https://doi.org/10.2352/ISSN.2470-1173.2021.3.MOBMU-073

Conception and Implementation of Professional Laboratory Exercises in the field of ICS/SCADA Security - Part I: Fundamentals

Maximilian Richter [1] ***, Klaus Schwarz*** [2,3] ***, Reiner Creutzburg*** [1,2]

[1] ***Technische Hochschule Brandenburg, Department of Informatics and Media, IT- and Media Forensics Lab, Magdeburger Str. 50, D-14770 Brandenburg, Germany***
Email: maximilian.richter@th-brandenburg.de, creutzburg@th-brandenburg.de

[2] ***SRH Berlin University of Applied Sciences, Berlin School of Technology, Ernst-Reuter-Platz 10, D-10587 Berlin, Germany***
Email: klaus.schwarz@srh.de, reiner.creutzburg@srh.de

[3] ***The University of Texas at San Antonio, College of Engineering, 1 UTSA Circle, San Antonio, TX 78249-0669, USA***

Abstract

Industrial control systems are essential for producing goods, electricity generation, infrastructure maintenance, and the transport of energy, water, and gas. They form the core of the critical infrastructure of modern industrial nations and are therefore of particular interest. Through the increased inter-connectivity of formerly isolated ICS process environments and standard IT technologies such as Ethernet, processes can be optimized and synergies leveraged. However, ICS/SCADA also becomes the target of the same cyber-attacks as conventional IT systems. Therefore, it is necessary to combine IT security has accumulated knowledge and experience with the classic Safety-First-mentality of ICS/SCADA environments to avoid significant problems in the foreseeable future. The new course was created for precisely this purpose. The investigation of the security of systems and organizations in Red and Blue Teams has long proven it is worth and is used worldwide. The first part of the Red Team side exercise deals specifically with finding and exploiting security vulnerabilities. Red Teaming refers to an independent group that acts as a counterpart to an organization to improve its operational effectiveness and enhance its security. It is the declared goal of the Red Team to detect security vulnerabilities. This work is intended to convey this interfacing knowledge; in the practical exercises for Red Teaming, these hybrid infrastructures and systems' weak points are identified and exploited. Students will participate in numerous hands-on exercises throughout the course using the tools and techniques that form the basis for attacks on infrastructure, such as industrial control systems. A detailed accompanying theory precedes the exercises, and the course is structured as follows:

Introduction

- *ICS Cyber Kill Chain*
- *Types of information gathering*

Red Team Tools

- *Nmap*
- *Maltego*
- *Shodan*
- *Google hacking*
- *The Harvester*
- *Wireshark*
- *GrassMarlin*
- *Metasploit Framework (MSF)*
- *John the Ripper*

Exercise 1 - Open Source Intelligence (OSINT)

- *Gathering information with Maltego*
- *Find Remote Access with Google and Shodan*

Exercise 2 - Analysis of network recordings

- *Analysis of ICS network recordings with Wireshark*
- *Analysis of ICS network recordings with GrassMarlin*

Introduction and Motivation

Industrial control systems are essential for producing goods, generating electricity, maintaining infrastructure, and transporting energy, water, and gas. They are at the heart of critical infrastructure and are vital for the preservation of our civilization. The increasing networking of ICS/SCADA infrastructures and the growing exchange of information with IT systems lead to more efficient use and reduced administrative expenses. However, the danger of cyber-attacks has increased in recent years. According to a survey by Bitkom, around a fifth of all industrial companies surveyed will be victims of a cyber attack in 2018, in which digital sabotage of information and production systems takes place [1]. In addition to the attack on the Iranian nuclear program by the malware, Stuxnet [2], a security incident in a German steel plant in 2014 was the first publicly confirmed case of physical destruction of production systems by a cyber attack. The German Federal Office for Information Security (BSI) considered this incident in its 2014 status report on IT security in Germany [3]. According to the BSI's management report on IT security in Germany in 2018, the threat to the critical infrastructure is at a high-level overall [4], with the telecommunications and energy

sectors significantly affected. This development clearly shows that the protection of ICS/SCADA systems and networks has taken on a high priority, and capable personnel is required for this.

Objectives and Demarcation

This work aims to familiarize students with IT knowledge with the ICS/SCADA concepts and unique features. Additionally, convey complex exercises in the field of Red Teaming - practical knowledge and procedures of individual phases of the ICS Cyber Kill Chain [5]. Understanding the attackers' methodologies and tools is interesting for penetration testers and is also of great value for implementing an effective defense against cyberattacks on ICS. For this reason, the students are guided through the individual phases of dealing with a security incident in the subsequent Blue Teaming complex exercises. Since the target audience is students of computer science without previous knowledge of the ICS/SCADA topic, more in-depth analysis and manipulation of ICS protocols and the execution of a complex security incident handling exercise will not be necessary.

Structure of the work

After the introduction, the second chapter introduces the essential components of ICS/SCADA environments, the Perdue reference model is presented, and the differences between IT systems and ICS are pointed out. Cybersecurity concepts are also covered for completing the lab courses and the basics of IP networks and other IT technologies. This information is provided in the third chapter. Furthermore, possible attack scenarios and types of attackers are mentioned and described. After explaining the laboratory setup and the students' instructions, the first exercise complex on the topic of Red Teaming follows. While working on the tasks, the students will be introduced to the ICS Cyber Kill Chain [5] after a short introduction. They will get a practical understanding of how an attacker can create a comprehensive dossier about employees of an organization by using social media and freely available information. Also, the analysis of network recordings from an ICS infrastructure will help to internalize the use of Wireshark and GrassMarlin. In the last exercise, the students will learn how to use a Windows VM via the internal network and then adopt it. The second set of exercises on the subject of Blue Teaming puts the students in an incident responder who has to take action in the individual phases of a security incident. The work is concluded with a summary and an outlook into the future of ICS/SCADA security.

Terms in ICS/SCADA

Industrial Control System(ICS)

ICS is a collective term for all types of control systems in industry and critical infrastructure. An ICS consists of combinations of control elements (for example: electrical, mechanical, hydraulic, pneumatic) that work together to achieve a goal in the physical world, for example, the production or transport of a good or energy. In the upper graphic, one can see a simplified representation of an ICS process. The term process is used for the part of the system that provides the actual output. The controller

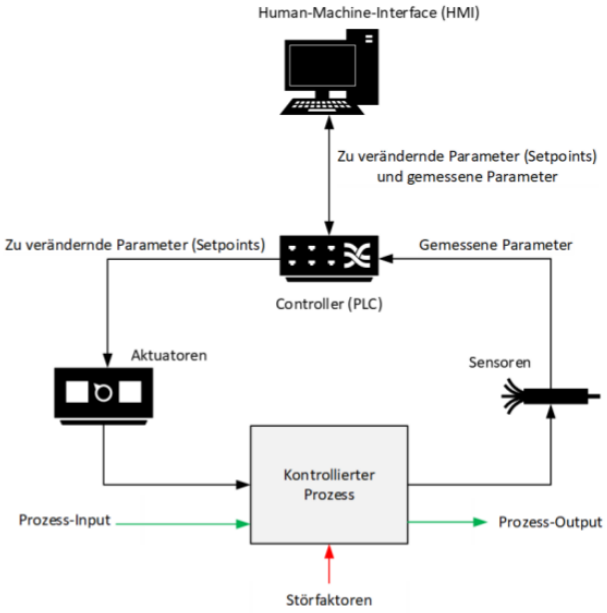


Figure 1. *Simplified representation of an ICS process (according to NIST SP800-82 [6])*

part ensures that the given specifications are met. Using a Human Machine Interface (HMI), a human (operator) can enter new parameters to adjust the process (setpoints). Actuators, such as pumps or motors, convert the parameters into reality, and sensors provide feedback to the controller whether the actual conversion is correct.

Supervisory Control And Data Acquisition (SCADA)

A SCADA system is a type of ICS control system. Its unique feature is implementing very extensive processes, often involving several locations and large geographical distances. An essential requirement for SCADA systems is central control and data collection. These processes can be divided into two types, industrial processes and infrastructure processes. [6]

- Industrial processes include the production of goods, power generation, or the control of refineries.
- Infrastructure processes include, for example, the control of water supply and wastewater disposal, the distribution, and transmission of electricity, the operation of oil and gas pipelines, and the control of large telecommunications networks.

Figure 2 shows a simplified representation of a SCADA system controlling an industrial process with three geographically separated locations.

Programmable Logic Controller (PLC/PLC)

PLC are devices that can be programmed to control and regulate mechanical processes. Compared to earlier control devices, the unique feature is the possibility to change the stored programs if necessary without having to exchange the device itself [7]. Due

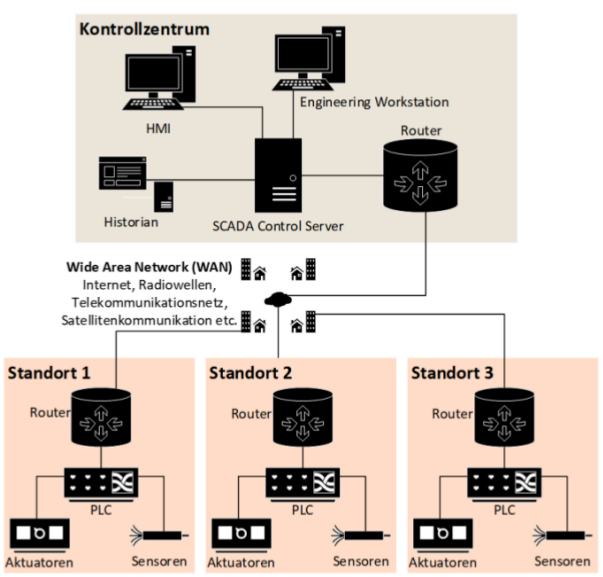


Figure 2. *Simplified representation of a SCADA system with 3 locations (self created)*

to the external conditions in their operating locations, the devices are designed to withstand physical stress such as pressure, dirt, and heat. They have multiple I/O (input/output) connectors, and their outputs are adjusted as needed based on the new inputs. The logic is controlled and executed using states. In Germany, the term Programmable Logic Controller (PLC) has become generally accepted.

Field Devices

Field devices are the interface from the digital and analog world to the physical. They are divided into actuators and sensors. Actuators carry out the mechanical actions dictated by the control signals of ICS systems such as PLCs. Sensors measure specific parameters of the process and send these measured values back to the controlling systems. Actuators are, for example, valves, pumps, motors, compressors, or centrifuges. Sensors measure, for example, temperature, humidity, pressure, or vibrations. The communication to these devices is called I/O (Input/Output).

Human Machine Interface (HMI)

A Human Machine Interface (HMI) provides a graphical user interface (GUI) that allows operators to overview the process's current state quickly. In case of emergency, warnings are displayed here, and usually, there are buttons to directly change the parameters of the process. The figure 3 shows an example of an HMI.

HMIs are the systems that most people think of when they imagine a control room in a factory or power plant. However, they are still an optional component [7], as the actual process can also be completely automated, but in most cases, an HMI is extremely valuable in preventing potential damage. HMI can take many forms, from traditional panels with electrical switches and warning lights to web interfaces in web browsers. Since an

Figure 3. *Example of a HMI [44]*

HMI provides a simplified representation of the process and a direct manipulation possibility, such systems are a worthwhile target for potential attackers.

Master Server/ Control Server

There are many names for the Master Server within ICS environments, such as Control Server, SCADA Server, Supervisory Controller, or Master Terminal Unit(MTU), but these systems are the same scope of this paper and are therefore referred to as Master Servers in the following.

A master server runs the control software that communicates with the individual PLCs within an ICS network. For this purpose, the proprietary protocols of the respective manufacturers are used, or free alternatives such as Modbus [8], which will be discussed in detail in this work. The devices controlled in this way are called slaves. A unique feature of ICS protocols is that communication connections can only be started from the master. [6] In most cases, master servers do not use unique ICS operating systems, but regular server operating systems such as Windows Server or Linux derivatives like Redhat. [7] This makes it especially important to isolate these servers from the Internet, as they are vulnerable to regular IT malware.

Engineering workstation

Engineering workstations are computers with a regular operating system, such as Linux or Windows, used to make changes to ICS systems, for example, for maintenance work or programming. Because of these extensive rights, these workstations are particularly worthwhile targets. In addition to the possibility of directly changing processes, two important files can also be stolen: Project Files and Runtime Libraries. Project files contain details about the control systems used, the network architecture, configuration states, the logic and parameters of the processes, and the individual inputs and outputs' names. An attacker can use this information; a well-known example for such a scenario would be Stuxnet [2]. Runtime libraries can be compared to conventional programming interfaces (API). They are installed on servers, workstations, and individual devices in the ICS network and provide a standardized interface. This

enables easier integration of ICS components from different manufacturers into one infrastructure. Furthermore, data from the ICS area can be made available to the business area. An insight into these libraries provides attackers with a detailed listing of the network structures and the individual components. [6]

Historian

A historian is a central database system for ICS process data. Most historians are based on traditional relational database management systems such as Oracle or SQL Server. Functions for data analysis and evaluation are provided. The stored process data includes classic logs with timestamps and connection information and process inputs like mixing ratios or timers. All other important information is also stored here, such as quantities of resources still available for production or processing. This information is enormously valuable for the business side of the company to optimize and automate procurement processes. There is a strict division due to the risk of a possible attack on historians by infected systems on the Internet-connected business level. The so-called master Historian is located in the ICS control zone, which performs the tasks mentioned above, and a Read-Only Data Historian in the Control System DMZ. These terms will be explained in the context of the Perdue model. The read-only Historian is filled with selected data records from the master historian through a unidirectional gateway. This ensures a strict separation between ICS and business.

Safety Instrumented System (SIS)

Safety Instrumented Systems (SIS) are devices and systems that monitor specific parameters and intervene if deviations are too large to prevent man and machine damage. These systems are usually isolated from the rest of the ICS infrastructure to minimize the chances of failure. Deviations are detected by the safety monitoring systems, including leakage warning devices, fire detectors, radiation meters, or gas detectors.[7] If a deviation occurs, the Safety Remediation Instruments ensure that the damage is limited. These include pressure relief valves, emergency stop switches, and sprinkler systems. The specific control functions performed by SIS are called Safety Instrumented Functions (SIF). These are implemented according to the risks identified, their damage potential, and the probability of their occurrence.

Unidirectional gateway/data diode

A unidirectional gateway is a mixture of hardware and software designed to isolate the IT infrastructure's ICS infrastructure while still allowing information to flow into the business systems. A data diode ensures the isolation in the hardware; data flow is only possible in one direction. In recent years, increased requirements for site redundancy, remote support, and business process optimization have made it necessary to open up the ICS infrastructure. The gateway's software components enable the transfer of information to databases and historians in the Control DMZ.

Perdue Reference Model

The Perdue reference model is a conceptual representation of the connections and dependencies of infrastructure components with ICS systems. [9] Based on this productivity reference model, experts developed the ICS410 reference model [7], the aim being to make a concrete recommendation regarding the placement of the devices within the network of a production site or power plant, for example. However, the term "production reference model" will be used in the following work for better comprehensibility; the authors also recommend this. The reference model is divided into several zones with their corresponding levels. A unique feature is the so-called Enforcement Zones, which control the flow of information between the individual areas and ensure a defense-in-depth for the ICS systems' adequate protection. Firewalls and data diodes are used in these zones.

Business Zone

The business zone contains both the systems that provide web services and the regular systems of the office environment.

Level 5: Enterprise Business Network

Figure 4. *Example for devices in the Enterprise Business Network (self-created according to [7])*

This level includes systems with which customers can interact and are used for processes within an entire company. Devices in level 5 can be, for example, email servers, web servers for the company homepage, intranet servers, WiFi access points, personnel management systems, or DNS servers.

Level 4: Site-specific network

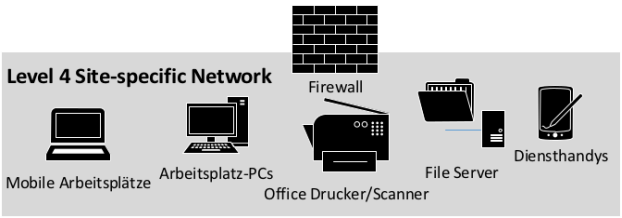


Figure 5. *Example of devices in a site-specific network and representation of the first enforcement zone (self-created according to [7])*

Between levels 5 and 4, there is the first enforcement zone in the form of a firewall, which protects the intranet's systems from possible attacks that may emanate from publicly accessible servers of a higher level. This is the last level, which should have a permanent connection to the Internet since processes such as the procurement of resources, personnel management, or communication with business partners occur here. This level contains the classic office IT; printers, workstation PCs, file servers, business intelligence systems, laptops, and service cell

phones, and directory services.

Control System DMZ Firewall

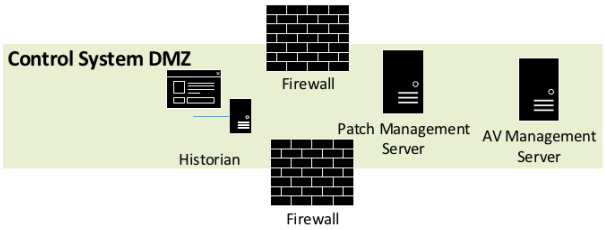


Figure 6. *Example for devices in the Control System DMZ (self-created according to [7])*

This demilitarized zone is necessary for the strict separation of the ICS and IT infrastructure; two firewalls are used to establish the enforcement zones between the business zone and the control zone. Services are provided in this zone to exchange information between the two zones in a controlled manner, so the business zone needs information from production to optimize procurement processes. The production systems also require updates and updated signatures for their antivirus (AV) programs at regular intervals. Devices typically placed in the Control System DMZ are patch management servers, antivirus management servers, historians, development systems, and backup database systems.

Control Network

Level 3: Operations Support and Level 2: Supervisory Control

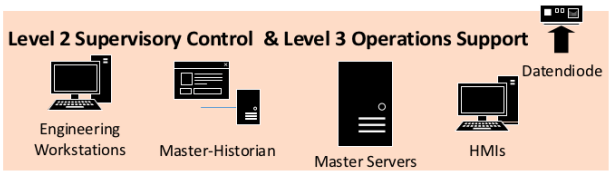


Figure 7. *Example of devices in Operations Support and Supervisory Control (self-created according to [7])*

These two levels are responsible for managing the production environment, monitoring and controlling of the manufacturing processes. The systems of these two levels constitute the control room of the production facility. Data diodes are used to transport information from these levels to the Control System DMZ to prevent bidirectional communication. These systems include the HMIs, the master historian, the engineering workstations, alarm systems, and various master servers.

Level 1: Control Devices

The systems at this level are directly responsible for controlling the individual process steps. These systems include the PLCs and device-specific HMIs as well as operator workstations.

Level 0 Instrumentation

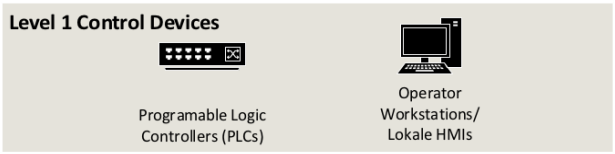


Figure 8. *Examples for Control Devices (self-created according to [7])*

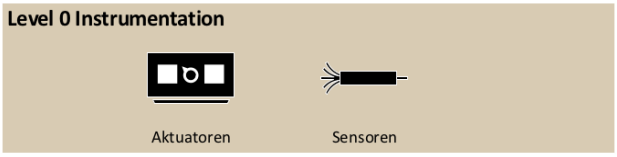


Figure 9. *Examples of instrumentation devices (self-created according to [7])*

At this level, the conversion of information into physical processes, the measurement of physical conditions, and the transmission of the determined information occur. The actuators and the sensors realize this.

ICS Protocols

What is the communication protocol?

A communication protocol is a formalized agreement between two entities that defines how the two entities connect (see [8]). Communication in IP networks such as the Internet is described by the TCP/IP stack, a collection of several standard communication protocols that do the other layer's work. This encapsulation and abstraction make it possible to send different communication protocols over the same hardware infrastructure.

Modbus / Modbus TCP

The Modbus protocol was developed in the 1970s by the company Modicon to realize communication between PLCs. Due to its simplicity and lack of license fees, it is one of the most widely used ICS protocols today. The communication follows the master-slave model; the master server must actively address the individual slaves to obtain information, a connection establishment from a slave is not possible. Communication consists of request and response packets. [8] Due to the widespread use of Ethernet networks, a version of Modbus TCP has been developed to communicate using IP and MAC addresses. This is realized by a TCP wrapper around the actual Modbus protocol; an example is shown in the screenshot below a Modbus TCP packet in Wireshark. One can see the master and the slave's IP addresses, the standard Modbus TCP port 502, and the actual payload.

PROFIBUS/ PROFINET (Process Field Network)

Profibus (Process Fieldbus) is a communication protocol between PLC, field devices, and master servers. Like Modbus, it is based on the master/slave principle. The Ethernet implementation is called Profibus. [8]

EtherNet/IP (Industrial Protocol) / Common Industrial Protocol (CIP)

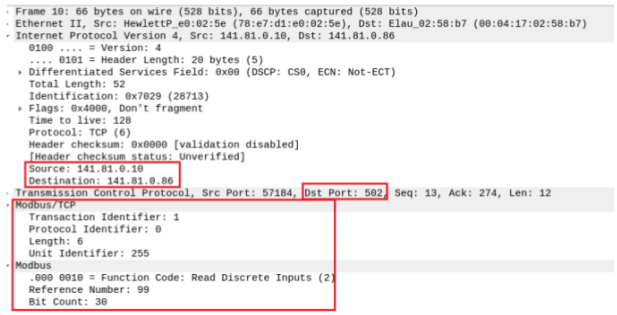


Figure 10. *A Modbus TCP packet in Wireshark broken down into its individual layers (source: own screenshot)*

EtherNet/IP was created to enable ICS systems to use an existing Ethernet infrastructure to transfer communication packets between PLCs, master servers, actuators, sensors, and other devices. EtherNet/IP forms Ethernet frames around the actual ICS communication. This communication is realized by the Common Industrial Protocol (CIP). Therefore, when looking at network recordings from Ethernet networks in Wireshark, EtherNet/IP and CIP are considered a unit. [7] Figure 11 shows this encapsulation of the CIP packet within the EtherNet/IP packet.

Figure 11. *An EtherNet/IP+CIP packet in Wireshark broken down into its individual layers (source: own screenshot)*

S7 Communication

The S7 Communication Protocol is a proprietary communication protocol from Siemens, which is used for programming and communication between the PLC and Master Servers. [10] It should be noted that the actual S7 Communication packets are packed into Connection-Oriented Transport Protocol (COTP) packets. Therefore, when analyzing the protocol in Wireshark, both the S7COMM and the COTP packets are to be considered as S7 Communication.

Differences between IT and ICS

The following 3 tables illustrate the difference between IT and ICS.

IT	ICS
Expertise in the IT world is transferable between individual agencies and companies in many fields.	Company and industry-specific engineering skills, hardware as well as software. Expert knowledge is often required.
Computing power, memory, RAM, and similar hardware limitations scale well.	Processing power and memory of the field devices and PLC is often limited, and the devices have little to no expandability.
Risk assessments focus on losses in the business sense or Data loss.	Risk assessments go beyond business losses, focusing on the loss of life and damage to the environment.
Regular operating systems such as Windows, Linux, BSD, etc., are used.	Regular operating systems such as Windows and Linux, as well as special real-time operating systems (RTOS) are used in the controllers.

General differences between IT and ICS

IT	ICS
Operation takes place in climate-controlled data centers and office environments. Therefore, tolerances in the hardware used are quite high.	The operation happens especially with Field Devices and PLC mostly in environments with extreme temperatures, impurities, vibrations, etc.. This leads to high demands on the hardware used. hardware.
There are regular maintenance and update cycles.	System updates only happen when urgently needed; systems often have to be shut down for maintenance.
Errors in operation cannot be ruled out with the software used but are acceptable within certain limits.	The software used requires error-free operation in order to function (States). With the help of predictive maintenance, components are replaced before the error can occur.

Differences in availability and reliability between IT and ICS

Cybersecurity Terms for ICS/SCADA

Critical infrastructure

Critical infrastructure includes facilities and systems that are ”essential to the maintenance of essential societal functions, health, safety, security and the economic or social well-being of the population and whose disruption or destruction has a significant impact on a country.” (see [11]) Many of these tasks are implemented by ICS systems, which leads to high requirements regarding their security. Operators and manufacturers must implement the applicable regulations in their respective countries and prove to the legislator that they have implemented the necessary protective measures.

Red Teaming & Blue Teaming

These terms have been taken from military and intelligence terminology and denote the attacker’s role or the defender in a cybersecurity context. The difference of a red-team approach compared to a conventional penetration test is a more realistic attack scenario since other attack vectors such as social engineer-

IT	ICS
The communication protocols used are standards that already include many security features such as end-to-end encryption.	Many manufacturer-specific protocols are used for communication. These often do not include any security features.
The devices and systems used are now being developed with a focus on security.	The devices and systems used are now mainly developed with a focus on reliability and safety.
The hardware components used are standard IT products. This simplifies procurement and ensures relatively low costs.	Many components are special hardware that is often only offered by a few manufacturers. In conjunction with the high requirements due to the working environment, this results in high costs.
There is a large market of security solutions for networks, server and client systems, etc.	Security solutions usually have to be adapted in order to be used in the ICS environment. One such example of successful adaptation would be the use of firewalls in ICS networks.

Differences in security between IT and ICS

ing attempts are used and the classic testing of IT systems and networks. This way, the results can support the affected company in identifying possible weaknesses and implementing appropriate defense measures. Blue teaming includes the company's holistic protection by continually monitoring and hardening the IT infrastructure and actively seeking undiscovered malware in one's network (Threat Hunting). Furthermore, this area includes the operation of an Incident Response Team (IR Team) to be able to react quickly and efficiently in case of a security incident.

Malware

Malware, also known as malware or malicious software, is a collective term for computer programs that perform functions on the target system that directly or indirectly harm the actual owner. The main targets of malware include the destruction of data and the theft of information. Some categories of malware: [7]

- Virus
  - The execution of computer code spreads a virus by the user. The malicious program itself is stored on the system. Client systems and workstations are the preferred targets, as interaction by the user is required.
- Computer worm
  - Unlike conventional viruses, computer worms can spread independently in a network and infect other systems. This type of spreading is a major risk for systems connected to the Internet.
- Trojans / Remote Access Trojans (RAT)
  - Trojans are characterized by the fact that they hide inside a computer program that appears benign to the user, a popular example of this is illegal versions of programs such as Adobe Photoshop or Microsoft Office. Trojans are often used to obtain backdoors, in which case one speaks of a Remote Access Trojan (RAT).
- Backdoor
  - This type of malware opens a backdoor for the attacker on the target system, usually taking advantage of the fact that known ports such as 443 for HTTPS are open on the firewall, and the connection is made from the internal company network to the outside. The connection is called C2 (Command&Control) servers, mostly to enable remote access and to reload further malware.
- Bot/Zombie
  - This is the name given to systems that a C2 server can remotely control. These systems are used for DDoS (Distributed Denial of Service) attacks, where large networks of bot systems make simultaneous requests to the target systems until they become overloaded and shut down.

Vulnerabilities (CVE)

Vulnerabilities are errors in a system or process that can be exploited by a threat to cause damage. Such weaknesses are unavoidable in complex systems. They are usually the result of bad program code, misconfigured security solutions, or incorrect operation [6]. There is a common name for specific vulnerabilities in systems and programs in the IT and ICS security industry, the Common Vulnerabilities and Exposure (CVE), whereby an identified vulnerability is assigned an abbreviation including an identification number to facilitate the exchange of information by security researchers. Databases containing the collected information are freely available online; an example of this would be the National Vulnerability Database2 of the American National Institute of Standards and Technology (NIST).

Firewall/Packet Filter

A firewall, also known as a packet filter, is a system that controls network traffic between computer networks and filters it according to specific rule sets. There are both dedicated hardware solutions and software firewalls that run on regular servers or end-user devices. [6] In addition to the classic filtering of data streams based on IP addresses and ports used, there are firewall solutions that monitor the content of data packets (application-level firewalls) and check whether a valid communication connection already exists (stateful firewalls). Firewalls are used in the ICS/SCADA environment to isolate the business zone and the control zone and protect against malware and manipulation of ICS communication. An advantage of firewalls at the control level is implementing strict whitelisting, i.e., any communication that is not explicitly allowed is blocked. The generated traffic of an ICS process is predictable and constant, so maintaining a restrictive whitelist is economical.

IT Protocols and Technologies in the ICS Environment

Domain Name System (DNS)

The Domain Name System is an essential service in IP-based networks. It is used to obtain the IP address associated with a domain; this process is called name resolution. DNS simplifies the navigation on the Internet because instead of cryptic IP addresses, speaking domain names can be used. So if a client wants to communicate with the domain test.de, it sends a DNS request to one of the central DNS servers, which has a mapping table with the name-IP address pairs. After the corresponding IP address is found, it is communicated to the client. Modern web browsers handle this process automatically; the user usually does not notice anything. The results of DNS queries are cached on the client system for a short period in order to be able to make different page calls under the same domain faster and to keep the load on the DNS servers low. Within company networks (intranet), DNS servers are also used to simplify the navigation of individual services for employees. At the control level, however, the use of DNS servers is not yet widespread. One of the essential DNS servers on the Internet is 8.8.8.8, owned by Google.

IP, MAC addresses & hostnames

Devices in an IP-based network have a MAC address, an IP address, and optionally a hostname. Media Access Control (MAC) addresses are static and are burned in by the manufacturer during the production of the network card, which is used to identify individual devices uniquely. The length of MAC addresses in standard Ethernet networks is 48bit (6 bytes). Using the Address Resolution Protocol (ARP), an IP address is assigned to a MAC address. [7] IP addresses are used by other protocols such as HTTP or Modbus to identify the sender and receiver of the individual data packets. Hostnames can be found out by using DNS. There are currently two IP versions, IPv4 and IPv6.

IPv4	IPv6
32-bit addresses Example: 12.45.102.7	128-bit addresses Example: fe80::23:45:e32:df21
4.2 billion possible addresses	340 sextillion (10^{36}) possible addresses
Encryption is implemented by other protocols	Has functions for encryption
Combination of MAC and IP addresses for unique identification	Each device has its own IPv6 address for unique communication, the MAC address is not needed.

Comparison between IPv4 and IPv6 (simplified according to [7])

IPv4 networks are specified in CIDR notation; an example would be 192.168.1.0/24. CIDR stands for Classless Inter-Domain Routing. To calculate the number of available addresses, one has to subtract 2 with the difference of 32 and the number after the slash; therefore, our example network contains $2^{(32-24)} = 256$ addresses. For a detailed consideration of the conversion, only knowledge of the notation is relevant for the completion of the exercises in the context of this work. In the following diagram of the company "Test," you can see the process of a connection establishment of the user to the internal email server; there was no connection to it in the run-up. Therefore an ARP broadcast is necessary to establish the connection. After these four steps, the user can access his email box.

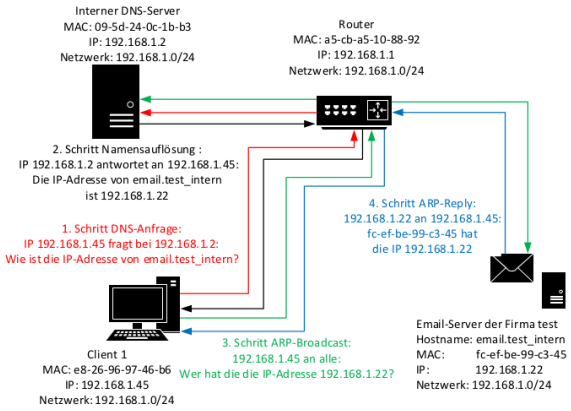


Figure 12. *Representation of the individual steps in establishing a connection in an IP-based network.*

Transport Control Protocol & User Datagram Protocol (TCP & UDP)

TCP and UDP are widely used network protocols that define how data is exchanged between network devices. They differ in their properties and application areas, which are shown in the following table.

Transport Control Protocol (TCP)	User Datagram Protocol (UDP)
A connection is established before the actual data exchange (TCP handshake).	Data packets are sent directly to the destination IP.
There is a confirmation in case of a successful transfer.	There is no confirmation regarding the successful transfer.
Larger headers are required in the individual data packets to store the connection data. Therefore, the transmission of data quantities is slower overall, since more packets are required.	Due to a lower overhead compared to TCP, the transmission of data quantities is faster because fewer packets are required.

Differences between TCP and UDP (simplified according to [7])

Motivation and goals of attackers

Types of Attackers

- Small-time criminals and script kiddies fall into the same category. Their goals are mostly opportunistic, either for financial reasons or to gain recognition among like-minded people. They do not have significant financial or technical

resources, and traditional IT security solutions can prevent their attacks. However, there is a risk through social engineering or the publication of powerful hacking tools by governmental organizations. An example of this would be the Wannacry malware, which was based on attack tools of the American National Security Agency (NSA) that had become public and exploited by groups with little technical expertise to cause great damage [12].

- Hacktivists and terrorists are politically and/or religiously motivated groups that pose a threat, especially concerning the central role of ICS systems in critical infrastructure. Their attacks serve to enforce their political or religious goals and values. Here, the physical protection of systems and locations must also be given special consideration, as these attacks allow access to IT systems or destroy them directly. The financial and technical resources vary greatly between individual organizations, especially if there are connections to state actors (APT), a high threat potential can be assumed [12].
- State actors, also known as Advanced Persistent Threat (APT), are usually military or intelligence organizations of individual governments. They have a high level of technical and financial resources. In addition to the classic espionage for government bodies, industrial espionage is also carried out for companies in their own country. This attacker is the greatest threat to ICS/SCADA systems, as critical infrastructures are a worthwhile target in modern conflicts (cyberwar).

Why are ICS systems attacked?

ICS systems represent most of the critical infrastructure of most states, and they are still essential for the production and transport of goods and commodities in all industries. Therefore, targets include financial gain or damage, industrial espionage, terrorist attacks, IT-supported warfare (cyberwar), and public attention to the attackers.

Attacks on ICS servers and workstations

Inadequately protected master servers pose a major risk to an organization because they control the largest number of devices and processes. Workstations can include the HMIs of the process owner and the engineering workstations of the programmers, who have extensive rights to manipulate the processes. Access to an HMI enables even less experienced attackers to cause damage with just a few clicks. One reason why attacks focus on this level is the familiar structure of a TCP/IP network for attackers; well-known IT security tools and procedures can be used here. Once project files or HMI interfaces have been discovered, this can be used to plan targeted attacks on the Perdue model's lower levels. Attacks on ICS servers and workstations are mostly from the Internet via business-level devices with communication links to the control level despite all isolation. These can be remote maintenance accesses of the manufacturers or the own administrators. A further possibility for Internet connections to the control level is the so-called shadow IT; these are devices brought along privately by the staff, not listed in any network plan. These can be anything from own WLAN routers to game consoles and private computers. [7] Malware can still penetrate the control layer via infected mobile data carriers, as in the case of Stuxnet, an attack on an Iranian uranium enrichment plant. A USB stick used to transfer updates to the isolated ICS zone was infected, allowing the malware, which originally spread via the Internet, to spread to the control of the centrifuges. [2]

Operating systems of the ICS servers as gateway

The majority of ICS servers and workstations use regular operating systems like Windows or Linux. This results in lower costs for acquisition, maintenance, and employees' training than a particular system. [13] However, these operating systems bring a large number of weaknesses and exploits from IT security; these are documented and can be found quite quickly by using search engines. The fact that an attacker who can take control of the operating system also has extensive access rights for the installed ICS software, including incoming and outgoing communication streams, is problematic.

ICS protocols as vulnerability

ICS protocols such as Modbus and Profibus were developed when security aspects were not relevant, there was no connection to the Internet, and the systems were located in physically secure places such as a power plant site. [13] Even by extending the protocols for Ethernet networks, no functionalities were implemented to protect the three security objectives of confidentiality, availability, and integrity. There is no authentication between the individual communication partners and no encryption. This makes them vulnerable to man-in-the-middle attacks and recording of traffic for replay attacks. There are efforts to set new standards to extend existing protocols by end-to-end encryption and authentication checks. Currently, additional security measures need to be taken, including restricting access and entry rights to ICS systems and associated premises, encrypting communication links using Virtual Private Networks (VPNs), and strictly isolating ICS networks from the business level through an ICS Control DMZ.

Attack Methods for ICS/SCADA

Brute forcing and standard passwords in ICS/SCADA

Passwords are used in the ICS/SCADA environment to access HMIs, workstations, servers, PLCs, and other specialized devices. Typically, users are not prompted to change the manufacturer's default passwords when setting up the devices, so this is often not done. As a result, attackers can obtain valid access data for highly sensitive systems such as the HMI from system documentation or simple search engine queries. Since older systems in particular only provide a limited character set for passwords, these phrases can be cracked within a short time by automated trying (brute-forcing) of all possible combinations. One way to defend against attacks on passwords is therefore to change the standard passwords and to orientate oneself to the password guidelines of general IT.

Social Engineering

Social engineering is the art of manipulating people with a mixture of logic and emotion to meet the attacker's demands. In many cases, a careless employee is an easier target than a secure IT environment. Possible scenarios include pretending a false identity to the IT helpdesk to reset a password or accessing server rooms with a fake technician's uniform to place infected USB sticks. Defenses against social engineering are largely interpersonal. Common methods and psychological tricks used by fraudsters can be taught in awareness programs and targeted training. This is particularly recommended for key personnel who have frequent contact with people, such as secretaries, receptionists, or IT service personnel. [7]

Phishing and Spearphishing

Phishing can be classified as social engineering, where messages are sent to many people hoping that enough individuals will fall for the scam. These can be classic scam emails with a clickable link, under which the affected person catches malware or is cheated of his credit card data. [13] Spearphishing is a more targeted form of spearphishing, in which the circle of those affected has been limited in advance. The messages are individualized with the help of collected information from public and non-public sources; this can be a fake sender with the name of an actual business partner or a subject about a target person's current project. This phishing attack has a significantly higher success rate and is a major threat, especially for executives. In addition to defenses against social engineering attacks, email filtering solutions and content filters for Web browsers can reduce phishing attacks' damage potential.

Watering Hole

Similar to spearphishing, a specific group of potential individuals is targeted. In contrast to phishing, however, a specific web page is prepared so that visitors are infected with malware. For example, this could be the website of a company's canteen, where the daily menu can be viewed. It is therefore highly probable that a call and/or download will occur from the work computer. Besides spying out the targets or a suitable web presence, a successful takeover of these is also necessary for this kind of attack. Therefore one can already speak of an advanced attack technique.

Structure and equipment of the laboratory

Description of the laboratory

Structure of the laboratory

Two virtual machines are used to simulate the engineering workstation and the hacker system. VirtualBox is used as virtualization software. The significant advantage is that this software is open source and free of charge and can be used on all current operating systems. For the hacker VM the ControlThings platform is used, the victim VM was set up with a Windows Vista 32-bit. Since this is an unpatched Windows system without an active firewall, the VM was assigned only the host-only adapter since an Internet connection is a high risk. To establish communication between the two virtual machines to fulfill the training tasks, a host-only adapter is used in VirtualBox. DHCP is enabled, i.e., the two VMs are automatically assigned their IP addresses when they connect to the lab network. The ControlThings VM has two network interfaces to install additional tools if needed and perform the tasks requiring an active Internet connection.

ControlThings platform

The ControlThings Platform is a Linux distribution that provides all standard tools for cybersecurity tasks immediately after installation. Unlike similar distributions such as Kali Linux, the focus is on ICS/SCADA. [14] A significant advantage for students is the included Reading Room, which offers a selection of helpful introductory books and documents and real network recordings with ICS protocols for practice and analysis. The latter is particularly noteworthy as it is challenging to get access to such recordings without an own lab or a real production environment.

Velocio PLC and the sample ICS process

In addition to the two VMs, a Velocio Ace 11 PLC is provided for the exercises; it has 6 digital inputs and 6 digital inputs. A simulator stick with 6 switches is used to simulate digital input signals. [15] Based on an exercise from the SANS410 course [7], a program for a simple chemical mixer was installed. If the PLC receives a power supply and switch number 1 is flipped, the program will run automatically. If switch 1 is turned off again, the process stops. A mixture of three chemicals in the mixing ratio 1:1:2 is to be produced.

A regular production process runs through the following steps:

1. The pump for chemical 1 is started and runs for 2 seconds
2. The mixer is started, chemical 2 and 3 are pumped in for 2 seconds
3. Chemical 3 is pumped in for another 2 seconds
4. The mixer runs for another 4 seconds
5. The finished mixture is pumped off for 5 seconds

If switch 6 is flipped, this will trigger the emergency stop, the contents of the mixer will be pumped out immediately for 5 seconds, the warning light will light up, and the process will be stopped until switch 6 is turned off. The 6 LEDs indicate the process on the right side of the PLC; these digital outputs could also control a real mixer. The first 3 LEDs from the left represent the 3 inlet pumps of the chemicals, the fourth the mixer, the fifth the drain pump, and the sixth the emergency condition. This process is described again in the handout, as this information is necessary for the students to complete the complex tasks and verify Velocio PLC's readiness.

The sample ICS process

A program for a simple chemical mixer was loaded into the memory of the PLC. If the PLC receives power and switch number 1 is flipped, the program will run automatically. If switch

1 is turned off again, the process stops. A mixture of three chemicals in the mixing ratio 1:1:2 is to be produced.

A regular production process runs through the following steps:

1. The pump for chemical 1 is started and runs for 2 seconds
2. The mixer is started, chemical 2 and 3 are pumped in for 2 seconds
3. Chemical 3 is pumped in for another 2 seconds
4. The mixer runs for another 4 seconds
5. The finished mixture is pumped off for 5 seconds

Figure 13. *Correct setup of the Velocio PLC (Source: own screenshot)*

If switch 6 is flipped, this will trigger the emergency stop, the contents of the mixer will be pumped out immediately for 5 seconds, the warning light will light up, and the process will be stopped until switch 6 is turned off. The 6 LEDs indicate the process on the right side of the PLC; these digital outputs could also control a real mixer. The first 3 LEDs from the left represent the 3 inlet pumps of the chemicals, the fourth the mixer, the fifth the drain pump, and the sixth the emergency condition.

Summary and Outlook

The vast amount of data that the Internet represents has excellent potential for various analyses from the world of open-source intelligence. Social networks with freely accessible private information such as Facebook and Instagram have 3.2 billion visitors daily, about 42% of the world's population. However, by far, Facebook and Instagram are not the only networks of interest for OSINT data analysis. The course created in this work gives participants a comprehensive overview of the topic of Open Source Intelligence. It allows them to work independently with the newly taught tools, collect data from freely available sources, and aggregate it into investigation results. For this purpose, the tasks were designed for several laboratory exercises.

References

[1] A. Berg and T. Haldenwang, "Bitkom: Wirtschaftsschutz in der Industrie," 13. September 2018. **https://www.bitkom.org/sites/default/files/file/import/Bitkom-PK-Wirtschaftsschutz-Industrie-13-09-2018-2.pdf** (last access February 22, 2021)

[2] N. Falliere, L. O Murchu and E. Chien, "W32.Stuxnet Dossier," Februar 2011. **https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf** (last access February 22, 2021)

[3] BSI, "Die Lage der IT-Sicherheit in Deutschland 2014," 15. Dezember 2014. **https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?blob=publicationFile** (last access February 22, 2021)

[4] BSI, "Die Lage der IT-Sicherheit in Deutschland 2018," 2018. **https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?blob=publicationFile&v=6** (last access February 22, 2021)

[5] M. Assante and R. Lee, "SANS Institute: The Industrial Control System Cyber Kill Chain," Oktober 2015. **https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297** (last access February 22, 2021)

[6] NIST, "National Institute of Standards and Technology Special Publication 800-82r2 Guide to Industrial Control System (ICS) Security," Mai 2015. **https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf** (last access February 22, 2021)

[7] J. Searle, "Kurs: SANS ICS410: ICS/SCADA Security Essentials," SANS, 2018

[8] E. Knapp, "Industrial Network Security - Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems", Syngress, 2011, ISBN: 978-1-59749-645-2

[9] P. Ackerman, "Industrial Cybersecurity - Efficiently secure critical infrastructure systems", Packt Publishing, 2017, ISBN: 978-1-78839-515-1

[10] DHS, "Department of Homeland Security Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies," September 2016. **https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf** (last access February 22, 2021)

[11] T. Wiens, "S7 Communication (S7comm)," 13. Mai 2016. **https://wiki.wireshark.org/S7comm** (last access February 22, 2021)

[12] EU, "Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern," 08 Dezember 2008. **https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32008L0114** (last access February 22, 2021)

[13] K. Fowler, "Data Breach Preparation and Response: Breaches are Certain, Impact is Not", Syngress, 2016, ISBN: 978-0-12-803451-4

[14] C. Bodungen, B. Singer and e. al, "Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions", McGraw-Hill Education, 2017, ISBN: 978-1-25-958972-0 (E-Book)

[15] J. Searle, "ControlThings I/O," **https://www.controlthings.io/home** (last access February 22, 2021)

[16] Velocio, "Produktbeschreibung: Velocio Ace PLC," **http:**

//velocio.net/ace/ (last access February 22, 2021)

[17] E. Hutchins, M. Cloppert and R. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chain," **https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf** (last access February 22, 2021)

[18] eLearn-Security, "Kurs: PTPv5 Penetration Testing Professional," 2018

[19] Nmap-Community, "Nmap Overview and Introduction," **https://nmap.org/** (last access February 22, 2021)

[20] Maltego, "Maltego CE," **https://www.paterva.com/buy/maltego-clients/maltego-ce.php** (last access February 22, 2021)

[21] Shodan, "What is Shodan?" **https://help.shodan.io/the-basics/what-is-shodan** (last access February 22, 2021)

[22] J. Long, "The Google Hacker's Guide: Understanding and Defending Against the Google Hacker," **http://pdf.textfiles.com/security/googlehackers.pdf** (last access February 22, 2021)

[23] OTW, "SCADA Hacking: Finding Vulnerable SCADA Systems using Google Hacking," (September 08, 2019). **https://www.hackers-arise.com/single-post/2016/07/05/SCADA-Hacking-Finding-Vulnerable-SCADA-Systems-using-Google-Hacking** (last access February 22, 2021)

[24] GoogleGuide, "Search Operators," **http://www.googleguide.com/advanced_operators_reference.html** (last access February 22, 2021)

[25] C. Martorella, "Github Page: theHarvester," **https://github.com/laramies/theHarvester** (last access February 22, 2021)

[26] Wireshark, "About Wireshark," **https://www.wireshark.org** (last access February 22, 2021)

[27] NSA, "National Security Agency: GRASSMARLIN User Guide Version 3.2," **https://github.com/iadgov/GRASSMARLIN/raw/master/GRASSMARLIN%20User%20Guide.pdf** (last access February 22, 2021)

[28] Rapid7, "Metasploit - Getting Started," **https://metasploit.help.rapid7.com/docs** (last access February 22, 2021)

[29] D. Kennedy, J. O'Gorman, D. Kearns and M. Aharoni, "Metasploit: The Penetration Tester's Guide", No Starch Press, 2011, ISBN: 978-1-59327-288-3

[30] A. Peslyak, "John the Ripper password cracker," **https://www.openwall.com/john/** (last access February 22, 2021)

[31] "Simpsons Meme," **https://imgur.com/a/WSFVBma** (last access February 22, 2021)

[32] NIST, "National Institute of Standards and Technology Special Publication 800-61r2: Computer Security Incident Handling Guide," August 2012. **https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf** (last access February 22, 2021)

[33] R. Lee, "Kurs: SANS ICS515: ICS Active Defense and Incident Response," SANS, 2018

[34] Mandiant, "M-Trends 2015: A View from the Frontlines," 2015. **https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf** (last access February 22, 2021)

[35] FireEye, "M-Trends 2019: FireEye Mandiant Services Special Report," 2019. **https://content.fireeye.com/m-trends** (last access February 22, 2021)

[36] K. A. Monnappa, "Learning Malware Analysis - Explore the concepts, tools, and techniques to analyze and investigate Windows malware", Packt Publishing, 2018, ISBN: 978-1-78839-250-1.

[37] VirusTotal, "How it works," **https://support.virustotal.com/hc/en-us/articles/115002126889-How-it-works** (last access February 22, 2021)

[38] Any.RUN, "What is ANY.RUN," **https://app.any.run/docs/** (last access February 22, 2021)

[39] B. Filkins and D. Wylie, "SANS 2019 State of OT/ICS Cybersecurity Survey," Juni 2019. **https://radiflow.com/wp-content/uploads/2019/06/Survey_ICS-2019_Radiflow.pdf** (last access February 22, 2021)

[40] BSI, "Industrial Control System Security - Top 10 Bedrohungen und Gegenmaßnahmen 2019," 01 Januar 2019. **https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005.pdf?blob=publicationFile** (last access February 22, 2021)

[41] P. Kobes, Leitfaden Industrial Security - IEC 62443 einfach erklärt, VDE Verlag GmbH, 2016, ISBN: 978-3-8007-4166-3 (E-Book)

[42] J. Luttgens and M. Pepe, Incident Response & Computer Forensics, Third Edition, McGraw-Hill Education, 2014, ISBN: 978-0-07-179868-6

[43] OTW, "SCADA Hacking: Finding SCADA Systems using Shodan," 30. Juni 2016. **https://www.hackers-arise.com/single-post/2016/06/30/Hacking-SCADA-Finding-SCADA-Systems-using-Shodan**. (last access February 22, 2021)

[44] A. Soullie and A. Torrents, "Brucon 0x07 ICS Workshop: Pentesting ICS 101", Oktober 2015.

[45] D. Vukadinovic, "Was ist der Unterschied zwischen HTTP und HTTPS?," 26. Juni 2018. **https://www.globalsign.com/de-de/blog/unterschied-zwischen-http-und-https/** (last access February 22, 2021)

[46] "Stock Image einer HMI". **http://www.infind.com.ar/data/servicios/Automation.jpg** (last access February 22, 2021)

[47] Schwarz, Klaus; Franziska Schwarz, Reiner Creutzburg: "Conception and implementation of professional laboratory exercises in the field of open source intelligence (OSINT)". Proceed. Electronic Imaging Symposium 2020 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms & Applications Conference (MOBMU) 2020, **https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-278**

[48] Schwarz, Klaus; Reiner Creutzburg: "Design of Professional Laboratory Exercises for Effective State-of-the-Art OSINT Investigation Tools - Part 1: RiskIQ PassiveTotal". Proceed. Electronic Imaging Symposium 2021 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms & Applications Conference (MOBMU) 2021 (in print)

[49] Schwarz, Klaus; Reiner Creutzburg: "Design of Professional Laboratory Exercises for Effective State-of-the-Art OSINT Investigation Tools - Part 2: Censys". Proceed. Electronic Imaging Symposium 2021 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms & Applications Conference (MOBMU) 2021 (in print)

[50] Schwarz, Klaus; Reiner Creutzburg: "Design of Professional Laboratory Exercises for Effective State-of-the-Art OSINT Investigation Tools - Part 3: Maltego". Proceed. Electronic Imaging Symposium 2021 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms & Applications Conference (MOBMU) 2021 (in print)

[51] Schwarz, Klaus; Reiner Creutzburg: "Design of Professional Laboratory Exercises for Effective State-of-the-Art OSINT Investigation Tools - Part 3: Maltego". Proceed. Electronic Imaging Symposium 2021 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms & Applications Conference (MOBMU) 2021 (in print)

[52] Schwarz, Klaus: "Conception and Implementation of Professional Laboratory Exercises in the Field of Open Source Intelligence (OSINT) for use in English and German Training Market for Security Authorities". Master Thesis, Technische Hochschule Brandenburg, Department of Computing and Media, April 2020

[53] Kant, Daniel; Reiner Creutzburg: 'Investigation of risks for Critical Infrastructures due to the exposure of SCADA systems and industrial controls on the Internet based on the search engine Shodan". Proceed. Electronic Imaging Symposium 2020 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms & Applications Conference (MOBMU) 2020 **https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-253**

[54] Pilgermann, Michael; Thomas Bocklisch; Reiner Creutzburg: "Conception and implementation of a course for professional training and education in the field of IoT and smart home security". Proceed. Electronic Imaging Symposium 2020 (San Francisco, USA), Mobile Devices and Multimedia: Technologies, Algorithms & Applications Conference (MOBMU) 2020 **https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-277**

Author Biography

Maximilian Richter received his M.Sc. degree in Computer Science from Technische Hochschule Brandenburg (Germany) in 2020. His research interests include IIoT/OT Security, Active Defense, Threat Intelligence and Cyber War. He currently works as a SOC Analyst in the financial sector.

Klaus Schwarz received his B. Sc. and M.Sc. in Computer Science from Technische Hochschule Brandenburg (Germany) in 2017 and 2020, respectively. His research interests include IoT and Smart Home Security, OSINT, Mechatronics, Sensorics, Embedded Systems, Artificial Intelligence, and Cloud Security. As a faculty member, he is developing a graduate program in Applied Mechatronic Systems focusing on Artificial Intelligence at SRH Berlin University of Applied Sciences.

Reiner Creutzburg is a Retired Professor for Applied Computer Science at the Technische Hochschule Brandenburg in Brandenburg, Germany. Since 2019 he is a Professor of IT Security at the SRH Berlin University of Applied Sciences, Berlin School of Technology. He is a member of the IEEE and SPIE and chairman of the Multimedia on Mobile Devices (MOBMU) Conference at the Electronic Imaging conferences since 2005. In 2019, he was elected a member of the Leibniz Society of Sciences to Berlin e.V. His research interest is focused on Cybersecurity, Digital Forensics, Open Source Intelligence (OSINT), Multimedia Signal Processing, eLearning, Parallel Memory Architectures, and Modern Digital Media and Imaging Applications.

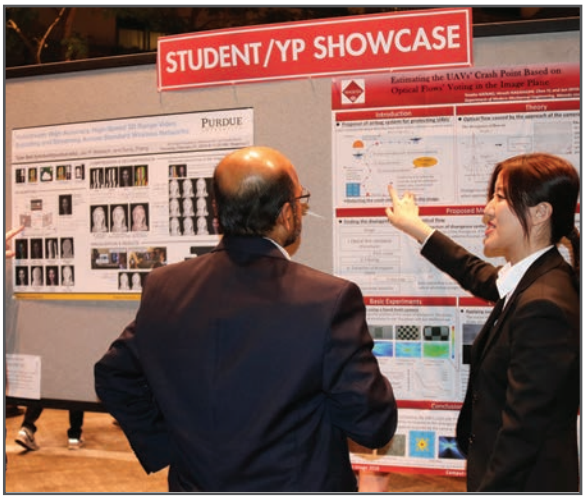
JOIN US AT THE NEXT EI!

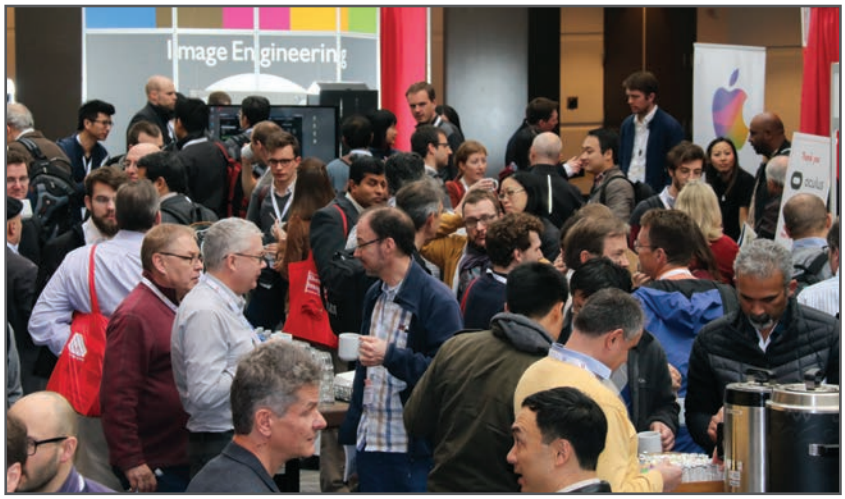
IS&T International Symposium on

Electronic Imaging

SCIENCE AND TECHNOLOGY

Imaging across applications . . . Where industry and academia meet!





• SHORT COURSES • EXHIBITS • DEMONSTRATION SESSION • PLENARY TALKS •
• INTERACTIVE PAPER SESSION • SPECIAL EVENTS • TECHNICAL SESSIONS •

www.electronicimaging.org

IS&T
imaging.org