D. Demmler, D. Krupka, H. Federrath. (Hrsg.): INFORMATIK 2022,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2022 1571

Interactive graphical modeling of security artefacts for abstracted Industry 4.0 automation systems

Louis Roger Tchuegoue Djeukoua[1] Edin Kreho[2] Siwar Belaidi[3] Karl Waedt[4]

Abstract: The frontend and backend are found in all software and therefore also on all websites. These two terms describe two different layers that make up programs or pages. About two thirds of all companies have their own website, and most employees use computers.Globally, cyberattacks are becoming more prominent and spreading to multiple areas, and the move to Industry 4.0 requires increased security measures. Important security precautions must be taken from the development of industrial devices that use the Industrial Internet of Things, with IEC 62443, ISO/IEC 27001, and their integration into the architecture of existing information and automation systems must be secure. IEC 62443 focuses on the IT security of so-called industrial automation and control systems (IACS), which are necessary for the safe and reliable operation of automated factories or infrastructures. [Her08] Since security breaches are inevitable, it is also important to implement detection and response mechanisms in industrial automation and control systems (IACS). Together, these measures will enable various organizations to achieve an appropriate level of resilience. This paper discusses the interactive graphical representation of large-scale industrial automation systems for the purpose of modeling and evaluating cybersecurity during all phases of the industrial equipment life cycle. In addition, it addresses the expressiveness and scalability of front-end graphical problems by assuming that a multi-user back-end server with a semi-formal representation of cybersecurity-related artifacts is available, at least in software prototype form.

Keywords: Industrial Automation and Control System; Web Framework; Graphical User Interface; bi-directional data binding; cooperative real-time development; Cybersecurity; Attack Scenarios; Cyber Physical System

1 Introduction

Advances in the Industrial Internet of Things (IIoT), interconnectivity, continued growth of smart ecosystems, and quintessential process automation have not only opened up immense opportunities, but also expanded the cyber threat and attack landscape. The main

[1] Hochschule für Technik und Wirtschaft Berlin (HTW Berlin), Fachbereich 1 - Energie und Information, Treskowallee 8, 10318 Berlin, Germany, rogerdjeukoua@yahoo.fr
[2] Friedrich-Alexander-Universität Erlangen(FAU Erlangen), Lehrstuhl Informatik Fau Erlangen, Schlossplatz 4, Erlangen, Germany edin.kreho@fau.de
[3] Framatome GmbH,ICETA-G Department ,Paul-Gossen-Straße 100,91052, Erlangen,Germany siwar.belaidi@framatome.com
[4] Framatome GmbH, ICETA-G Department, Paul-Gossen-Straße 100, 91052, Erlangen, Germany karl.waedt@framatome.com

doi:10.18420/inf2022_136

manifestation of this shift is that industries are striving to align with Industry 4.0 goals on demand. In particular, it has become clear that the convergence and amalgamation of industrial operational technology (IoT) and information technology (IT) is driving the sophistication, complexity of the IIoT ecosystem, paradigm shift, and global security changes.The more innovative companies become, the greater their vulnerability to attack. The failure of a single factory can result in losses of millions of dollars or Euros per day or even endanger human lives. Therefore, it is critical to minimize the risks of cyber attacks. [Her08] [Ple19]

2 Problem Statement

Industry 4.0 and other IoT environments are typically composed of many different components such as sensors, pumps, pressurizers, valves, motors, circuit breakers and other similar devices. These frequently exchange data, building up a complex and confusing information network. In the event of an intrusion, it is important to quickly assess which data could be compromised. However, due to insufficient documentation and analysis techniques, companies and institutions often have difficulties or it takes a very long time to find out which data is actually affected.Based on the modeling, analysis tools can then be used to quickly assess how attacks on abstracted industrial automation systems can be avoided or eliminated. This paper addresses the interactive graphical representation of large industrial automation systems with the goal of cybersecurity modeling and assessment during all lifecycle phases of industrial equipment. The graphical representation includes primary and supporting assets as defined in ISO/IEC 27005:2022. [22] (See fig. 1)

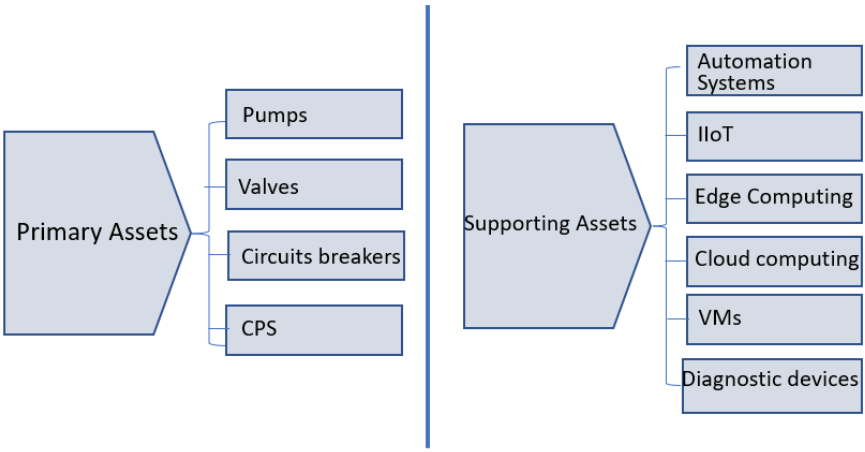

Figure 1: Primary and supporting assets mentioned in this paper

As described on the figure above, primary assets addressed and graphically modeled in this paper include pumps, valves, circuit breakers, and general Cyber Physical Systems (CPS) that interact with automation systems. Supporting assets are distributed automation systems, industrial IoT systems (IIoT), edge computing, cloud computing, virtual machines, and diagnostic devices that are only temporarily connected to other supporting assets.[Wik22][Beh17] In this paper, only the expressiveness and scalability issues of the graphical front-end are addressed. It is assumed that a multi-user capable backend server with a semi-formal representation of cybersecurity-related artifacts is available, at least as a software prototype[Kie13].

3 Abstracted Industry 4.0 automation systems

3.1 Definition

According to DIN 19 233, the term automation is understood to mean the “equipment of a device so that it operates wholly or partly as intended without the assistance of a human being”. It is also defined as the use of artificial systems that automatically follow a program and make decisions on the basis of the program to control and, if necessary, regulate processes [Vet82].

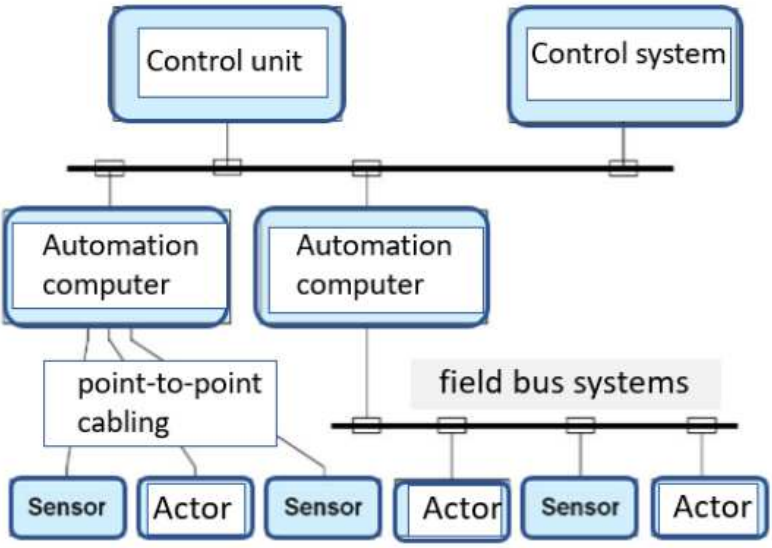

Figure 2: Basic structure of example automation systems

Additionally, the term automation includes the assumption of process control and possibly process regulation tasks by artificial systems. [Her08] The figure 2 above describes the basic structure of an example automation systems. An Abstracted Industrial Automation System is a conceptual generalized automation platform that allows the representation of different concrete industrial automation systems. The concept of industrial automation system in this paper is not about an automation system from a specific manufacturer but a fully configurable or meta automation system that is not tied to a specific manufacturer.[Wit22] In the sense of Cloud Computing Reference Architecture or Big Data Reference Architecture or IoT Reference Architecture. The concept approaches Automation Architecture what means that the automation system will assume certain characteristics, such as:

- an automation platform that allows multiple automation systems to be configured
- the automation platform supports the implementation of networked automation systems
- each automation system consists of automation subsystems
- each subsystem contains several hardware modules (assemblies or compact hardware units) The hardware modules are also called embedded components
- A hardware module optionally belongs to a subrack (rack/subrack)
- The hardware executes real-time software
- A hardware subsystem is optionally located in a IC cabinet (which is optionally lockable and optionally indicates whether the cabinet door is open.
- Optionally, a DCS cabinet can have two doors (front door to plug in the boards and rear door to perform wiring)
- The embedded subsystems are optionally connected to service devices or diagnostic equipment (usually notebooks). Service devices can remain continuously connected. Diagnostic devices are only connected temporarily, e.g. for initial software loading, parameterization and troubleshooting.
- The control cabinets (or directly the embedded systems) are located in a lockable (or not lockable) room.
- The rooms are located on a certain corridor (level) of a building.
- A facility (power plant or factory) may contain multiple buildings. (Separate buildings or rooms are often required for safety reasons, e.g., so that not all buildings are affected in an assumed unlikely airplane crash.
- All hardware components have certain interfaces that are relevant for security considerations, e.g. RJ45 for network communication via copper cables, optical connections, USB interfaces, serial interfaces (especially embedded systems), ...

- Security measures (security controls) are applied at all levels (building, hallway, room, control cabinet, ... , application software).

3.2 Application fields of Abstracted Industry 4.0 automation systems

Industry 4.0 includes cyber-physical systems (CPS), the Internet of Things (IoT), the Industrial Internet of Things (IIOT), cloud computing, cognitive computing and artificial intelligence.In addition to purely industrial applications, such as intelligent manufacturing and production environments in various industries (smart factories), cyber physical systems are also used in many other areas[Vet82]. These include intelligent power grids (Smart Grids), electronic health, age-appropriate assistance systems, but also intelligent traffic monitoring systems or automatic early warning systems in disaster control.Industrie 4.0 and CPS exhibit a high degree of networking and operate largely autonomously. One of the greatest challenges is to establish standards and industry grade products that ensure the interoperability of cyber-physical systems. Only seamless interaction between the various technologies and hardware or software components will enable Industrie 4.0 to realize its full potential. Cross-company networking of cyber-physical systems is necessary to control complex plants and processes.[Pre16]

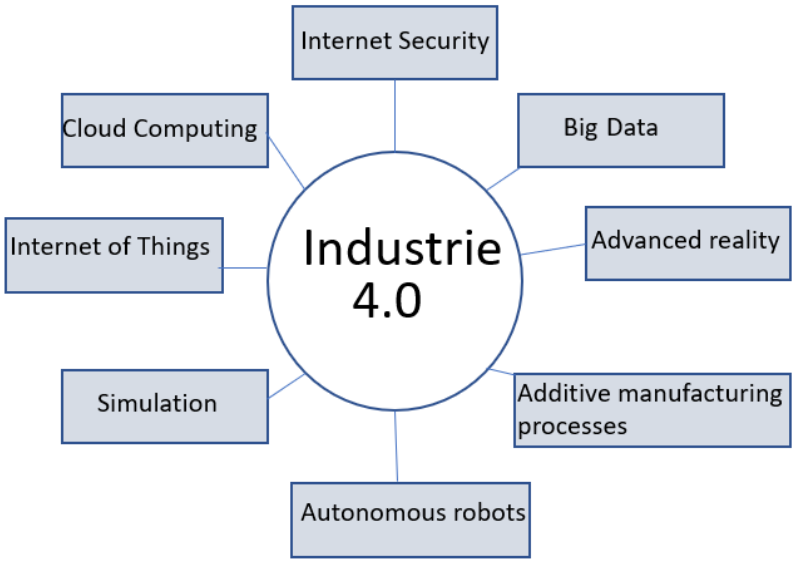

Figure 3: Application fields of industry 4.0

3.3 Interconnection and structuring of UI model with interactive assets representation

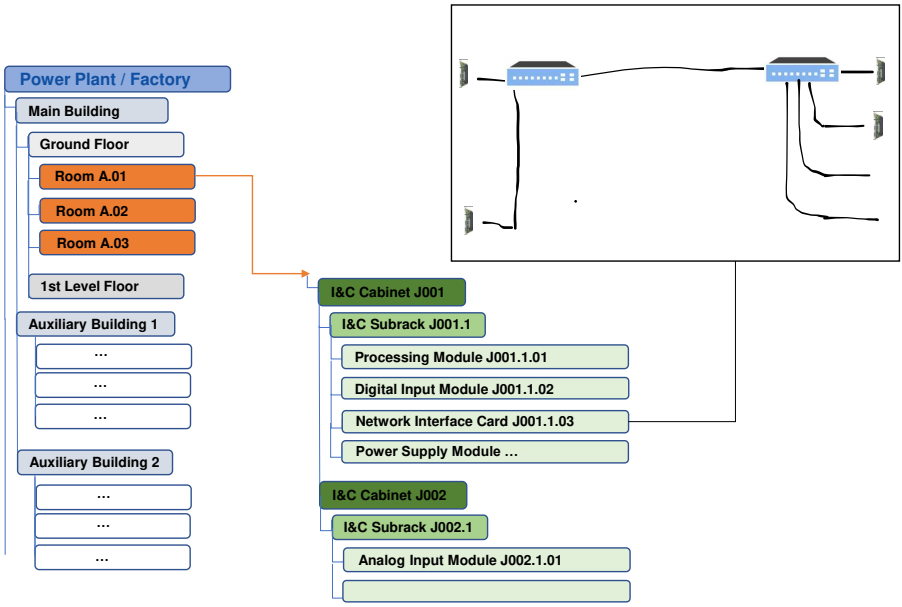

Figure 4: Assure UI top-level – tree view example

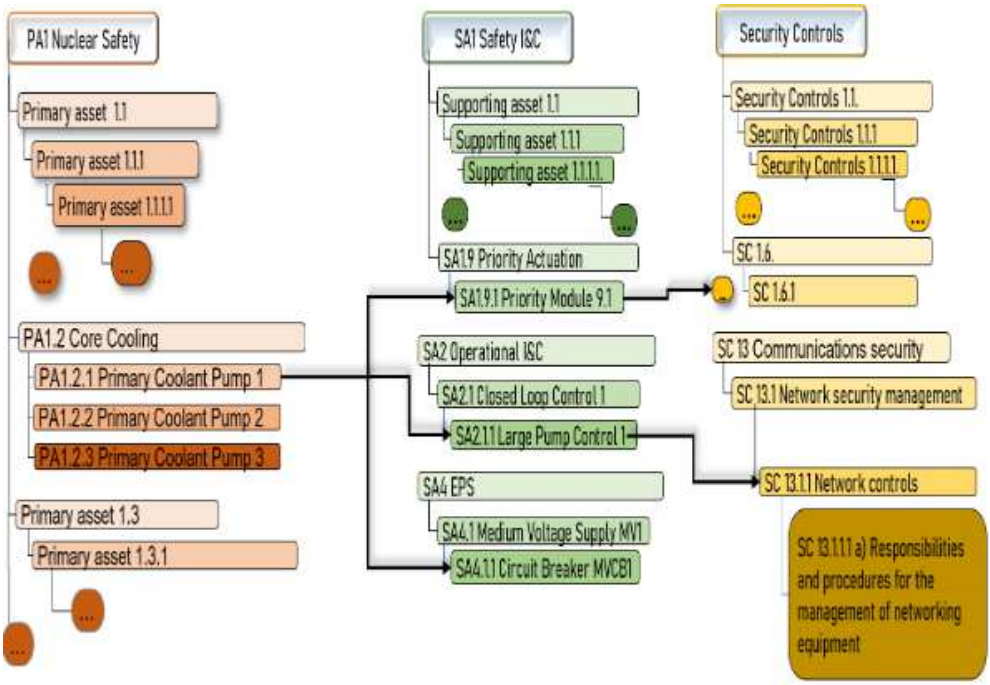

Figure 5: Interaction among primary assets, supporting assets and security control

The diagram in Fig. 5 illustrates all assets and their relationships.Several types of security controls are available, such as: categories - objectives - security controls - security sub-controls.For example: Communications Security - Network Security Management - Network Controls - Responsibilities and Procedures for Managing Network Equipment). However, assets are exposed to potential attacks, so it is critical to structure the primary and supporting assets so that a target security level can be assigned to the primary assets so that security controls are properly modeled and implemented.

4 Web Framework

4.1 Definition within the intended industrial application scope

A framework is a structure that you can build software on. Vue.js 3 proved once again how simple and fast JavaScript frameworks can and should be. Whether professional app development or in the private sector - Vue.js has many industry proponents and is becoming increasingly industry mainstream [Jos21]. With Vue.js version 3, many new features and optimizations appeared that raise the JavaScript framework to a new level. No

wonder many consider Vue.js one of the easiest and most accessible frameworks. For example, Vue allows direct support for HTML templates, while tools like React still have to define Digital Optics Monitoring (DOM) elements and use JavaScript for this. It provides various tools to help the developer in his work. This is not only about the different graphical elements, but also about what happens in the background.One of the main advantages of Vue.js is its ability to provide very simple responsive two-way data binding for custom form inputs and Vue components. There are also special libraries (that can be used in Vue.js) that provide pre-built components, graphical elements (controls) (Matthias Jost, 2021). Because Vue 3 is smaller and faster than Vue 2, it provides some low impact APIs and offers improved TypeScript support and a more maintainable code base[Sto17].

4.2 Graphical User interface of the considered Web Framework

A graphical user interface (GUI) is an interface that allows the user to interact with various electronic devices and industrial processes using icons and other visual indicators. The graphical user interfaces were created because the command line interfaces were quite complicated and it was difficult to learn all the commands they contained. Also, the visual feedback and structuring are essential for scalability. Within this paper, the library Elementplus will be used to create to design the GUI of the considered Web Framework. Element Plus is a component library offering a cool design language, many customization options and detailed documentation. It builds on Vue 3.0 for developers, designers and product managers and uses TypeScript, the composition API to create a better experience for developers.[Plu]

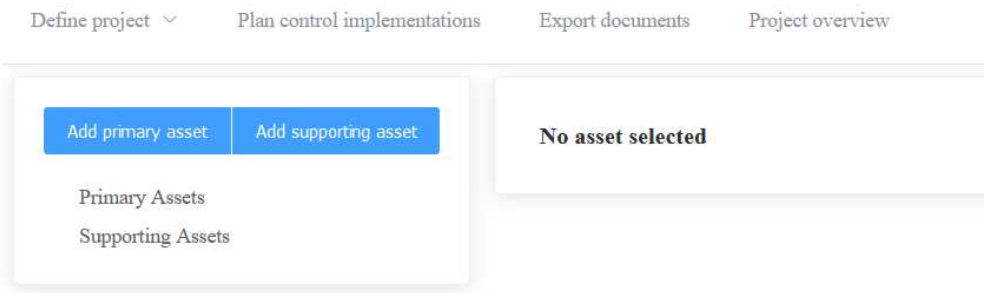

Figure 6: Initial Minimalist Graphical User Interface

5 Bi-directional Data Binding

When a bidirectional data binding is requested, the runtime environment retrieves the source value and initializes the specified target property with that value. Each time the source value changes, the data binding retrieves the new value and reinitializes the target property. When

the value of the target property changes, for example, when the user makes an input to an edit control, the data binding retrieves the new value of the target property and transfers it back to the source. The two-way data binding is the default type of data binding[Mic22]. The bi-directional data binding is especially important when multiple clients (as indicated in Fig. 7) are simultaneously modelling security artefacts of a plant or factory.

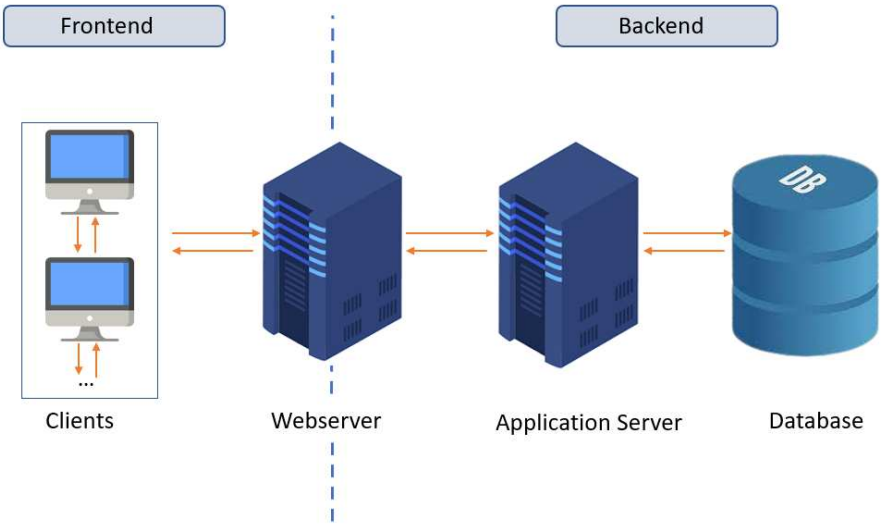

Figure 7: Bi-directional Data Binding

5.1 Backend data management

MongoDB is an open source, non-relational database management system (DBMS) that uses flexible documents instead of tables and rows to process and store various types of data. It is a schema-free document database written in C++, which is being developed in an open source project primarily run by 10gen Inc, that also provides professional services related to MongoDB. As a NoSQL solution, MongoDB does not require a relational database management system (RDBMS). Therefore, it provides an elastic data storage model that allows multivariate data types to be easily stored and queried by users. This not only simplifies database management for developers, but also creates a highly scalable environment for cross-platform applications and services. The main goal of MongoDB,

according to its developers , is to bridge the gap between fast and highly scalable key/value stores and feature-rich traditional RDBMSs (Relational Database Management Systems). MongoDB databases are located on a MongoDB server, which can host several such databases that are independent of each other and stored separately by the MongoDB server. Typically, a database contains one or more collections consisting of documents. A number of database security credentials can be defined to control access to the database. [DB]

5.2 The IoT Attack Lifecycle

The attack lifecycle describes the process by which attackers can typically gain access to organizations, their networks, systems and data.

Figure 8: Stages of the IoT attack lifecycle [Pal22]

6 Scalability of Graphical Front-end

Scalability generally refers to the ability of an organization, network, or process to evolve and be able to keep up with increased demand. Scalability is one of the most critical requirements for the success of a web application. When a company's front-end becomes scalable, it automatically gains an advantage over its competitors because it can now easily adapt to the changing needs of customers and/or consumers. This not only shows that the company is competitive, but also that it is stable and ready to deal with a sudden surge in demand, changing needs and trends, and the appearance of new competitors in the market.

7 Conclusion

The progress of digitalization is accompanied by various solutions in the field of automation. Cybersecurity plays a first-class role not only in Industry 4.0, but also in all IT areas because without cybersecurity, digitization will not be successful. Security measures aim to protect the confidentiality, integrity and availability of an IT system from being compromised by deliberate or accidental attacks. process and security improvement Security improvement must be a continuous activity. Cybersecurity must be a priority for Industry 4.0 organizations, from manufacturers to critical national infrastructure. The structured, scalable and interactive representation of security artefacts for simultaneous use by multiple cybersecurity team members is intended to cater towards more comprehensive and more effective planning, implementation and tracking of cybersecurity related artefacts.

Literatur

[22] *ISO/IEC 27005:2022 -Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. en. Standard. International Organization for Standardization, 2022. URL: https://www.iso.org/standard/80585.html.

[Beh17] Jan Odenbach Dr. Edgar Göll Dr. Siegfried Behrendt. „Industrie 4.0 – digital-vernetzte dezentrale Produktion“. In: *https://www.researchgate.net/* 47 (Jan. 2017).

[DB] MONGO DB. *Build faster Build smarter*. URL: https://www.mongodb.com/docs/manual/introduction/.

[Her08] Christof Hübner Hermann Merz Thomas Hansemann. *Building Automation*. 2008. ISBN: 978-3-410-16760-0. DOI: https://10.1007/978-3-319-73223-7. URL: https://link.springer.com/book/10.1007/978-3-319-73223-7.

[Jos21] Matthias Jost. *Enthusiastic About Software Development*. 2021. URL: https://www.matthias-jost.ch/warum-vuejs-einfach-erlernbar-ist/#:~:text=Vue.js%20dient%20dazu%20grafische%20Oberfl%C3%A4chen%20%28Frontends%29%20f%C3%BCr%20Webapplikationen,grafischen%20Elemente%2C%20sondern%20darum%2C%20was%20im%20Hintergrund%20passiert..

[Kie13] Jan U. Kieß. *Objektorientierte Modellierung von Automatisierungssystemen*. 2013. URL: https://link.springer.com/book/10.1007/978-3-642-79905-1.

[Mic22] Microsoft. *Data Binding*. 2022. URL: https://docs.microsoft.com/en-us/dotnet/desktop/wpf/data/?view=netdesktop-6.0.

[Pal22] Palaolto. *Impacts of Cyberattacks on IoT Devices*. 2022. URL: https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/research/impacts-of-cyberattacks-on-iot-devices.

[Ple19] Valentin Plenk. *Grundlagen der Automatisierungstechnik kompakt*. 2019. ISBN: 978-3-658-24469-9. URL: https://link.springer.com/book/10.1007/978-3-658-24469-9.

[Plu] Element Plus. *Element Plus - a Vue 3 based component library for designers and developers*. URL: https://element-plus.org/en-US/.

[Pre16] Giovanni Prestifilippo. *Auswirkungen von Industrie 4.0 auf Warehouse-, Transport- und Supply-Chain-Management-Systeme*. Springer, 2016. ISBN: 978-3-662-53250-8.

[Sto17] Christopher Stock. *A Review Paper on Botnet and Botnet Detection Techniques in Cloud Computing*. 2017. URL: https://blog.mayflower.de/6135-typescript.html.

[Vet82] Günter Vettin. In: *Verfahren zur technischen Investitionsplanung automatisierter flexibler Fertigungsanlagen*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1982, S. 130–138. ISBN: 978-3-642-81904-9. DOI: 10.1007/978-3-642-81904-9_11. URL: https://doi.org/10.1007/978-3-642-81904-9_11.

[Wik22] Wikipedia. *Industrial internet of things*. Juni 2022. URL: https://en.wikipedia.org/wiki/Industrial_internet_of_things.

[Wit22] Christoph Witte. *A Review Paper on Botnet and Botnet Detection Techniques in Cloud Computing*. 2022. URL: https://it-rebellen.de/2019/01/16/bedenkliche-einstellung-zur-cybersecurity-von-industrieanlagen-risiken-werden-unterschaetzt/.