https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-253

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

Daniel Kant [1]***, Reiner Creutzburg*** [2]***, Andreas Johannsen*** [1]

[1] ***Technische Hochschule Brandenburg, Department of Business and Management, Magdeburger Str. 50, D-14770 Brandenburg, Germany***

[2] ***Technische Hochschule Brandenburg, Department of Informatics and Media, IT- and Media Forensics Lab, Magdeburger Str. 50, D-14770 Brandenburg, Germany***

Email: kantd@th-brandenburg.de, creutzburg@th-brandenburg.de, johannse@th-brandenburg.de

Abstract

Industrial Control Systems occur in automation processes and process control procedures within Critical Infrastructures (CI) - these are institutions with important significance for the common good of the state and thus for the maintenance of a society. Failures or disturbances in industrial plants can have serious physical consequences, such as power outages or interruptions in production. Energy suppliers, in particular, are an attractive target for cyber attacks due to their interdependencies with other infrastructures. A large number of SCADA systems and Industrial Control Systems are directly connected to the Internet and inadequately secured from an information technology perspective, this represents a considerable risk for IT security and, consequently, for the availability of Critical Infrastructures. The Shodan search engine reveals a worrying extent of exposed industrial control equipment on the Internet. The collected information and metadata about Industrial Control Systems from this search are freely available online. They can serve as a basis for potential attacks. Without authentication mechanisms, anyone can connect to open ports using industrial and remote maintenance protocols. The resulting risks and consequences for the companies, operators as well as for the society due the exposure of industrial plants and Critical Infrastructures are examined based on the Shodan search engine within the scope of this work.

Keywords

Industrial Control Systems; ICS; Critical Infrastructure; Energy supply; Shodan; Human Machine Interface; Industrial Protocols; Remote Control Protocols; Remote Maintenance Protocols

Introduction

Critical Infrastructures (*abbrev.:* CI) are institutions with important significance for the common good of a state - e.g. energy suppliers, telecommunications infrastructures, hospitals, or banks - and thus for the maintenance of a society [13]. An IT attack on Critical Infrastructures can lead to massive impairments within the social coexistence. Industrial Control Systems (*abbrev.:* ICS) are used within Critical Infrastructures, especially for automation processes. These ICS have become a potential and lucrative target for cyber attackers in the last decades. Today only a computer and an internet connection is needed for successfully initializing a cyber attack. Even expert knowledge is no longer necessary because there is a global criminal market for tools with which even a non-specialist can successfully launch an attack. The nuclear accident at Chernobyl (1986) warns that Industrial Control Systems can cause a significant and immediate threat to the physical safety of the population. The dependence of modern societies on Critical Infrastructures is rising continuously [16]. As a result, their vulnerability also increases. In December 2015, a coordinated cyber attack occurred in Ukraine to a local energy operator, which resulted in massive power outages from which approximately 225,000 people were directly affected. Unlike conventional search engines, which usually contain websites, the search engine Shodan can be used to search for devices and servers that are directly connected to the Internet [17]. Through an online article of *CNN Money* [10] [11], the search engine Shodan came into the public focus for the first time in 2013 and revealed a significant exposure of Industrial Control Systems and SCADA systems on the Internet and their serious security vulnerabilities [21].

Industrial Control Systems (ICS)

Industrial Control Systems (*abbrev.*: ICS) are a class of automation systems that fully or partially automate control and monitoring processes in production and industrial facilities [1] - from chemical plants to power generation and distribution including gas and water supply. They are an integral part of Critical Infrastructures [2] [36]. These industrial control components are an attractive target for potential cyber attackers because they can directly handle physical processes and thus cause serious damage in the real world [39]. The controllers exhibit a high degree of complexity, consisting of thousands of components, which are distributed geographically across different locations and must also meet real-time requirements [1]. Industrial controls also place high demands on physical security [6]. Conventional hardware and software fault detection in industrial plants are appropriate for counteracting random errors or design errors. However, they are not suitable for preventing malicious errors (e.g. caused by an IT or cyber attacks). The physical security of the systems corre-

lates with cyber security, meaning, cyber security flaws can result in physical damage [6].

SCADA

Through SCADA (*Supervisory Control And Data Acquisition)*, technical processes are controlled, monitored, and visualized. An essential advantage of SCADA systems is the central monitoring of processes. SCADA systems thus differ historically from process control systems, which are commonly used more locally within a facility (e.g., inside a factory) [8].These strict terminologies tend to become increasingly blurred so that today, both terminologies are combined in the uniform generic term *Industrial Control Systems* [8]. Since the mid-1990s there has been an increasing convergence and integration between the original industrial technology (also called *operational technology* (OT) [1]) - which directly controls or monitors the physical terminals - and the conventional *information technology* (IT) [26] [8]. SCADA systems can manage highly geographically distributed locations of several thousand square kilometers [5]. For large geographical distances WAN connections (Wide Area Network) are used (Figure 1). The systems are designed for availability and reliability, i.e., they are suitable for industrial real-time applications. Since SCADA systems communicate over long geographical distances, they were designed to avoid or compensate delays and data loss in transmission [5]. Because locations are geographically distributed, and low latencies must be guaranteed, SCADA systems are also designed for performance. The communication latency of such a management system is lower than if malfunctions would have to be reported manually to a central site. This ensures real-time intervention in critical situations. From an economic point of view, SCADA systems are profitable in acquisition and maintenance [8], because fewer employees are required to control the local field devices (this reduces personnel costs), as well as today only standard hardware is required for the maintenance. A further advantage is a versatility: The systems were designed with the aim of optimally supporting a heterogeneous environment (different devices, interfaces, and industrial protocols). This means that terminal devices such as Programmable Logic Controllers from any manufacturer can be easily integrated. The control of SCADA systems can be held completely automated or taken over by operators [8]. Today's SCADA systems have a modular design: Individual modules can be deactivated, shut down, or updated without limiting the availability of the overall system [8]. However, such functionality is more likely to be found in modern systems. Many older SCADA systems have been in operation for decades and have no modularity or do not experience a continuous update process.

Programmable Logic Controller (PLC)

Programmable Logic Controllers (*abbrev.:* PLC) are required in Industrial Control Systems as control elements for field devices. PLCs act self-correcting on a physical process [5] e.g. in a hydropower plant they are needed to physically open valves or control pumps to regulate the water flow. Programmable Logic Controllers manage discrete processes in real-time to ensure both availability and reliability requirements. They are internationally programmed according to the *IEC 61131* standard [38], which includes a simple logic (*ladder logic*). This guarantees efficient processing and thus leads to low latencies, which has a positive effect on compliance with real-time requirements. Ladder logic is the predominant method for programming and controlling industrial processes in general (and thus also for PLCs) [4]. The whole logic can be seen as a decision tree, which is traversed deterministically - depending on whether conditions are fulfilled or not (if-then-else). The processing of instructions is strictly sequential. The program logic is applied to the discrete inputs and outputs connected to the PLC. The analog signal at the sensors is converted to a discrete value, which is compared to a set point (for example, minimum or maximum level in a water tank). Based on the state of the concrete inputs, the appropriate interaction is performed at the outputs (e.g., throttle motor). Programmable controllers can use a variety of analog and digital communication methods, usually, they use field bus protocols to communicate [2]. PLCs include a central processing unit (CPU), a power supply, input and output interfaces, as well as an operating system (mostly the firmware) and the actual user program (including all set points and thresholds). Unlike conventional desktop systems, PLCs react automatically to inputs - e.g., in the form of sensors [2]. The actual program logic is executed cyclically: The time dimension for reading inputs, processing them, and initiating outputs are to be classified in the millisecond range [1]. Besides, PLCs can have expansion shafts or modules to enable external connectivity. This allows communication via interfaces, common network protocols, industrial protocols, communication standards, and network devices [4]. PLCs are a lucrative cyber security target because they are directly connected to input and output interfaces and support both common network standards (such as Ethernet) and industrial protocols [4]. Programmable Logic Controllers are widely used in all industrial processes [5].

Remote Terminal Unit (RTU)

Remote Terminal Units (*abbrev.:* RTU) are utilized within Industrial Control Systems to read data from field devices in the form of sensors, which are then transmitted to higher-level SCADA systems for automated processing. In addition to PLCs, RTUs are the second common type of control units for industrial plants that can control field devices. RTUs contain of a power supply, a CPU, as well as analog and digital input and output modules. Remote Terminal Units are usually connected to the higher-level Master Terminal Unit via a modem, a mobile phone connection, or a WAN connection. RTUs are commonly used outdoors. Therefore, they must withstand adverse environmental and weather conditions (e.g., such as high or low temperatures, humidity, rain, snow, thunderstorms or animals). The units do not have a high data throughput. Accordingly, they use mechanisms like *report by exception*, which only transmit values that have changed. There is a tendency that the functionalities of PLCs and RTUs overlap more and more and even flow into each other - a clear separation is not always given [2].

Human Machine Interface (HMI)

Using the Human Machine Interface (*abbrev.: HMI*), operators are able to communicate with PLCs and RTUs. Thus their processes and states are both controlled and monitored (Figure 2) [2]. Individual processes can be controlled or stopped by entering commands via keyboards, touch screens, or operator panels. The HMI is a lucrative target for attackers because processes can be directly influenced by taking over the control panel (e.g., via

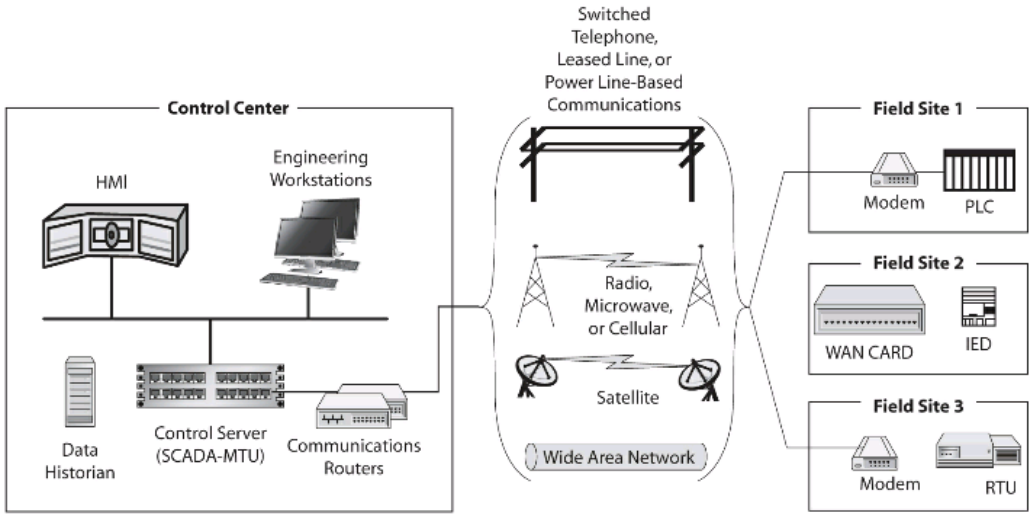


Figure 1. *Common SCADA network topology [5]*

remote maintenance protocols like RDP or VNC), what can be considered as a critical incident [26].

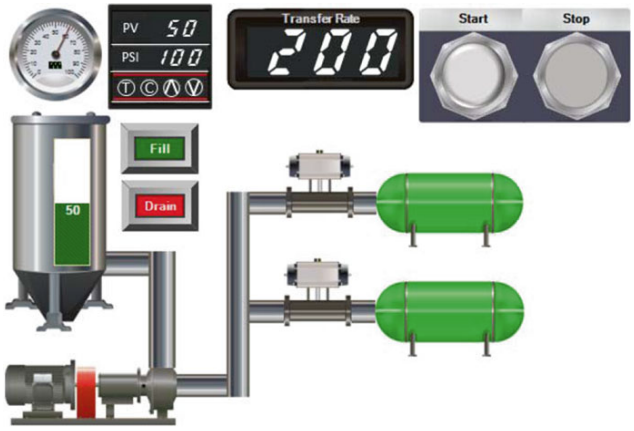


Figure 2. *Common HMI Control interface [1]*

Field Devices

Field Devices can be considered as the interface for the interaction with the physical world. The term refers to control and reading devices such as sensors, converters, actuators, and any machines which are directly connected to the control units (e.g., PLC or RTU) via an interface sending analog or digitally processed signals. Field Devices usually use industrial protocols such as Modbus or PROFIBUS to communicate with the controllers. Sensors measure temperature, humidity, pressure, volume, vibration, voltage, or current as well as other physically measurable quantities and can trigger alarms and alerts [5]. Actuators interact with their environment in the form of valves, motors, pumps, turbines, frequency converters, combustion engines, or compressors [1].

Industrial Network Protocols

Industrial network protocols can be divided into two categories: fieldbus protocols and backend protocols [2]. The fieldbus protocols such as *Modbus-TCP*, *EtherNet/IP* or *DNP3* are required to connect field devices with control units (e.g. PLCs). Backend protocols are particularly needed to connect several industrial plants or control centers directly with each other. Industrial protocols developed from originally proprietary protocols to compatibility with common network protocols and standards such as the Internet Protocol (IP) or Ethernet [2]. The protocols themselves are designed for efficiency and reliability [2]. This is why many protocols use checksums, but this provides inadequate protection against cyber attacks [1]. With regard to reliability, industrial protocols have to meet hard real-time requirements (also concerning the monitoring of ICS in real-time) [2]. Because the protocols are also designed towards efficiency, all further functions or features are omitted or neglected in order to ensure the lowest possible protocol header [2]. However, the protocols were designed without security mechanisms such as authentication or encryption because the equipment was originally operating in isolated areas [5]. These inherently missing security mechanisms of most common protocols represent a significant IT security risk [4] i.e. Industrial Network Protocols can be abused as a possible attack vector within an industrial environment. Therefore it is necessary to know the exact header and mechanisms of the individual protocols and how they can be exploited for a potential cyber attack [2]. Examples of common industrial network protocols are Modbus, DNP3, PROFIBUS, PROFINET, EtherNet/IP, EtherCAT, Powerlink, Sercos, OPC, DCOM, ICCP, and AMI [2].

Modicon Communication Bus (Modbus)

Modicon Communication Bus (*abbrev.:* Modbus) is the most widely used of all industrial protocols, especially because it is an open standard, simple and robust [2] [4]. The Modbus protocol was originally developed by the company *Modicon* (today *Schneider Electric*) and was developed in the late 1970s as a serial protocol to communicate with Programmable Logic Controllers [4]. Today Modbus is used in higher-level monitoring

systems such as SCADA. Since the protocol was introduced, it has been adapted several times to ensure compatibility with common communication standards such as Ethernet [4]. Therefore, the serial Modbus protocol was encapsulated in a TCP header. Modbus can be regarded as a Layer-7 protocol in the OSI reference model [2]. Modbus uses a client/server architecture, i.e., communication takes place via request and response. The protocol also takes advantage of a master and slave architecture: Using Modbus, a master (e.g., a computer) can connect to several slaves in order to control them. Today there are different variants of Modbus: *Modbus-RTU*, *Modbus-ASCII* and *Modbus-TCP* [2]. *Modbus-TCP* is very similar to *Modbus-RTU*. However, TCP/IP packets are used to transmit the data. Unlike *Modbus-RTU* there is no error checking at the end of the header. Since 2007 the version *Modbus-TCP* is part of the standard *IEC 61158*. The TCP port 502 is reserved for *Modbus-TCP* [22]. The Modbus protocol is extremely lucrative for attackers [2] due to its high distribution and inadequate IT security mechanisms (e.g., missing authentication).

Automation Control Process

In order to automatically control physical processes (e.g., water heating), inputs and processing steps are run through cyclically in the form of control loops [2]. One possibility of this cyclic processing is the ladder logic as used in PLCs. The inputs are read in at regular intervals. Then these inputs are compared with thresholds, and it is decided if required changes have to be made to the output. [2]. In a closed control loop, the outputs influence the inputs again. For instance, a liquid heater warms water to 90^o C (setpoint). The temperature is permanently measured at the input. When the corresponding temperature is reached, the heating coil is deactivated [2]. Industrial Control Systems usually have multiple control loops, which even depend on each other. The change of a process variable within a cyclic control loop leads to a change of another industrial control process [5] and consequently to a change of the overall system. Therefore, the consequences of IT attacks on industrial plants are less predictable than those on conventional IT systems and require comprehensive knowledge of the functioning of the plants [9]. Also, the operators use a special combination of industrial hardware and suppliers - this makes the overall control process unique for each company and environment. Figure 3 shows the usual control process for industrial plants.

Industrial Network Design

From a network design point of view, the process control network (PCN) is increasingly being mixed with the conventional IT company network [2]. Many networks have grown historically: the once isolated industrial plants are connected to the Internet for remote maintenance purposes without a clear separation of the process control network from the corporate network. If such segmentation (no Demilitarized Zone, firewalls, and zone segregation) does not exist, even industrial terminals can be an attack vector to successfully compromise the corporate network and vice versa . There is no generic network design, especially regarding the segmentation into zones or the degree of abstraction. The concrete network plan for both (the process control network and the IT company network) is unique in every company or facility.

IT Properties of ICS

Traditionally, industrial controls have been designed for reliability and physical security [12] [6]. The focus is, therefore, different from traditional IT systems, which are oriented towards confidentiality, availability, and integrity [6]. This inadequate consideration of IT security aspects is immanent in the architecture of these systems [5]. However, industrial networks are maintained and operated by engineers - less by IT security specialists. Therefore, the systems are often inadequately configured [4]. Conventional IT security solutions cannot be adopted one-to-one for the ICS context [6]. Instead, the solutions must be tailor-made for the respective environment [5]. Industrial Control Systems were isolated systems for a long time and only vulnerable to local threats because they were only used in physically secured environments. Individual components were not connected to IT systems or networks [5] and had no connectivity to other domains [1]. This circumstance did not require robust protocols (such as, e.g., cyclic redundancy checking of packets) or cryptographic mechanisms [1]. In addition to proprietary control protocols, specialized hardware and software were used [5], which could only be operated by specialists [1]. Extensive information on industrial controls is nowadays freely available on the Internet [1]. Also - from an economic point of view - there was a necessity to save costs. Therefore information had to be collected centrally, and processes had to be monitored, evaluated, and optimized. This required new technologies: The first generation of SCADA systems was born. In order not to lose competitiveness in the age of *Industry 4.0*, value chains in companies are digitized, virtualized, networked, and controlled in real-time. The machines themselves, the sensors and field devices in the production plants, ERP systems as well as marketing, sales, and purchasing areas are now interconnected. As a direct consequence of the advancing digitization and networking, this extension beyond external borders creates new points of attacks. The primary objective is to avoid the failure or impairment of production and business processes. Remote maintenance and progressive integration into management systems, as well as the use of conventional hardware, standard protocols, and widespread operating systems (such as Windows or Unix [1]) led to the fact that ICS were increasingly adapted to conventional IT systems [5] [7]. The integration and adaptation of these formerly isolated systems offer many advantages in management but increases the risk of IT security incidents and, consequently, the need to adequately secure these assets - especially against external threats [5]. Ethernet became more and more accepted as a communication standard. With the spread of the Internet Protocol (IP), previously used manufacturer-specific and proprietary protocols (e.g., DeviceNet) were partially or completely replaced [4], which also led to an increase of IT security incidents [5].

Remote Maintenance

In the past, companies had to hire maintenance technicians for maintenance work on the systems, machines, and equipment, so that they could then solve the respective problems locally. The maintenance process today takes place via remote maintenance on the Internet using insecure, unencrypted protocols (e.g., Telnet) or proprietary protocols [7], which facilitate network sniffing and successfully analyzing the captured network traffic. The architecture of most facilities is not designed to interact with the Internet. Especially for older ICS applications, industrial proto-

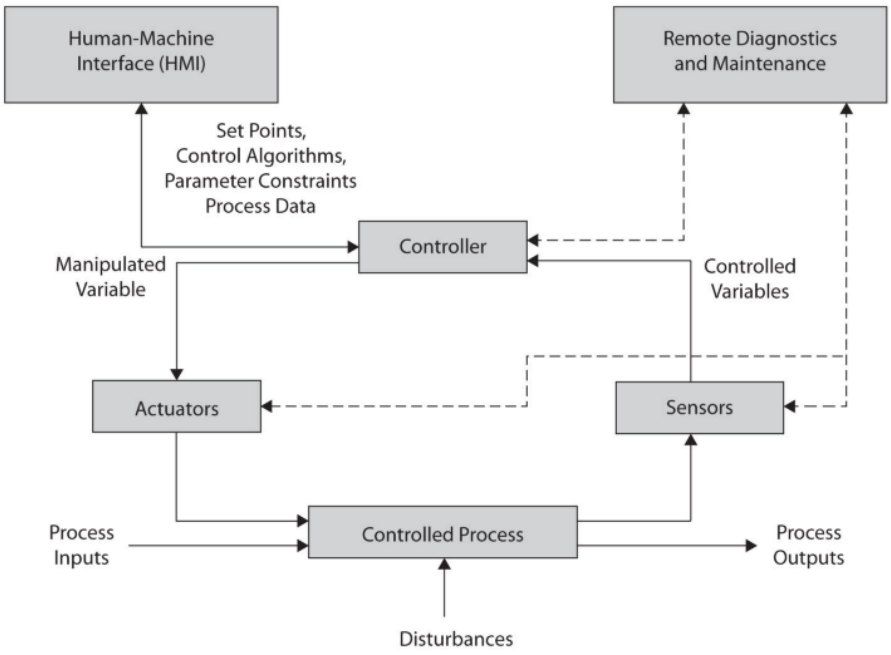


Figure 3. *Automation Control Process for industrial control systems [4] (according to NIST SP 800-82 [5])*

cols, and remote maintenance protocols, no authentication methods have been implemented [4]. Furthermore, access controls for remote maintenance are predominantly role-based and not user-based, i.e., a privileged user account is used for all operators. Unlike conventional IT systems, industrial control requires high demands on availability and, consequently, on the quality of communication: jitter or packet loss are not tolerable [5]. The systems also place high demands on performance as well to meet real-time requirements [5]. The use of cryptography in industrial plants, therefore, leads to latencies and endangers the adherence to hard real-time (i.e., the encryption of communication is thus not activated). Besides, there is a susceptible or faulty implementation of cryptographic protocols and poorly preconfigured software on the part of the manufacturers. The manufacturer delivers a standard configuration that should be usable by as many customers as possible. As a result, the software is not individually adapted to the respective customer environment - security-critical services and ports are unnecessarily activated. Additionally, standard passwords are used, which are not changed temporarily or at all [43]. Also, hard-coded backdoor management is built into devices without the possibility of disabling these persistently installed backdoor accounts [47]. Furthermore, industrial plants are challenging to maintain, scale, and change [5]. Moreover, these systems do not have a modular structure - they consist of several depending components that cannot be replaced individually.

Update Process

Originally designed and commissioned once, the systems - unlike conventional IT systems - do not experience a cyclic update process. IT security is a continuous process that makes updates mandatory. The planned maintenance intervals of some operators (e.g., once a year or once every two years) are insufficient. Additionally, there are inflexible maintenance contracts and high installation costs in the event of a change of provider or a new acquisition [37]. The availability of the plants must be guaranteed permanently: A downtime is unacceptable in the ICS context and leads to significant financial losses (especially when production systems are involved, and high availability requirements are violated). Since the systems are part of critical processes, updating the software of real-time systems can be challenging. Industrial plants have an enormous runtime. In order to avoid severe errors in case of an update - which can significantly limit the availability - the use of obsolete operating systems is widely accepted [42]. Thus outdated operating systems are no longer supported. Critical operating system updates do not exist, which represents another attack vector. As a result, many unpatched and insecure Windows systems are used (including SCADA controls) [40] [41]. There are thousands of vulnerabilities and exploits for obsolete and/or unpatched Windows systems [4]. For the National Institute of Standards and Technology (NIST), unpatched software applications are one of the main *vulnerabilities* for industrial control systems [5]. Furthermore, wireless connections are an increasing threat to industrial equipment [5]. This trend will continue to increase in the context of the Industrial Internet of Things (IIoT) [6].

ICS Attack vectors

The inadequate protection of industrial control systems represents an enormous problem for the operators of critical infrastructures, as these controls are used in almost all infrastructures. The systems are not sufficiently protected against cyber attacks by their architecture. Operator companies usually have multiple connections to the Internet - mostly for remote maintenance reasons. Vulnerabilities are another entry point for successful attacks on industrial controllers. The following attack vectors can be regarded as high threats for the ICS context [39] [5] [1]:

- Malware susceptibility
- Usage of insecure maintenance protocols
- Missing authentication or cryptographic mechanisms
- Usage of outdated operating systems and firmware
- Flawed or inappropriate configuration of ICS
- Vulnerable software applications
- Vulnerable network devices such as routers or firewalls
- Missing IT guidelines
- Usage of default/factory or weak passwords
- Usage of vulnerable web interfaces and web applications

Critical Infrastructures (CI)

The term critical infrastructure (*abbrev.:* CI), which originates from NATO usage, refers to facilities, installations, or parts that belong to the energy, information technology, and telecommunications, transport, health, water, food, finance, and insurance sectors. They are of high importance for the functioning of society because their failure or impairment would result in significant supply shortages or threats to public safety. CI is exposed to a multitude of threats, which must be fully taken into account for the prevention of incidents, from physical causes such as natural disasters and threats based on information technology (cyber attacks) to anthropogenic causes such as human errors.

Interdependency and Criticality

A distinction can be made between systemic criticality and symbolic criticality. Infrastructures are related to systemic criticality if they are because of their structural, functional, and technical positioning in the overall system [...] of particularly high interdependent relevance. This means that failures in one infrastructure sector can lead to further failures in other sectors. The energy sector, for example, is of outstanding systemic criticality due to its interdependencies with other infrastructures (Figure 4). A power supply is a prerequisite for the provision of all other critical services. Therefore, in the event of serious failures, *"domino effects"* could lead to further failures for other infrastructure areas. A dependency between two infrastructures is a unidirectional relationship, where the infrastructure *i* is dependent on infrastructure *j* using one connection, whereas *j* is not dependent on *i* using the same connection. An interdependence, on the other hand, is a bidirectional relationship in which *j* is dependent on *i* using the same connection [15]. These mutual relations between the infrastructure sectors are to be evaluated as particularly serious: The failure of a sector and/or an infrastructure leads to the failure of another infrastructure, whose operability, however, requires the trouble-free functioning of the first collapsed infrastructure. This so-called "*cascade effect*" can be expected especially in the sectors *information technology and telecommunications* as well as in the *energy sector* [14]. Due to their networking size and strength, a large-scale and long-lasting failure can lead to serious disturbances in social processes and public safety. Another infrastructure sector with systemic criticality is the *transport and traffic* sector, which guarantees the logistics of all infrastructure sectors, as well as the supply of the population. A failure of this supply would have catastrophic consequences for the life or health of the population. An infrastructure possesses symbolic criticality if the institution has a "*cultural*" or "*identity-giving meaning*" and can thus destabilize and unsettle a society emotionally (e.g., destruction of architectural buildings).

Vulnerability

In the context of critical infrastructures a *vulnerability* is understood as an error or a weak point in the design, in the implementation, in operation, but also in the management of an infrastructure system or one of its elements [44]. If the infrastructure is exposed to a danger or a threat, this vulnerability makes the infrastructure system susceptible to an inability to work properly or even to destruction and consequently leads to the reduction of stability of the overall system [44]. Depending on the severity of the vulnerability, a system is less resilient, which can lead to cascading effects. By *resilience* the ability of infrastructure is understood to resist an exposed danger or to limit the effects of an incident [44]. The dependence of modern societies on Critical Infrastructures is continuously increasing [16]. Thus also, the vulnerability of modern societies grows.

Shodan search engine

Launched in 2009, Shodan is a search engine that specifically lists those devices that are directly connected to the Internet. This can be a server, a router, or any IP-enabled device. The search engine received broader media attention for the first time in 2013 by an online article of the information platform *CNN Money*, which reported that it succeeded in gaining mass access to traffic control systems as well as other control and service systems in the United States through Shodan [10] [11]. The search engine works similar to *Google*, with the difference that the so-called "*Shodan-Crawlers*" do not only search web pages but also record all accessible servers and their services in order to index them. Shodan uses scanners distributed around the world [25] and searches all IPv4 addresses on the Internet for "*well-known-ports*" used by popular services, and then automatically connects to these services or ports. Servers automatically send data to the users, when a connection to the server is initialized. This connection data ("*Banner*") can contain valuable information and is automatically stored by Shodan in a database. For a web server, this is the *header information* (HTTP version, the character set used, etc.), for Telnet even the complete login screen is saved, which can contain useful information such as the default password (or user) for the device or the name of the corresponding company. The information may vary depending on which services the devices actually provide: A Siemens ICS device based on the *S7 protocol*, for example, reveals different header information than the previously mentioned web server, such as *firmware-version*, *moduletype*, *module-description* or *serialnummer*. In addition to the banner data, metadata are also collected about the specific devices from which further information can be obtained, such as used operating system, active services, versioning, DNS hostnames, geographic information based on the IP address, GPS coordinates, protocols or open ports, and much more. [17]. This collected data is the basis on which potential attackers can try to gain unauthorized access to the systems. Since 2012 Shodan reveals the enormous extent of the exposure of Industrial Control Systems on the Internet as well as their serious security gaps [27]. The search engine has a separate subcategory for industrial control systems on its website[1]. A distinction can be made between the two different methods of interacting with industrial control

[1] `https://www.shodan.io/explore/category/industrial-control-systems` - retrieved: April 2019

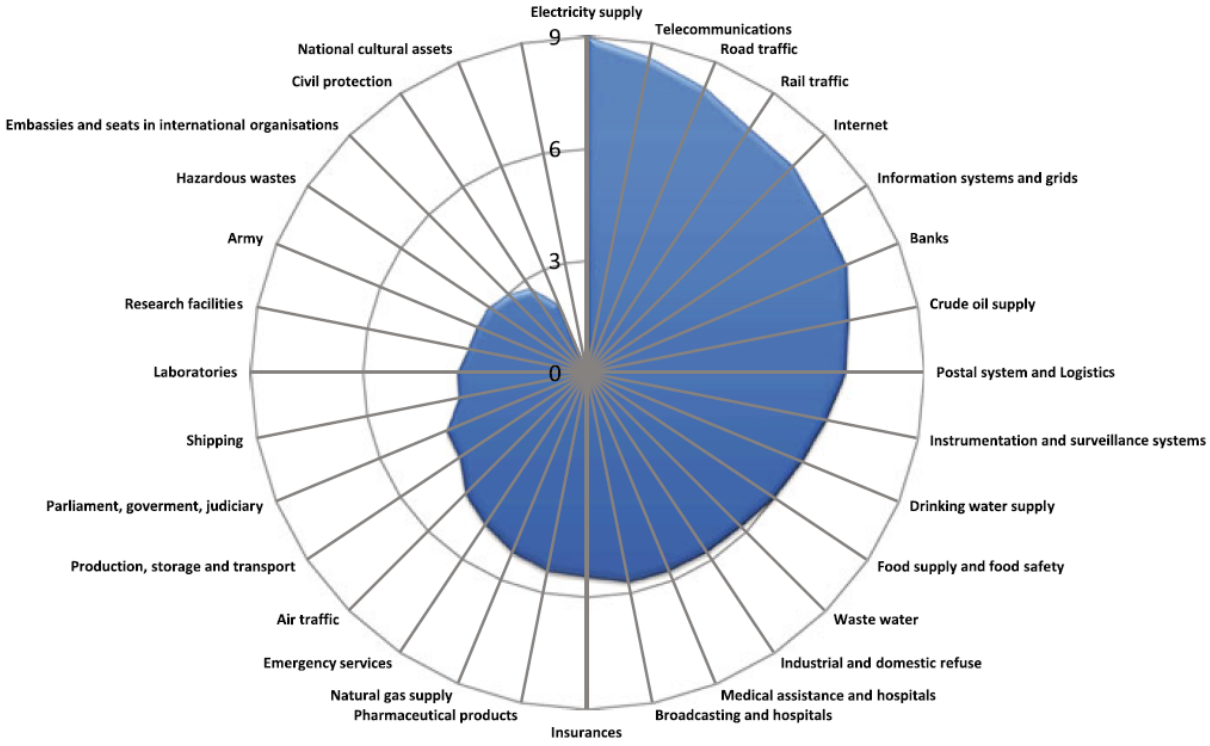


Figure 4. *Criticality of critical infrastructures [44]*

equipment: one is via web servers or SCADA systems, which are then connected to the respective controller via remote maintenance. The second method covers Industrial Control Systems that are directly accessible over the Internet, but use special industrial protocols (such as Siemens S7). These industrial protocols differ in the attributes they reveal, have a unique header, and can, therefore, be accurately identified. There are also proprietary RAW protocols from their respective vendors, so no authentication is required for interaction. However, this interaction can turn out to become difficult because special software or frameworks are required to communicate with the respective protocols.

Exposure of ICS

Investigations by security researchers from 2012 to 2014 revealed - based on Shodan - that within this period, at least 2 million devices worldwide were publicly accessible via the Internet, which are either themselves ICS or are related to them [34]. According to the research, at least 65,000 Industrial Control Systems were directly connected to the Internet with their bare interfaces and industrial protocols - without authentication and security mechanisms [17]. Many SCADA and control systems are insufficiently configured and have an active web server, that by default, allows communication with HTTP (port 80), FTP (ports 20 and 21), SNMP (port 161) or Telnet (port 23) [34]. About 7,200 entries were considered as critical infrastructures within the United States [35]. There is a worrying tendency to notice that industrial control equipment or control components are increasingly directly connected to the world wide web [17]. Even if they are not directly connected, control components are - at least for management reasons - reachable via the corporate network [43]. In March 2017 worldwide still more than 100,000 industrial plants were directly connected to the Internet - half of all hits were located in the United States [18] [19]. A heat map (based on Shodan data) shows a significant accumulation of industrial controls directly connected to the Internet in the United States and Europe (March 2017) (Figure 6). Worldwide 126,269 ICS-related devices[2] are found in November 2019 (still 52,015 ICS-devices[3] were found within the United States). As for Europe, in March 2017, especially in Germany, over 15,000 ICS-devices were found - the majority of the used protocols can be regarded as highly unsafe [3]. For November 2019 still 5,569 ICS-related devices[4] within Germany are issued by Shodan.

ICS Risk Scenarios

Based on the exposure of Industrial Control Systems, possible risk scenarios arise. Usually, the risk assessment process takes place from within a company. In our paper, the assessment of risks is based on the search engine Shodan. This basis of information corresponds to that of an attacker who collects external information about a company via the Internet in order to gain ac-

[2] `https://www.shodan.io/search?query=category%3Aics&language=en` - search:"category:ics" - retrieved: November 2019

[3] `https://exposure.shodan.io/#/US` - retrieved: November 2019

[4] `https://exposure.shodan.io/#/DE` - retrieved: November 2019

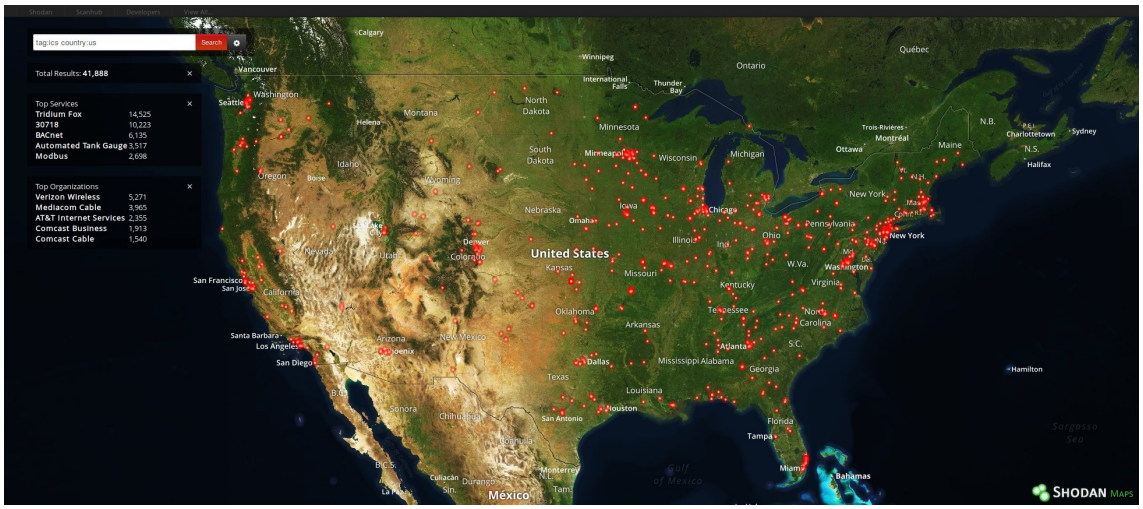


Figure 5. *Shodan Maps arranges hits geographically (satellite view) [17]*

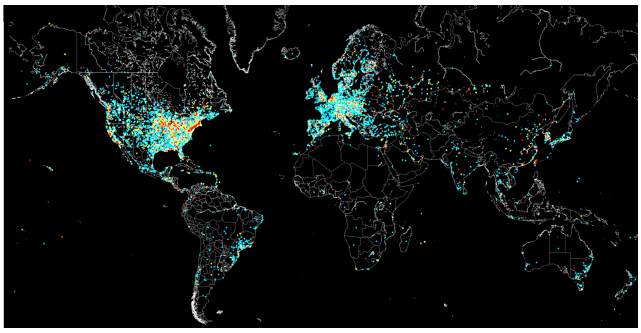


Figure 6. *Heatmap of Industrial Control Systems worldwide found by Shodan (March 2017, picture has been cut) [20].*

cess to systems. A particularly lucrative target for attackers are HMIs (Human Machine Interfaces), from which industrial plants are controlled - often by remote maintenance. Denial-of-Service attacks (DoS) also pose a considerable risk, as they can limit the availability of plants, which can violate high availability requirements. Also *man-in-the-middle attacks* (in particular *replay attacks*) represent a latent danger, because arbitrary commands can be infiltrated and executed. These attacks are greatly simplified by the lack of authentication and encryption mechanisms [2]. Standard operating systems such as UNIX or Windows are used as SCADA controls, so any open TCP/UDP port poses a massive danger to successfully damage, take over the systems or at least obtain information that can be used for further attacks. The following risk scenarios were examined under laboratory conditions.

Scenario 1: Compromising Siemens PLC

Only for the year 2019 the database "*Common Vulnerabilities and Exposures*" issues 62 vulnerabilities for Siemens PLCs and their management applications [29]. According to the CVSS[5] 18 vulnerabilities have a "high" or "critical" severity [29]. A particularly significant risk is posed by *stack-overflow vulnerabilities* that can be used to execute arbitrary program code [4] [24]. Siemens PLCs of the S7-300/400 product series use the proprietary "*S7Comm protocol*" [31] for communication. This is an RPC protocol, based on *TCP/IP* and *ISO-over-TCP* [31]. The research group around *SCADACS*[6] published a malicious software named *PLCinject*[7], which can inject malicious code into the running program of a Siemens PLC [31] [32]. For January 2018 an amount of 808 devices and controllers were found that are directly connected to the Internet in Germany via port 102 (Siemens S7comm protocol) (Figure 7). The level of exposure is constant in Germany with 784 hits[8] for November 2019. Worldwide Shodan counts 21,489 devices[9] with open TCP port 102. Every single accessible device can be easily examined via the search engine (Figure 8).

With *Snap7*[10] (based on the STEP 7 software for programming SIMATIC-S7 PLCs) applications exist to connect to Siemens PLCs. Various manipulations without any authentication of the PLC are very easy to perform with this multi-platform application (Figure 9). A manipulation of data in the area of a PLC can lead to critical malfunctioning. Metasploit modules are also available for Siemens PLCs[11] [23]. With the help of the module *auxiliary/admin/scada/simatic_s7_300_command* a Siemens Simatic S7-300 PLC can be started and stopped [30] [4]. A comparable module[12] is available for the S7-1200 series. The Metasploit module *simatic_s7_300_memory_view.rb*[13] allows

[5] `https://www.first.org/cvss/specification-document` - retrieved: November 2019

[6] `https://www.scadacs.org/` - retrieved: January 2018

[7] `https://github.com/SCADACS/PLCinject` - retrieved: January 2018

[8] `https://www.shodan.io/search?query=port%3A102+country%3ADE` - retrieved: November 2019

[9] `https://https://www.shodan.io/search?query=port%3A102` - retrieved: November 2019

[10] `http://snap7.sourceforge.net` - retrieved: Jan 2018), Application: `https://github.com/SCADACS/snap7` - retrieved: Jan 2018

[11] `https://github.com/moki-ics/s7-metasploit-modules` - retrieved: January 2018

[12] `https://www.exploit-db.com/exploits/19833/` - retrieved: January 2018

[13] `https://github.com/moki-ics/s7-metasploit-modules/blob/master/simatic_s7_300_memory_view.rb` -

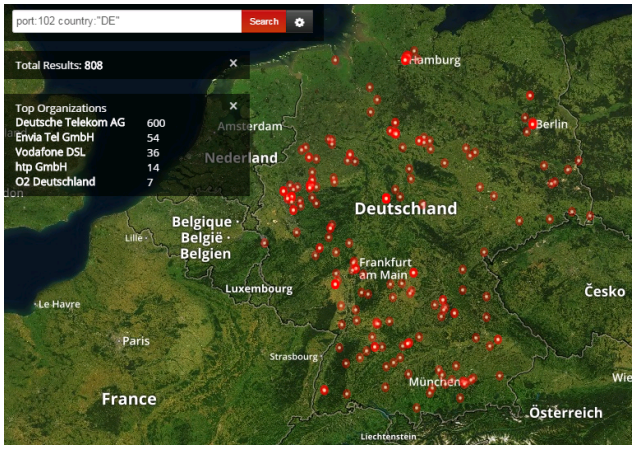


Figure 7. *Accessible S7 systems in Germany found by Shodan search (request: January 2018)*

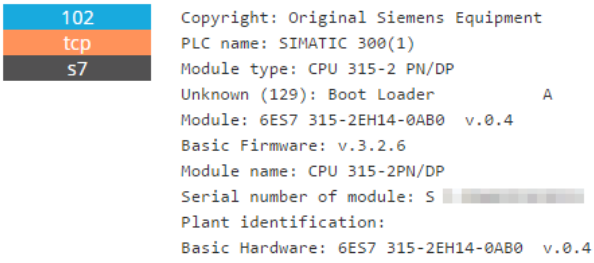


Figure 8. *A single Siemens PLC SIMATIC 300 device found by Shodan (request: January 2018)*

to read the memory of a S7-300 PLC. Furthermore the community *SCADA Strangelove* published a brute force tool for S7 PLCs[14], with which the password can be extracted.

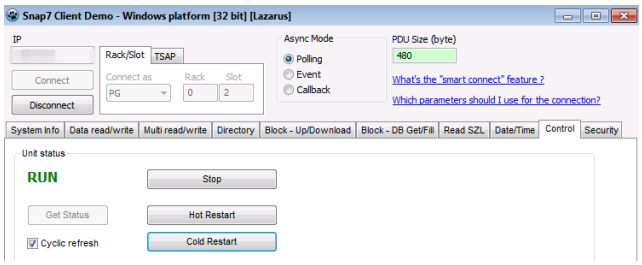


Figure 9. *GUI control panel for Snap 7 (laboratory environment)*

Scenario 2: Attacks based on open SMB and SNMP ports

The occurrence of ransomware in critical infrastructures can have serious effects. The cryptoworm *WannyCry* used serious exploits based on the SMB (*Server Message Block*) protocol in May 2017. This SMB protocol uses TCP port 445 and is mainly used for file sharing. The usage of the protocol should be restricted to the local network and not be freely accessible on the Internet (especially if no encryption or authentication mechanisms are implemented). According to a report in 2017 - 42% of the open SMB ports found in Shodan even allow a connection as a guest account. Of the servers that allow a connection, 95% use the free application *Samba* as an SMB server (which is known for various vulnerabilities). Furthermore, over two million devices found by Shodan still use the SMB protocol version 1 (which is considered insecure). The Metasploit module *smb-login-check* enables brute force and dictionary attacks. With another module *psexec* it is possible to take over the complete system on *Samba* systems. The CVE website contains 435 hits[15] concerning security matters, which are associated with the SMB protocol.

SNMP

The *Simple Network Management Protocol* is a network protocol that can be used to centrally monitor and control network elements (e.g., routers, switches, or printers). By default, the connectionless UDP port 161 is reserved for SNMP. The protocol setup is standardized according to *RFC 1157* and *RFC 3410*. The latest protocol version has three security mechanisms, as well as implemented key management. Using the Metasploit module *auxiliary/scanner/snmp/snmp_enum*, further information based on the SNMP protocol can be obtained from devices that might be used during a reconnaissance phase, such as hostnames, network interfaces, operating times, routing information, TCP information or ports used. The module *snmp_login*[16] allows brute force and dictionary attacks when authentication is enabled.

Scenario 3: Attacks based on the Modbus protocol

The properties of the Modbus protocol are presented on the section Industrial Network Protocols. It is the most widely used of all industrial protocols [2] [4]. Modbus has no security mechanisms such as authentication implemented and is therefore vulnerable to any attacks affecting the authenticity of Modbus frames - unauthenticated commands can be easily transmitted [2]. The protocol is also vulnerable to replay attacks in which the identity of a certain communication partner is pretended [4]. A search query from April 2017 to Shodan returned 14,871 freely accessible Modbus devices worldwide based on TCP port 502. For November 2019 an amount of 21,456 modbus-related devices[17] are found. Libraries exist like *pymodbus*[18] and *rmodbus*, which can be used to create, parse and receive Modbus packets [4]. Another tool for manipulating Modbus packets is *Scrapy*[19] in conjunction with a Modbus extension of *Digital Bond*[20]. For the simple readout of Modbus coils - this is how individual inputs and outputs are addressed in the context of the protocol - the com-

As of: 07.01.2018

[14] `http://scadastrangelove.blogspot.de/2013/01/s7brut.html` - Program code: `https://pastebin.com/0G9Q2k6y` - retrieved: November 2019

[15] `https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=SMB` - retrieved: November 2019

[16] `https://www.offensive-security.com/metasploit-unleashed/scanner-snmp-auxiliary-modules/` - retrieved: January 2018

[17] `https://www.shodan.io/search?query=port%3A502` - retrieved: November 2019

[18] `https://github.com/riptideio/pymodbus` - retrieved: October 2019

[19] `http://www.secdev.org/projects/scapy/` - retrieved: November 2019

[20] `http://www.digitalbond.com` - retrieved: November 2019

mand line tool *modbus-cli*[21] that can be integrated into *Kali Linux* (Figure 10).

```
root@HLKali:/home/hacker# modbus read 5.2.179.21 %MW100 5
%MW100        250
%MW101         88
%MW102       7500
%MW103       1000
%MW104       2640
```

Figure 10. *Reading a modbus device from the command line interface of modbus-cli*

With *modbus-discover*[22]a script is also available for the well-known network scanner *Nmap*. The script uses the Modbus function codes *43* and *90* to obtain extensive information about the target system such as manufacturer, network module, CPU module, firmware, revision, or last change. A Modbus tool for reading registers is also available for the Microsoft Windows operating system: *ShortBus Modbus Scanner*. Since no authentication is required for interaction using the protocol, successful communication with a Modbus terminal requires only a valid address, a function code, and generated data [2]. The data must address real existing registers or coils; otherwise, the packets will be discarded. Therefore additional information about the target system is needed. One possibility is to record the network traffic or to connect to the control unit and read out the respective configuration [2]. Using the function code *43*, information about the system can be obtained without prior knowledge. A further procedure is to be able to reproduce the addresses of the registers by arbitrary addressing them. Unlike other protocols, Modbus does not have any description fields for registers. Therefore the traceability of the functionality of registers can prove to be complex [4]. Modbus generally does not use encryption: commands and addresses are transmitted in plain text so that packets can be recorded and analyzed. Based on this, attackers can analyze the communication and create their own packets. Furthermore, the checksum (CRC) can be falsified by the Modbus protocol, since it is only generated at the transport level and not at the application level. With serial variants of Modbus, another property is used and that is broadcast communication: All connected devices on the bus may receive all messages [2]. Simulation applications such as *Modbus Simulator*[23] are used to test the previous tools under laboratory conditions without affecting active production systems. By a graphical representation in form of a GUI, the effects on the entire system become visible with changes of the registers or coils. Various exploits exist with regard to the Modbus protocol. An exemplary module for the *Metasploit Framework* is *auxiliary/admin/scada/modicon_command*[24]. With this module it is possible to connect to PLCS of the company *Schneider Electric* and stop the CPU there (this is equivalent to a DoS attack). The manufacturer uses the function code *90*, which is non-existent as Modbus function code according to the specification, therefore PLCs in particular are affected by *Schneider Electric* (the website *CVE-Details*[25] alone shows 206 vulnerabilities for devices of this manufacturer). This attack can have serious consequences [4], because unintentional faults in PLCs can generally cause serious damage to health, even life-threatening, as well as damage to controllers and systems [28].

```
root@HLKali:/home/hacker# modbus write 192.168.178.30 17 1 1 1 1 1 1 1 1
root@HLKali:/home/hacker#
```

Figure 11. *Write command for Modbus registers and coils in modbus-cli (laboratory environment)*

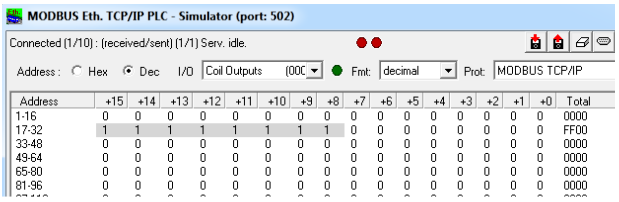


Figure 12. *Modbus Simulator successfully overwrites the addressed coils (laboratory environment)*

Therefore any tests were applied under laboratory conditions. As a result, registers and coils were successfully overwritten without any authentication (Figure 11 and 12). Another module worth mentioning is the *auxiliary/scanner/scada/modbusclient* - with it data can be read and written from PLCs using the Modbus protocol. A further Modbus exploit for *Metasploit* is the module *auxiliary/admin/scada/modi-/con_password_recovery*.

Scenario 4: Attacks based on the DNP3 and EtherNet/IP

Related devices to the *Ethernet Industrial Protocol* (*abbrev.:* EIP *or* EtherNet/IP) can be easily found in Shodan via the subcategory "Industrial Control Systems". The protocol has already been introduced in section *Industrial Network Protocols*. Even though the protocol was designed with the integrity of the packets in mind (checksum), no authentication or encryption mechanisms have been implemented [2]. The protocol uses - similar to Modbus - function codes. The sessions can be easily manipulated [2]. In January 2018 a search query to Shodan resulted 31,549 hits worldwide for the EtherNet/IP protocol. A Further request from December 2019 issued 49,304[26] hits (14,898 within the United States). Besides port 44818 (TCP/UDP), EtherNet/IP uses port 2222 for messages [4]. The project *pyenip* has released a *Python*-script[27], which can be used to collect information about EtherNet/IP-enabled devices. As long as the script is executed, packets can be recorded in *Wireshark*. One implementation of EtherNet/IP for the Windows operating system is the *Ethernet/IP*

[21] `https://github.com/tallakt/modbus-cli` - retrieved: November 2019

[22] `https://nmap.org/nsedoc/scripts/modbus-discover.html` - retrieved: November 2019

[23] `http://www.plcsimulator.org/` - retrieved: January 2018

[24] `https://www.rapid7.com/db/modules/auxiliary/admin/scada/modicon_command` - retrieved: January 2018

[25] `https://www.cvedetails.com/vulnerability-list/vendor_id-11651/Schneider-electric.html` - retrieved: November 2019

[26] `https://www.shodan.io/search?query=port%3A44818` - retrieved: December 2019

[27] `https://github.com/paperwork/pyenip/blob/master/ethernetip.py` - retrieved: January 2018

Explorer[28]. Another script named *enip-info*[29] exists for *Nmap*. This script is based on the *Python* script *ethernetip.py* and even displays the actual (private) IP address of a device, as well as ports even behind NAT firewalls (Figure 13) [4].

```
root@HLKali:/home/hacker# nmap -p 44818 --script enip-info [redacted]

Starting Nmap 7.40 ( https://nmap.org ) at 2018-01-21 14:19 CET
Nmap scan report for 115.134.134.180
Host is up (0.20s latency).
PORT      STATE SERVICE
44818/tcp open  EtherNet-IP-2
| enip-info:
|   Vendor: Rockwell Automation/Allen-Bradley (1)
|   Product Name: 1769-L33ER/A LOGIX5333ER
|   Serial Number: [redacted]
|   Device Type: Programmable Logic Controller (14)
|   Product Code: 107
|   Revision: 20.12
|_  Device IP: 192.168.1.10

Nmap done: 1 IP address (1 host up) scanned in 1.17 seconds
```

Figure 13. *The Nmap script enip-info scans open EIP ports*

The EtherNet/IP protocol, similar to other industrial protocols, has no security mechanisms implemented. Thus, exploits exist for this protocol[30] that can be used to perform replay attacks [4]. In Metasploit the module *auxiliary/admin/scada/multi_cip_command*[31] is found, with which control systems of the product line *ControlLogix* of the company *Allen Bradley*[32] can be stopped. The vulnerability is not within the devices themselves, but in the CIP protocol, which is inherent within the protocol stack [2]. On the basis of this protocol weakness, all variations of manipulations on devices using the EtherNet/IP protocol are conceivable [2]. The common *DNP3 protocol* is also found in the search engine Shodan. A request from December 2017 resulted in 3,916 hits related to the DNP3 protocol. Two years later in December 2019 the amount of exposed DNP3 ports has decreased to 434 hits[33]. In 2013, researchers found a serious vulnerability in the DNP3 protocol stack that affected (and still affects) an enormous number of vendors using the same vulnerable protocol library. Master and slave stations can be maliciously modified [2]. The protocol uses the TCP port 20000 by default. There is a *Nmap* script[34] available for the interaction with the DNP3 protocol stack, which must first be obtained and installed using the *Nmap Scripting Engine*. The script provides extensive information on open DNP3 ports.

Scenario 5: Remote maintenance based on the VNC protocol

In addition to the widespread industrial protocols, VNC (*Virtual Network Computing*) is also used for remote maintenance in the industrial environment [2] - in particular to control HMIs. This remote maintenance software is based on the RFB protocol (Remote Framebuffer Protocol), which is standardized in RFC 6143[35] and currently available in version 3.8. The client/server system uses the TCP ports 5900 and 5901 for maintenance purposes. Authentication is also supported but can be deactivated on the server-side [33]. Accessible VNC servers can be easily searched using *Shodan Images*. By means of Shodan 3.4 Million[36] open VNC ports were found worldwide in a request from December 2019). If no authentication is required from the VNC server, access to the operating system can still be secured by a blocking screen using password protection (screen saver). One module in Metasploit for detecting whether authentication has been enabled is the following: *auxiliary/scanner/vnc/vnc_none_auth*. VNC does not support authentication by username and password: only a password field can be used (eight-digit password). This strongly limits possible password strength and permutations. If authentication is activated, the passwords can easily be found out or guessed by trial and error due to the lack of password complexity. The *RFC 6143* explicitly refers to the fact that this type of authentication is considered cryptographically weak with VNC and should not be used in unsecured networks [33]. The passwords can be tried systematically and automatically using brute force or dictionary attacks. The pentesting framework *Metasploit* contains a module for brute force and dictionary attacks with VNC authentication enabled: *auxiliary/scanner/vnc/vnc_login*. Further serious known vulnerabilities for VNC are *CVE-2001-0167*[37] (CVSS: 7.6) and *CVE-2006-2369*[38] (CVSS: 7.5). Metasploit modules and *Nmap* scripts exist for both vulnerabilities. The CVE database[39] issues 112 entries related to VNC vulnerabilities.

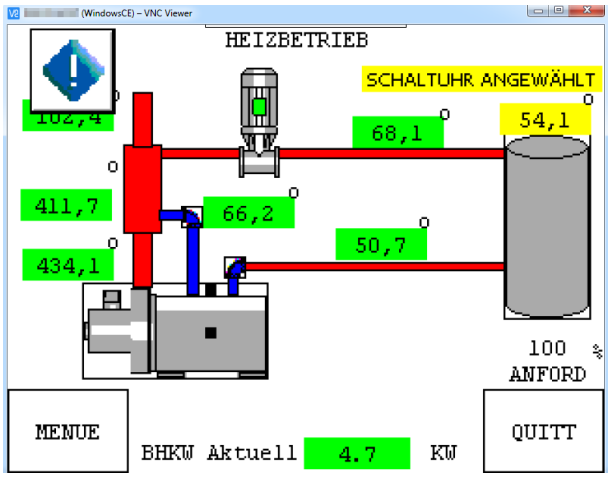


Figure 14. *Combined heat and power plant using VNC as remote maintenance (found via Shodan - January 2018)*

[28] `https://sourceforge.net/projects/enipexplorer/` - retrieved: January 2018

[29] `https://nmap.org/nsedoc/scripts/enip-info.html` - retrieved: January 2018

[30] `https://github.com/kenexis/PortableICS-MITM` - retrieved: January 2018

[31] `https://www.rapid7.com/db/modules/auxiliary/admin/scada/multi_cip_command` - retrieved: May 2018

[32] `http://ab.rockwellautomation.com/de/Programmable-Controllers/ControlLogix` - retrieved: January 2018

[33] `https://www.shodan.io/search?query=port%3A20000+source+address` - retrieved: December 2019

[34] `https://github.com/sjhilt/Nmap-NSEs/blob/master/dnp3-info.nse` - retrieved: January 2018

[35] `https://tools.ietf.org/html/rfc6143` - retrieved: January 2018

[36] `https://www.shodan.io/search?query=port%3A5900%2C5901` - retrieved: December 2019

[37] `https://www.cvedetails.com/cve/CVE-2001-0167/` - retrieved: November 2019

[38] `https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2006-2369` - retrieved: November 2019

[39] `https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=vnc` - retrieved: November 2019

Scenario 6: Remote maintenance based on the Remote Desktop Protocol (RDP)

The Remote Desktop Protocol (*abbrev.:* RDP) is a proprietary remote maintenance protocol, which is commonly used in the environment of Windows operating systems. By default, the protocol supports encryption and uses the TCP/UDP port 3389. Similar to VNC (previous scenario), RDP is also used for remote maintenance of industrial plants [17]. When RDP is used, it should always be used in conjunction with VPN, and port 3389 should under no circumstances be accessible over the Internet. An open RDP service can even lead to a complete takeover of the system because there are many unpatched and insecure Windows systems, which are also used by SCADA controllers [40] [41]. Especially obsolete Windows Server 2003 and Windows XP operating systems are affected by the vulnerability *CVE-2017-9073*. A request to Shodan from December 2019 resulted in over 5 Million accessible RDP ports worldwide. For the serious vulnerability *CVE-2012-0002*[40] applicable exploit modules exist for the *Metasploit Framework*. The module *auxiliary/scanner/rdp/ms12_020_check* checks the systems for the vulnerability *CVE-2012-0002*, which is called *MS12-020* in the Windows environment - without changing or restricting the system (Figure 15). Another Metasploit module *auxiliary/dos/windows/rdp/ms12_020_maxchannelids* can actively exploit the *CVE-2012-0002* vulnerability for a DoS attack. After applying the module *ms12_020_maxchannelids* the system issues a blue screen i.e. the target system is no longer available.

```
msf auxiliary(ms12_020_check) > exploit

[+] 192.168.200.65:3389   - 192.168.200.65:3389 - The target is vulnerable.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 15. *RDP server vulnerable to CVE-2012-0002, checked by Metasploit (laboratory environment)*

Other RDP vulnerabilities include *CVE-2016-0036*[41] and *CVE-2017-0176*[42]. A general overcoming of authentication with an RDP connection in the locked screen for Windows operating systems can be done by brute force or dictionary attacks; often even the user name (e.g. *Administrator*) is already specified in the login field. The Metasploit module *post/windows/escalate/screen_unlock* can also be used to break out of the locked login screen.

Scenario 7: Web interface as an attack vector

The attack on the basis of an industrial protocol is enormously extensive. Both, the structure of the protocol, as well as the functionality of the specifically connected terminal device (e.g. PLC) must be studied. A simpler way to compromise devices within an industrial environment is to attack activated web interfaces or configuration interfaces (Figure 16).

These web interfaces preferably use port 80 or 443. The inputs made in the HTML forms are transferred to PLCs, which then convert the inputs into control commands for the concrete

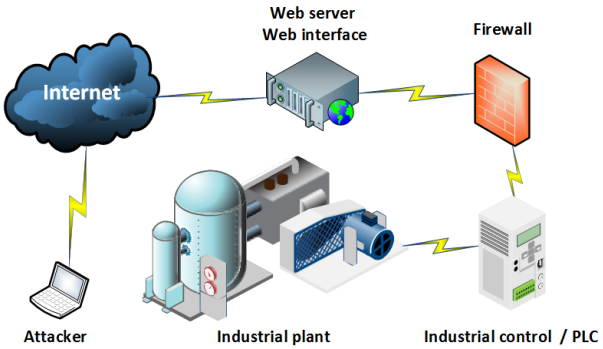


Figure 16. *Simplified representation of a web interface as a possible attack vector indirectly connected to an ICS*

industrial plants. A problem here is that control commands can reach the control system, which are not actually permitted within the web interface. It is crucial whether masking or filtering takes place, which checks the commands for their semantics and correctness. There are exploits for web servers that can be used to take over the entire system completely [24]. For the widespread web server *Apache* there are at least over 1200 known vulnerabilities on the website *CVE Details*[43]. Even an open TCP port 3306 on *MySQL* or port 5432 on *PostgreSQL* is sufficient to initiate brute force or dictionary attacks. *Vulnerability scanner* like *Burp*[44] or *OWASP Zed Attack Proxy*[45] disclose vulnerabilities in web applications. Since web server opens further ports for management purposes, it is also possible to attack Telnet, FTP or SSH. This applies to any open port that allows a direct or indirect connection to the system or its control or configuration. If login fields exist for users (e.g., administrator), attackers can try to gain access to the control of the system by brute force attacks. If failed logins are not sanctioned, brute force or dictionary attacks can easily be applied. A successful attack on login fields depends considerably on the complexity of the password and whether temporary login blocks are implemented for failed login attempts.

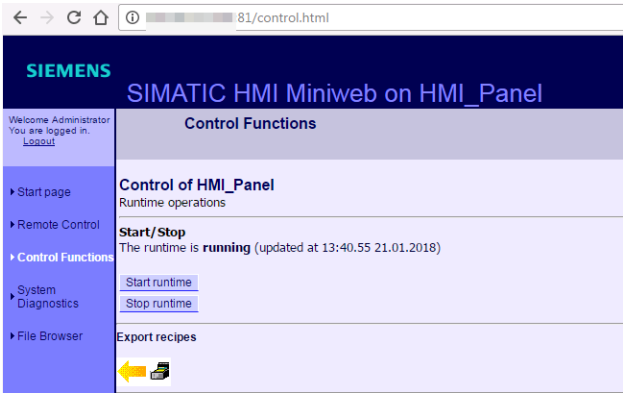


Figure 17. *Accessible web interface of SIMATIC 300 (port 80)*

For the devices *W2150A/W2250A* of the company *Moxa*, for

[40] https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2012-0002 - retrieved: January 2018

[41] https://www.cvedetails.com/cve/CVE-2016-0036/ - retrieved: January 2018

[42] https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2017-0176 - retrieved: January 2018

[43] https://www.cvedetails.com/vulnerability-list/vendor_id-45/Apache.html - retrieved: November 2019

[44] https://portswigger.net/burp - retrieved: November 2019

[45] https://www.zaproxy.org/ - retrieved: November 2019

example, the passwords for the delivered web interface are visible in the (free downloadable) manual [45]. The devices are so-called IIoT (Industrial Internet of Things). These are control units that interact directly with Industrial Control Systems (e.g., PLCs). The IIoT device *W2250A*, for instance, has serial ports, an Ethernet port, and a wireless connection [46]. IIoT devices were found in Shodan that did neither enable authentication nor encryption and were freely accessible through port 80 (Figure 17). With successful access to the configuration interface, it is possible to change IP addresses, the subnet mask, import any Firmware, change TCP/UDP ports, edit Access Control Lists, change the DNS and DHCP server as well as the default gateway (Figure 18). Ping input fields are even integrated into HTML forms, which can be used to check further devices or servers reachable from the interface. In addition to the standard password, the *NPort W2150A/W2250A* devices are vulnerable to cross-site scripting (XSS), cross-site request forgery (CSRF), stack overflows, command injections, insecure authentication and zero-day exploits [24]. Reverse engineering can also be used to rebuild the manufacturer's firmware [24].

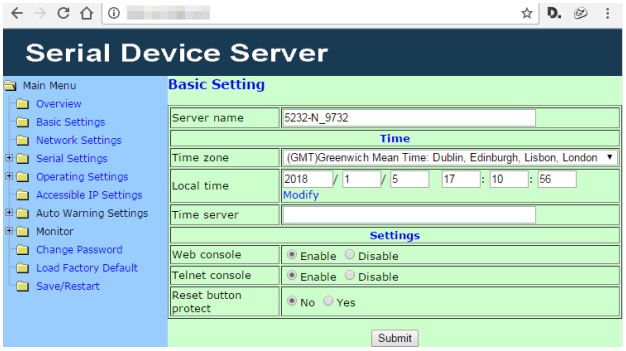


Figure 18. *Web interface of a Moxa 5232-N (found in Shodan January 2018)*

Summary and Conclusion

Industrial control equipment is used in automation processes and process control operations within Critical Infrastructures. The consequences of IT attacks on industrial plants are less predictable than those on conventional IT systems and require comprehensive knowledge of the functioning of the plants. The increasing network connectivity of these - today no longer isolated - systems beyond external borders represents a considerable risk for IT security and consequently for the availability of these systems. Remote maintenance and progressive integration into management systems, as well as the use of conventional hardware, standard protocols, and common operating systems, have resulted in industrial control equipment becoming more and more aligned with conventional IT systems. Initially, proprietary industrial protocols are now compatible with common network protocols and standards such as Internet Protocol (IP) or Ethernet. As a consequence, new attack vectors arise, so that the safety and protection level of industrial plants must be reassessed. Obsolete standard operating systems are no longer supported and updated, but they are still used as SCADA controllers. For Programmable Logic Controllers, as used in most industrial plants, (even critical) firmware updates are not applied by the operators. Web interfaces simplify the configuration and maintenance of equipment. However, when exposed to the Internet, these interfaces represent an additional attack vector. A compromise of a web server leads in severe cases to the complete takeover of the industrial control. Other critical features of these systems are unnecessarily opened TCP/UDP ports. This is particularly serious in the context of exposure to the Internet; active services or open ports make it possible to successfully take over the systems, or at least to obtain information that can be used for further attacks. Under laboratory conditions, it was proofed that activated ports and the use of unsafe industrial protocols represent an evident risk. The most common attacks on companies are done via the Internet and via outdated or poorly configured networks. The industrial network design of operators has shortcomings, such as insufficient segmentation into network zones. As a result, there are no security and control mechanisms between zones. A further lucrative target for attackers are HMIs (Human Machine Interfaces), from which industrial plants are often controlled by remote maintenance. Furthermore, missing encryption mechanism allows the sniffing of network traffic and consequently the analysis of network protocols. This can serve as a basis for *Man-in-the-Middle* attacks (such as replay attacks in particular). With *Stack-Overflow* vulnerabilities, there is a latent danger that arbitrary commands are injected into the controllers and be executed. The lack of authentication mechanisms greatly simplifies these attacks. A large number of SCADA systems and Industrial Control Systems are inadequately secured from an information technology perspective. Using the search engine Shodan, these inadequately secured control systems can be found accessible on the Internet. Without authentication, it could be connected to sewer systems, wind turbines, solar power plants, generators, or combined heat and power plants. This is a worrying extent of exposure that requires a paradigm change by implementing IT security mechanisms within the architecture of ICS devices and the environment ("security by design").

References

[1] Colbert, E. J. M.; Kott, A.: Cyber-security of SCADA and Other Industrial Control Systems, Springer International Publishing 2016, eBook ISBN: 978-3-319-32125-7, `http://www.springer.com/de/book/9783319321233`, (retrieved: June 2017).

[2] Knapp, E. D.; Langill, J. T.: Industrial Network Security, Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, Syngress 2014, ISBN-10: 0124201148, Kindle Edition.

[3] Industrial Control Systems in Germany, Report, April 2017, search query: "category:ics country:DE" in `www.shodan.io`, (retrieved: April 2017).

[4] Bodungen, C. E.; Singer, B. L. et al.: Hacking Exposed: Industrial Control Systems: ICS and SCADA Security Secrets & Solutions, McGraw-Hill 2016, ISBN-10: 1259589714.

[5] Guide to Industrial Control Systems (ICS) Security - Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), National Institute of Standards and Technol-

ogy 2015 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82.pdf, (retrieved: November 2016).
[6] Ginter, A.: SCADA Security: What's broken and how to fit it. 2016, ISBN-10: 0995298408, Kindle Version.
[7] Electricity Subsector Cybersecurity Risk Management Process (RMP), U.S. Department of Energy (DOE) 2012, DOE/OE-0003, https://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf, (retrieved: October 2017).
[8] Francis, G. L.: SCADA: Beginner's Guide, Kindle-Version, https://www.amazon.de/SCADA-Beginners-English-Francis-G-L-ebook/dp/B01M16XUYZ/ref=sr_1_fkmr1_1?ie=UTF8&qid=1494582498&sr=8-1-fkmr1&keywords=SCADA+beginer, (retrieved: May 2017).
[9] Krotofil M.; Larsen, J.: Rocking the pocket book: Hacking chemical plants for competition and extortion, August 2015, White Paper, DEFCON 23, Hamburg University of Technology, Video: https://www.youtube.com/watch?v=AL8L76n0Q9w (retrieved: July 2017), Abstract: https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20presentations/DEFCON-23-Marina-Krotofil-Jason-Larsen-Rocking-the-Pocketbook-Hacking-Chemical-Plants-WP-UPDATED.pdf, (retrieved: July 2017).
[10] Goldman, D.: Shodan: The scariest search engine on the Internet, CNN Money, New York, published: 8. April 2013, http://money.cnn.com/2013/04/08/technology/security/shodan/, (retrieved: October 2016).
[11] Goldman, D.: The Internet's most dangerous sites, CNN Money, New York 2013 http://money.cnn.com/gallery/technology/security/2013/05/01/shodan-most-dangerous-internet-searches/, (retrieved: May 2017).
[12] Russell, J.: A brief history of SCADA/EMS, http://scadahistory.com/, (retrieved: October 2017).
[13] Lopez, J. et al.: Critical Infrastructure Protection: Advances in Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense, Springer Science & Business Media, 2012, ISBN: 9783642289194.
[14] Luiijf, E.; Nieuwenhuijs, A.; Klaver, M.; van Eeten, M.; Cruz E.: Empirical Findings on Critical Infrastructure Dependencies in Europe, Springer, Berlin, Heidelberg, ISBN: 978-3-642-03551-7, http://publications.tno.nl/publication/101029/8dNFoC/pub124913.pdf, (retrieved: January 2018).
[15] Rinaldi, S. M; Peerenboom, J. P.; Kelly, T. K.: Identifying, understanding, and analyzing critical infrastructure interdependencies, IEEE Control Systems, Volume: 21, Issue: 6, December 2001, http://ieeexplore.ieee.org/document/969131/, (retrieved: August 2017).
[16] Reichenbach, G.; Göbel, R. et al.: Risks and challenges for public safety in Germany, Scenarios and key questions - Green Paper of the Future Public Security Forum, ProPress Publishing Company 2008, Berlin/Bonn.
[17] Matherly, J.: Complete Guide to Shodan, June 2016, https://leanpub.com/shodan, (retrieved: August 2016).
[18] Matherly, J.: More than 100.000 industrial control systems connected to the internet: https://www.shodan.io/report/btZPXVti, twitter-account: https://twitter.com/achillean (twitter entry: March 2017).
[19] Matherly, J.: A quick map of industrial control systems accessible over the Internet in the US. Most of them are buildings and connected via mobile net., February 2017, twitter-account: https://twitter.com/achillean, https://pbs.twimg.com/media/C3mdAX6UEAAqlkO.jpg:large, (retrieved: April 2017).
[20] Matherly, J.: A map of industrial control systems that are connected to the Internet (created for my talk next week at @KIACS_CS): http://i.imgur.com/FiwO5gj.png, March 2017, twitter-account: https://twitter.com/achillean.
[21] O'Harrow Jr., R.: Cyber search engine Shodan exposes industrial control systems to new risks, Washington Post, June 2012, https://www.washingtonpost.com/investigations/cyber-search-engine-exposes-vulnerabilities/2012/06/03/gJQAIK9KCV_story.html, (retrieved: July 2017).
[22] MODBUS APPLICATION PROTOCOL SPECIFICATION V1.1b3, April 2012, Modbus Organization, http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf, (retrieved: December 2017).
[23] Beresford, D.: Exploiting Siemens Simatic S7 PLCs, 2011, Black Hat USA 2011, https://media.blackhat.com/bh-us-11/Beresford/BH_US11_Beresford_S7_PLCs_Slides.pdf, (retrieved: August 2017).
[24] Roth, T.: SCADA - Gateway to (s)hell - Hacking industrial control gateways, 34C3, https://media.ccc.de/v/34c3-8956-scada_-_gateway_to_s_hell#t=980, (retrieved: January 2018).
[25] Getting the Most Out of Shodan Searches, SANS Penetration Testing, December 2015, http://pentesting.sans.org/blog/2015/12/08/effective-shodan-searches?utm_medium=Social&utm_source=Twitter&utm_content=SANSPenTest+Blog+Shodan+Searches&utm_campaign=SANS+Pen+Test, (retrieved: April 2017).
[26] Securing Industrial Control Systems-2017, SANS Survey, Bengt Gregory-Brown, June 2017, https://www.sans.org/reading-room/whitepapers/analyst/securing-industrial-control-systems-2017-37860, (retrieved: December 2017).
[27] O'Harrow Jr., R.: Cyber search engine Shodan exposes industrial control systems to new risks, Washington Post, online article, June 2012, https://www.washingtonpost.com/investigations/cyber-search-engine-exposes-vulnerabilities/2012/06/03/gJQAIK9KCV_story.html?utm_term=.ee3b7172f5e5, (retrieved: June 2018).
[28] Modicon M221 Logic Controller Programming

Guide, April 2014, Schneider Electric, http://pneumatykanet.pl/wp-content/uploads/2016/11/Modicon-M221-Logic-Controller-Programming-Guide-EN.pdf, (retrieved: January 2018).

[29] CVE Details, Siemens: Security Vulnerabilities Published in 2019, http://www.cvedetails.com/vulnerability-list/vendor_id-109/year-2019/Siemens.html, (retrieved: November 2019).

[30] Siemens Simatic S7-300/400 - CPU START/STOP Module (Metasploit), Author: Dillon Beresford, https://www.exploit-db.com/exploits/19831/, (retrieved: January 2018).

[31] Klick J.; Lau, S.; Marzin, D.; Malchow J.; Roth, V.; Internet-facing PLCs as a Network Backdoor, Freie Universität Berlin, 2015, SCADA CS, http://www.inf.fu-berlin.de/groups/ag-si/pub/plc_backdoor_spicy.pdf, (retrieved: February 2017).

[32] Klick J.; Lau, S.; Marzin, D.; Malchow J.; Roth, V.; Internet-Facing PLCs - A New Back Orifice, Freie Universität Berlin, 2015, SCADA CS, https://www.blackhat.com/docs/us-15/materials/us-15-Klick-Internet-Facing-PLCs-A-New-Back-Orifice.pdf, (retrieved: November 2017).

[33] The Remote Framebuffer Protocol, Internet Engineering Task Force (IETF), ISSN: 2070-1721, March 2011, https://tools.ietf.org/html/rfc6143, (retrieved: January 2018).

[34] Radvanovsky, B.: Project SHINE (SHodan INtelligence Extraction) Findings Report Based on intelligence gathered from the SHODAN search engine between 14 Apr 2012 through 31 Jan 2014, 2014, https://de.slideshare.net/BobRadvanovsky/project-shine-findings-report-dated-1oct2014, (retrieved: January 2017).

[35] ICS-CERT Monitor October/November/December 2012 - Industrial Control Systems Cyber Emergency Response Team 2012, https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2012.pdf, (retrieved: January 2020).

[36] Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, Industrial Control Systems Cyber Emergency Response Team, September 2016, https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf, (retrieved: November 2017).

[37] Byres, E; Lowe, J.: The myths and facts behind cyber security risks for industrial control systems, in Proceedings of the VDE Kongress, Vol. 116, 2004, http://www.controlglobal.com/assets/Media/MediaManager/The_Myths_and_Facts_behind_Cyber_Security_Risks.pdf, (retrieved: October 2017).

[38] IEC 61131–3: Programming Industrial Automation Systems: Concepts and Programming Languages, Requirements for Programming Systems, Aids to Decision-Making Tools, ISBN:3540677526, Springer February 2001.

[39] Industrial Control System Security - Top 10 threats and countermeasures 2016, Bundesamt für Sicherheit in der Informationstechnik, Germany, 2016, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005.pdf?__blob=publicationFile, (retrieved: October 2016).

[40] Johnson, R.: Survey of SCADA security challenges and potential attack vectors, Internet Technology and Secured Transactions (ICITST), 2010 International Conference for, pp. 1 –5, November 2010.

[41] Igure V. M.; Laugther, S. A.; Williams R. D.: Security issues in SCADA networks, Computers and Security, October 2006, ACM Digital Library, http://dl.acm.org/citation.cfm?id=2639551, (retrieved: April 2017).

[42] Hacking SCADA, online article, occupytheweb, published: May 2015, Null Byte, https://null-byte.wonderhowto.com/news/hacking-scada-0162095/, (retrieved: November 2016).

[43] Weiss, J.: Protecting Industrial Control Systems from Electronic Threats, Momentum Press, May 2010, ISBN-13: 978-1606501979.

[44] Kröger, W; Zio, E.: Vulnerable Systems, publisher: Springer-Verlag 2011, ISBN: 978-0-85729-654-2.

[45] NPort W2150A/W2250A Series Quick Installation Guide, Edition 6.1, September 2017, Moxa, http://file.moxa.com.cn/doc/man/NPort_W2150A_W2250A_Series_QIG_e6.1.pdf, (retrieved: January 2018).

[46] NPort W2150A/W2250A, 1 and 2-port serial-to-WiFi (802.11a/b/g/n) device servers with wireless client, Moxa, October 2017, https://www.moxa.com/doc/specs/nport_w2150a_w2250a.pdf, (retrieved: January 2018).

[47] Schneider Electric Quantum Ethernet Module Hard-Coded Credentials, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), 2013, https://ics-cert.us-cert.gov/advisories/ICSA-12-018-01B, (retrieved: November 2016).

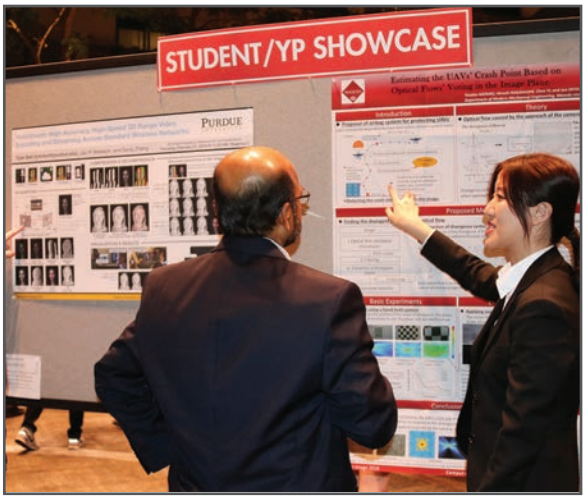
JOIN US AT THE NEXT EI!

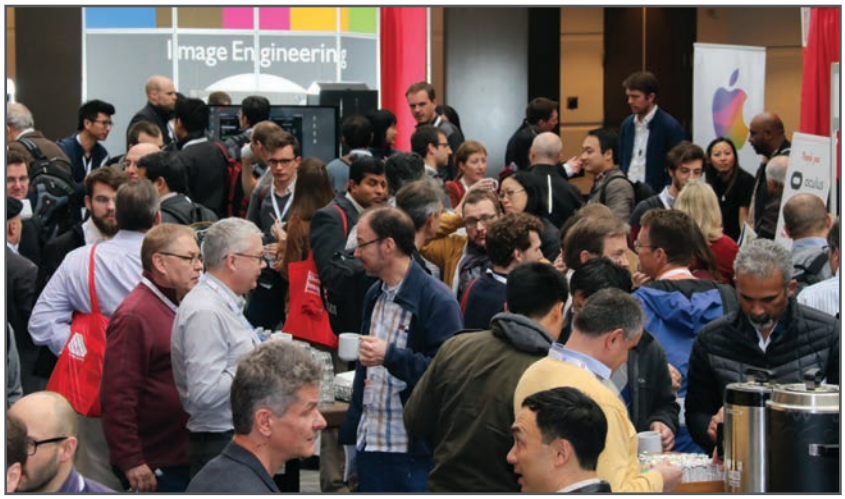
IS&T International Symposium on

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