacturers and integrators of industrial components. ISuTest® can be used both in test centres and during development. ISuTest® has been in commercial use for several years and has already identified hundreds of vulnerabilities. These successes show that with ISuTest® the vision of "Security by Design" does not have to remain a vision.

¹ Further information on ISuTest® can be found on the product page: www.isutest.com

Assistance systems to improve OT security in energy supply



Dennis Rösch, M.Sc.

Cognitive Energy Systems
(KES)

Phone +49 3677 461 188
dennis.roesch
@iosb-ast.fraunhofer.de



Dipl.-Ing. Steffen
Nicolai

Cognitive Energy Systems
(KES)

Phone +49 3677 461 112
steffen.nicolai
@iosb-ast.fraunhofer.de

New requirements for plant and system operators

Decarbonization, decentralization, and digitalization are key drivers of the transformation of the energy system towards a secure and sustainable energy supply. These trends not only present significant opportunities, but also pose challenges, particularly for power plant and system operators. Energy supply plays a crucial role in society and the economy, making the assurance of supply paramount.

In addition to traditional operational tasks, operators must also consider security and resilience aspects. The decentralized and digitalized structures necessitate continuous monitoring and active management. Consequently, there is a need to establish new organizational structures that address the specific challenges of operational technology (OT) communication infrastructures.

Comprehensive OT security management required

Industrial processes are directly dependent on the operational communication infrastructure. Supply security heavily relies on the availability, confidentiality, and integrity of communication devices. Unlike office IT, OT infrastructures are often less accessible, cannot be easily shut down for maintenance or updates, and are designed for significantly longer life cycles.

Effective security management for OT environments is essential. This includes network monitoring, continuous asset and vulnerability management, and a deep understanding of specific challenges. Operators must develop and provide the necessary expertise and technologies to meet the rising demands.



Fig. 1: Assistance systems support plant and network operators in holistic management and help to increase OT security.



Fig. 2: Hands-on training in the Cybersecurity Training Lab: Mobile training platforms at Fraunhofer IOSB-AST.

Urgent need for expertise and assistance

To address changing challenges, a new profile for personnel in control centers and secondary technology at power plants and system operators is emerging. There is a high demand for expertise in network technology, security, and monitoring of communication infrastructures to ensure the supply security of decentralized power grids. A fundamental realignment of education and specific further training is crucial.

Operators are increasingly faced with a flood of information that must be reviewed, interpreted, and assessed. The operational tasks of managing the electrical power grid need to be expanded to include monitoring the communication infrastructure. Assistance systems are crucial in this context, as they support with interpretation and decision-making while providing well-prepared information.

Current work at Fraunhofer IOSB-AST

Fraunhofer IOSB-AST is involved in various public and industrial research projects aimed at developing assistance systems to support power plant and system operators, particularly in the field of distribution systems. Different aspects are addressed,

including the simulation of coupled structures, digital twins for monitoring and evaluating operation scenarios, virtualization approaches for secondary equipment, and methods for monitoring power and communication networks.

Services offered by Fraunhofer IOSB-AST

Through the Cybersecurity Training Lab for energy and water supply, training is offered in network security, network monitoring, and secure configuration (hardening) according to current security standards. Insights from research and development projects provide valuable inputs for practical training. The hands-on training setup is shown in Figure 2. Additionally, Fraunhofer IOSB-AST supports clients through targeted service projects addressing specific OT security issues.

Cybersecurity Training Lab

Research and continuing education programs for cybersecurity in the context of production and critical infrastructures

In today's digitalized world, both industrial production and energy and water supply systems are facing a multitude of threats due to increasing automation and networking. Attacks on IT and OT systems (OT = operational technology), networks, and OT components can have significant impacts on supply security, production processes, and societal stability. In order to counter these threats effectively, companies must be familiar with and implement the regulatory requirements of the Cyber Resilience Act, the NIS 2 Directive and the Machinery Ordinance. The learning lab addresses these requirements by combining training, research and development in an interdisciplinary environment and making it accessible. Through practical training in state-of-the-art laboratory environments, companies are enabled to implement the latest security standards and technologies and thus strengthen their resilience against cyber threats.

The further education initiative Cybersecurity Training Lab consists of Fraunhofer institutes, universities of applied sciences and the Fraunhofer Academy. They develop high-quality continuing education programs in IT security to transfer the latest research knowledge in a hands-on way to industry and society. The various learning laboratories make it possible to impart knowledge not only in terms of content but also in a suitable environment – both in person and online. Fraunhofer IOSB offers state-of-the-art laboratory environments and training demonstrators for conducting the training courses, so that the knowledge learned can be applied in practice in an environment that is as close to reality as possible.

Focus “industrial production”

An increasing number of manufacturing companies are adopting Industry 4.0 approaches in their production processes. While the comprehensive networking of components, systems, and entire production facilities offers numerous opportunities, it also presents risks that must be addressed to protect sensitive data and prevent potential production disruptions caused by cyber-attacks. As part of the digital transformation, companies must understand their critical systems, facilities, and assets to implement appropriate protective measures. This includes recognizing and identifying typical vulnerabilities in the design and implementation of embedded systems and industrial components. Moreover, the latest developments in communication protocols, security features, and secure software development must be integrated into production facilities to ensure effective protection. The “Industrial Production” consortium of the Fraunhofer Cybersecurity Learning Lab has specialized in these topics and supports manufacturing companies with training and service offerings.

Focus “energy and water supply”

The ongoing digitalization of all areas of society poses significant challenges to ensuring secure and stable system operations in energy supply and water management. The increasing integration of decentralized facilities for data collection and transmission, along with inter-connected systems for energy generation, distribution, storage, and consumption, underscores the critical importance of IT and OT security in ensuring reliable service delivery.



Dr.-Ing. Christian Haas

Information Management
and Production Control (ILT)

Phone +49 721 6091 605
christian.haas
@iosb.fraunhofer.de

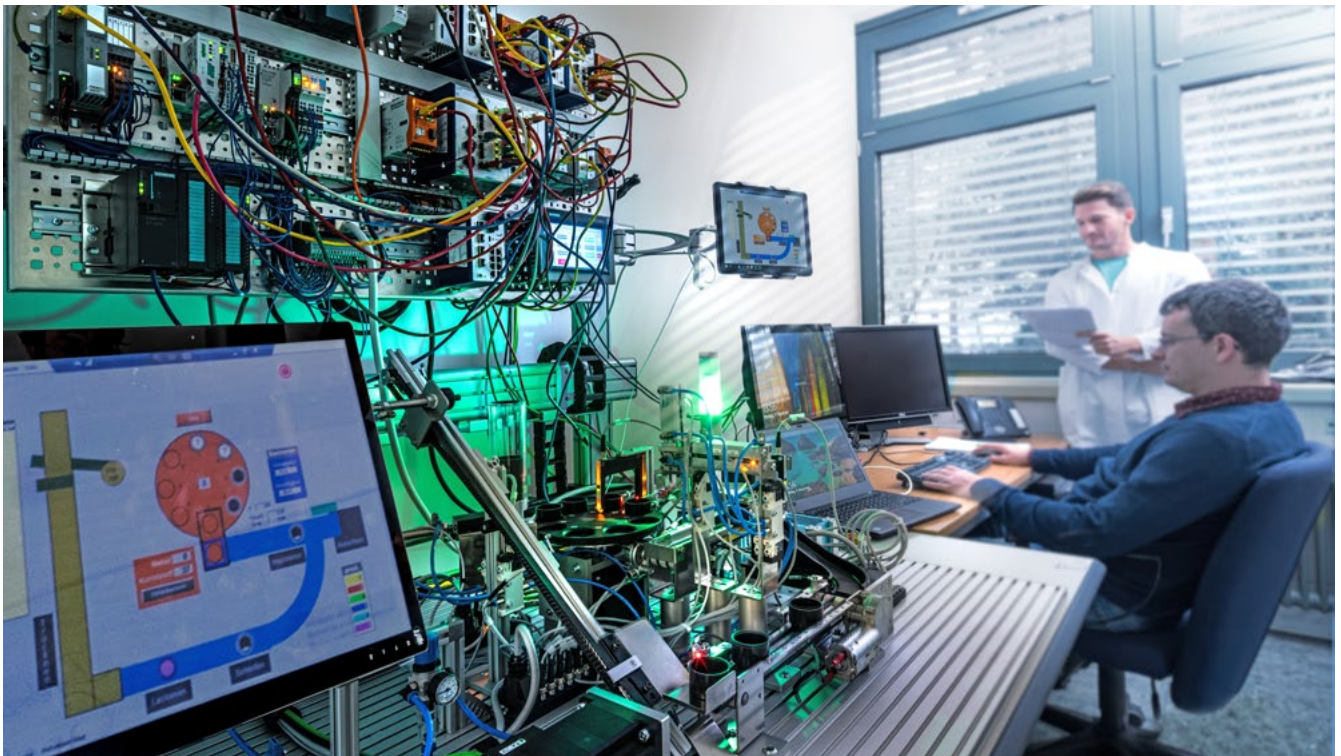


Fig. 1: A view into our Cybersecurity Training Lab at Fraunhofer IOSB.

Key aspects of the four locations

The Cybersecurity Training Lab at Fraunhofer IOSB-AST in **Ilmenau**, for example, offers you an ideal test environment for simulating real-world scenarios and investigating the effects of attacks on the IT infrastructure of utility network operators.

The Cybersecurity Training Lab at our **Görlitz** site focuses on the topic of IT security in energy and water supply and complements the lab in Ilmenau, which focuses on security in the area of operational technologies and in the process area. In the lab in Görlitz, a virtual utility company (energy and water) with its network infrastructure is mapped, which forms the basis for practical training. Topics of the training are:

- Cybersecurity
- Monitoring
- Attack detection
- Remote maintenance/access
- Attack vectors and corresponding protective measures

The Fraunhofer IOSB IT security laboratory in **Karlsruhe** has numerous demonstrators and learning environments for testing and applying industrial cyber security technologies. The Fraunhofer IOSB in Karlsruhe is a cooperation partner of ISA Europe and, with its certified trainers, offers training courses on topics

related to IEC 62443, among other things. Other areas of focus include security testing of automation components, secure OPC UA, and attack and anomaly detection in industrial networks and plants.

The Cybersecurity Training Lab of Fraunhofer IOSB-INA in **Lemgo** is equipped with high-performance test environments for investigating the effects of cyber-attacks and developing countermeasures. Key topics are:

- Quick check
- IEC 62443
- Secure software products
- Assessment of security incidents
- AI Intrusion Prevention

With a focus on energy and water supply and industrial production, the learning laboratories at Fraunhofer IOSB are making an important contribution to strengthening cybersecurity in essential areas of society and industry. They promote networking between industry, science and government agencies and set new standards in the transfer of expertise and the development of innovative security concepts.

¹ Further information on the services offered by the Cybersecurity Training Lab can be found at the following link: <https://www.cybersicherheit.fraunhofer.de/en.html>

“Engineering Security for Production Systems”

The Industrial Cybersecurity Lab within the KASTEL Security Research Labs

Industrial production is an important sector of Germany's economy and ranges from fully automated production over mixed production to manual assembly of complex or specialized components. At the same time, it is increasingly the focus of cyber-attacks.

As part of the “Engineering Secure Systems” research topic funded by the Helmholtz Association, we operate the “Engineering Security for Production Systems” laboratory together with the Karlsruhe Institute of Technology (KIT). We are therefore also one of the KASTEL Security Research Labs [1].

Mission of the lab

In the lab, we deal with the security of production infrastructures and with trustworthiness, privacy and transparency of assembly assistance systems that monitor and support employees. The specific challenges are as follows: Industrial infrastructures must be constantly available and therefore have very long system runtimes. This is why old and vulnerable components are often in use. At the same time, cyberattacks in an industrial environment can have safety implications that endanger people and the environment. Assembly assistance systems are operated by the employer, which harbors the risk of misuse. For example, the performance of employees can be secretly monitored in violation of concluded company agreements.

Demonstrators play a crucial role in the lab for raising awareness of industrial cyber security. Using our demonstrators, we educate professionals about the challenges and threats as

well as the importance of implementing robust security measures through hands-on demonstrations and training.

Cybersecurity of production infrastructures and components

In our work on self-learning anomaly detection, we use advanced algorithms to detect unusual patterns in network traffic that indicate potential security incidents. Using machine learning, the system continuously evolves and improves its detection capabilities over time. We successfully evaluated the self-learning anomaly detection in our lab environment (cf. Fig. 1) and were able to both improve the detection rate and reduce the false-positive rate.

In black box tests, vulnerabilities of a system are analyzed without having an insight into its internal functioning. This approach facilitates an objective analysis of potential security weaknesses and attack vectors. We developed several improvements to black box testing for industrial components by using existing information about the system under test. With our security testing framework ISuTest® [2], several new vulnerabilities in components were discovered and could be fixed by the manufacturers.

In continuous risk and vulnerability management, system operators continuously identify, assess, and prioritize vulnerabilities and risks within their systems.

This process is essential to ensure the security of operational processes. We are developing



Dr.-Ing. Pascal Birnstill

Information Management
and Production Control (ILT)

Phone +49 721 6091 612
pascal.birnstill
@iosb.fraunhofer.de

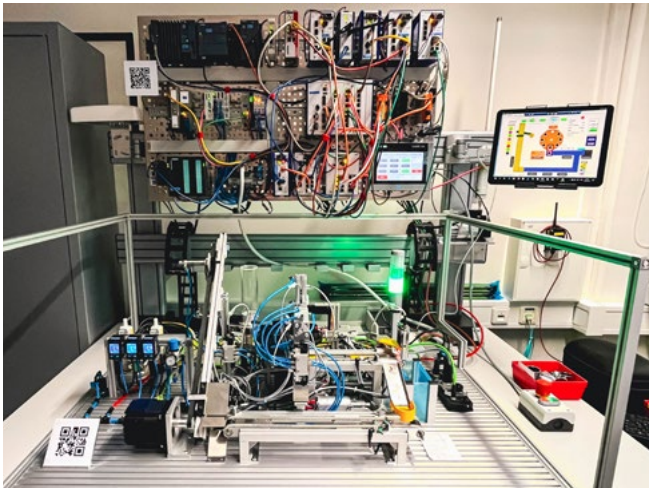


Fig. 1: Miniaturized production process with industrial infrastructure components.



Fig. 2: Interactive assembly station in our lab.

an integrated risk assessment framework to support asset owners at conducting risk assessments for their assets. It combines automated vulnerability management with AI-based threat detection and defense, and will serve as a tool for IEC 62443-based risk management.

Trustworthy and transparent interactive assistance systems

To realize trustworthy interactive assembly assistance systems (cf. Fig. 2), we leverage trusted computing technologies and their remote attestation capabilities. This enables us to make it verifiable for employees and works councils that the software and security configuration of a system are in an agreed state (cf. Fig. 3). To mitigate the risks associated with processed data, we implemented two frameworks that can protect data during storage (4Crypt) and during processing (DataSov).

4Crypt cryptographically enforces the approval of multiple trusted verifiers (multi-eye principle) before access to encrypted data is granted. DataSov implements distributed usage control in a trustworthy manner. This is done by ensuring the integrity of distributed components through heterogeneous attestation using various trusted computing technologies.

The European AI Act sets transparency requirements for certain application areas of AI and demands that decisions of such systems are understandable. Explainable AI is de facto the only technical implementation option to comply with the regulations. However, current methods focus on technical needs of

AI experts and data scientists. With RIXA, we implemented an interactive, explainable AI dashboard, which leverages large language models to make technical explanations understandable for laypersons.

The lab's research contributions address the long-term challenges for securing industrial production systems by developing innovative proof-of-concepts as well as technology demonstrators to support the transfer into practice.

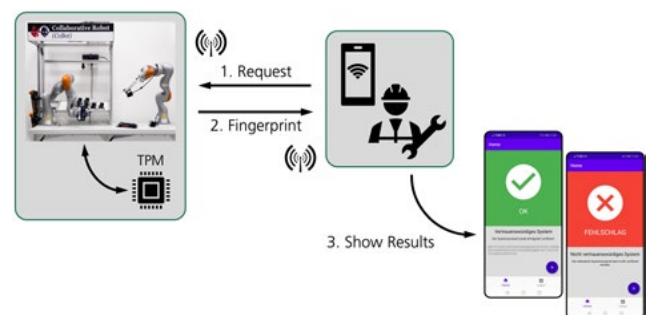


Fig. 3: Attestation of an assembly assistance system via NFC communication.

¹ <https://kastel-labs.de>

² <https://www.isutest.com>

Cyber resilience monitoring in industrial automation and control systems

Cyber resilience is the next stage of development in IT security and focuses on incident response and process recovery. This means that in the event of a critical cyber incident, an organization's operations should be maintained or restored as quickly as possible. Effective and appropriate monitoring of the process automation and infrastructure is essential for the technical implementation.

CyReM-ICS – a holistic monitoring system

In the CyReM-ICS (Cyber Resilience Monitoring in Industrial Automation and Control Systems) project, methods for attack detection and asset discovery were integrated into a holistic monitoring system.[1]. The system records input data from process infrastructures and serves as a basis for resilience metrics. CyReM-ICS was developed for the energy and industry domains and

aims to evaluate resilience properties and provide a clear overview of the condition of the systems. Different resilience metrics are combined to enable a process evaluation independent of the domain.

To unify both domains, process structures are summarized in such a way that status information about devices and network traffic is collected by freely available sensors as well as network and host intrusion detection systems (NIDS, HIDS). Specific modules, for example for detecting certain transmission protocols such as Profinet or IEC 61850, are available to the user.

How it works

The CyReM-ICS monitoring system consists of different modules based on an open-source SIEM system. This SIEM (Security Information



Dr.-Ing. Christian Haas

Information Management
and Production Control (ILT)

Phone +49 721 6091 605
christian.haas
@iosb.fraunhofer.de

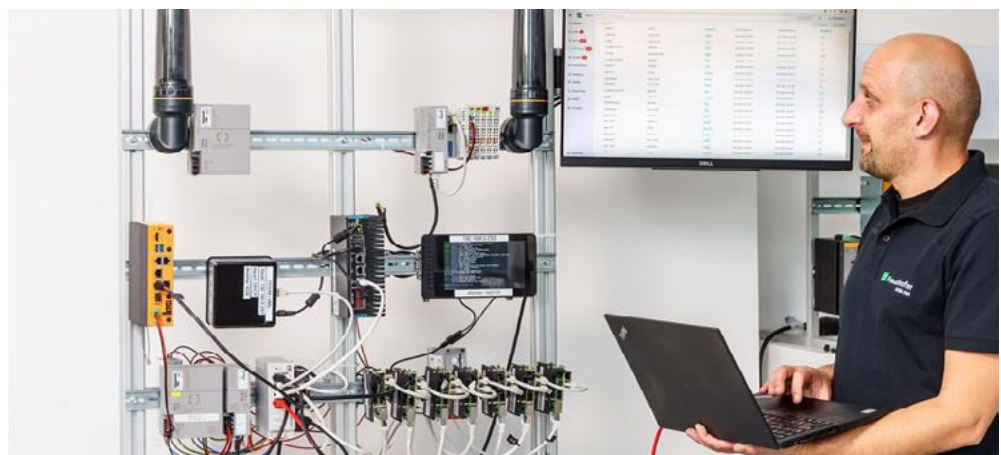


Fig. 1: CyReM-ICS is being evaluated using practical test setups that simulate real-life conditions in the energy and industry domains.



Fig. 2: Our extensive experience in vulnerability detection and hardening of industrial control systems flows into a new holistic resilience monitoring approach.

and Event Management) consists of a log database that is used for downstream evaluations, a defined pipeline for importing data from the connected sensors and systems, and a visualization of the collected data. Within CyReM-ICS, the collected data is used as a basis for continuously conducting resilience assessments with the help of an inventory system (asset inventory) and threat intelligence approaches, as well as risk analysis results. External data sources, such as vulnerability databases, are used as a further knowledge base for resilience assessment via defined interfaces.

The results of the resilience metric calculation are processed within the incident response and risk management and represent the outlook for an extension of the passive monitor to an assistance system.

What is the benefit of our system?

With CyReM-ICS, Fraunhofer IOSB can support operators of industrial automation and control systems as well as mechanical and plant engineering companies in conducting a transparent resilience assessment of their systems and plants and maintaining it during operation.

Mechanical engineers and operators of industrial control and automation systems are increasingly faced with the challenge of detecting cyber-attacks early and reliably and reacting accordingly. In addition to the Machinery Directive, the upcoming

EU NIS-2 Directive will provide a regulatory basis for this. As part of the Security Act, the German Federal Office for Information Security (BSI) is also tasked with offering manufacturer-independent solutions for detecting attacks and responding to them. With CyReM-ICS, Fraunhofer IOSB has a functioning demonstration environment for implementing projects and making results demonstrable.

Energy supply operators are increasingly using flow-based systems to detect attacks. The German Federal Office for Information Security (BSI) is using the mandatory use of attack detection systems as a lever to improve incident detection in critical infrastructure companies. Previous implementations and commercially available systems primarily rely on the analysis of network traffic and protocol information of exchanged messages. The logging information from the individual end devices is usually not integrated into central monitoring systems, such as SIEM systems integrated in the central IT systems, due to the diversity and the lack of competence to interpret the messages. Since ICS end devices can also provide a great deal of added value for detecting and combating attacks, an automated system is needed that integrates and processes the decentralized information and provides an interface to the central SIEM. CyReM-ICS supports companies in detecting attacks at an early stage, improving incident response and thereby ensuring compliance with EU directives.

1 <https://www.iosb.fraunhofer.de/en/projects-and-products/cyber-resilience-monitoring-industrial-automation.html>

Classification of cyberattacks on industrial control systems in encrypted network traffic



Felix Specht, M.Sc.

Cybersecurity in
production

Phone +49 5261 942 90 34
felix.specht
@iosb-ina.fraunhofer.de



Dr.-Ing. Jens Otto

Cybersecurity in
production

Phone +49 5261 942 90 44
jens.otto
@iosb-ina.fraunhofer.de

Industrial control systems (ICS) monitor and control cyber-physical production systems using specialized hardware and software, such as programmable logic controllers and input/output devices. Communication between these components is realized via industrial network protocols like Profinet, Modbus/TCP, and OPC UA [1]. Security monitoring of network traffic enables the early detection of cyberattacks, allowing timely initiation of countermeasures to protect production systems. This is also a central requirement of the EU Directive 2022/2555 “Measures for a high common level of cybersecurity across the Union” (NIS-2).

Efficient security monitoring in ICS must address several challenges: **(1)** The system should be capable of detecting novel and previously unknown cyberattacks; **(2)** attack detection must be possible even in encrypted network

traffic; **(3)** the analysis must consider specialized industrial communication protocols like Profinet or EtherCAT; and **(4)** the solution must operate efficiently on hardware with limited resources.

Researchers at Fraunhofer IOSB-INA have developed an innovative approach called CyberClas⁺ for classifying cyberattacks in industrial control systems, which meets the mentioned requirements [2]. CyberClas⁺ combines various machine learning methods to analyze network traffic in real time (see Fig. 1).

First, the network traffic from ICS is captured and split into individual connections. Each connection is then converted into a time series, during which statistical features are calculated – such as the number of network packets per second or the inter-arrival time between packets. Based on these features,

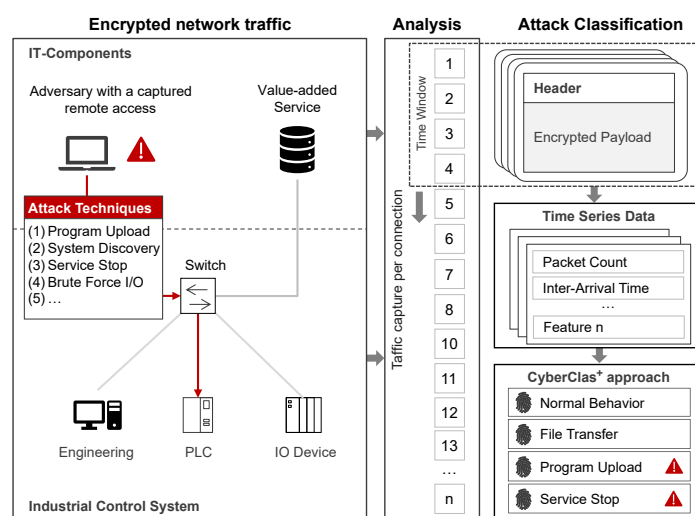


Fig. 1: Concept of the CyberClas⁺ approach for cyberattack classification of encrypted network traffic in industrial control systems.

thresholds are calculated, and a machine learning model is trained. The thresholds enable an initial distinction between normal and suspicious network traffic, while the machine learning model allows for the classification of various cyberattacks within the suspicious traffic according to the MITRE ATT&CK ICS classification scheme [3].

In an industrial test environment, the functionality of CyberClas⁺ was evaluated under real-world conditions (see Fig. 2). Fourteen different cyberattacks were successfully detected and distinguished from one another, with a classification accuracy of 97 percent. Additionally, by employing the initial threshold-based distinction, the execution time was reduced by up to a factor of 16 compared to traditional approaches.

CyberClas⁺ serves as a solid foundation for automated countermeasures against cyberattacks, such as network segmentation [4]. This technique divides the network into smaller, isolated segments, preventing the spread of attacks and thereby enhancing the security of production systems.

For companies, the use of CyberClas⁺ offers several advantages:

1. Real-time detection and classification of cyberattacks, which reduces response times during incidents.
2. Efficient operation even on hardware with limited resources, leading to cost savings.
3. Robustness against new threats through the ability to detect unknown attacks.
4. Enhanced security protects against production downtime and financial losses.
5. Assistance in complying with legal requirements, such as the NIS-2 Directive.

CyberClas⁺ is a key component of a comprehensive system called CyReM-ICS for monitoring cyber resilience. In addition to network traffic monitoring, the system enables the analysis

of syslog data to identify attacks directly at the device level. It gathers device information such as part numbers and known vulnerabilities, providing an up-to-date overview of potential risks. All relevant information is consolidated and made available so that responsible personnel can efficiently assess the security situation and respond quickly to incidents.



Fig. 2: The industrial test environment for evaluating the CyberClas⁺ solution.

- 1 J. Otto, B. Vogel-Heuser, O. Niggemann. Automatic parameter estimation for reusable software components of modular and reconfigurable cyber-physical production systems in the domain of discrete manufacturing. IEEE Transactions on Industrial Informatics, 14(1), 2018. DOI: 10.1109/TII.2017.2718729.
- 2 F. Specht, J. Otto. Efficient Machine Learning-based Security Monitoring and Cyberattack Classification of Encrypted Network Traffic in Industrial Control Systems. IEEE 29th International Conference on Emerging Technologies and Factory Automation (ETFA), September 2024. DOI: 10.1109/ETFA61755.2024.10711134.
- 3 O. Alexander, M. Belisle, J. Steele. Mitre att&ck for industrial control systems: Design and philosophy. The MITRE Corporation: Bedford, MA, USA, vol. 29, 2020.
- 4 J. Otto, N. Grüttemeier, F. Specht. Security Decisions for Cyber-physical Systems based on Solving Critical Node Problems with Vulnerable Nodes. AAAI-Workshop on AI Planning for Cyber-Physical Systems (CAIPI'24), Vancouver, Canada, 2024. DOI: 10.48550/arXiv.2406.10287.

Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB

info@iosb.fraunhofer.de
www.iosb.fraunhofer.de

Fraunhofer IOSB Karlsruhe
Fraunhoferstraße 1
76131 Karlsruhe, GERMANY
Phone +49 721 6091-0

Fraunhofer IOSB Ettlingen
Gutleuthausstraße 1
76275 Ettlingen, GERMANY
Phone +49 7243 992-0

**Advanced System Technology
branch IOSB-AST**
Am Vogelherd 90
98693 Ilmenau, GERMANY
Phone +49 3677 461-0
info@iosb-ast.fraunhofer.de
www.iosb-ast.fraunhofer.de

**Industrial Automation
branch IOSB-INA**
Campusallee 1
32657 Lemgo, GERMANY
Phone +49 5261 94290-22
juergen.jasperneite@iosb-ina.fraunhofer.de
www.iosb-ina.fraunhofer.de

Branches

**IT Security for critical infrastructures
ENERGY AND WATER research group**
Wilhelmsplatz 11
02826 Görlitz, GERMANY

**Fraunhofer center for the
Security of Socio-Technical
Systems SIRIOS**
c/o Fraunhofer FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin, GERMANY

**Smart Ocean Technologies
research group SOT**
Alter Hafen Süd 6
18069 Rostock, GERMANY

Active laser fibers research group
c/o HENSOLDT Optronics GmbH
Carl-Zeiss-Str. 22
73447 Oberkochen, GERMANY

Liaison office Beijing
Unit 0602G, Tower D1
DRC Liangmaqiao Office Building
19 Dongfangdonglu, Chaoyang District
100600 Beijing, PR China
muh@fraunhofer.com.cn



ePaper issue