Mälardalen University Doctoral Dissertation 391

Dynamic Access Control for Industrial Systems

Björn Leander

Mälardalen University

Mälardalen University Press Dissertations
No. 391

DYNAMIC ACCESS CONTROL FOR INDUSTRIAL SYSTEMS

Björn Leander

2023

School of Innovation, Design and Engineering

ISBN 978-91-7485-616-3
ISSN 1651-4238
Printed by E-Print AB, Stockholm, Sweden

Mälardalen University Press Dissertations
No. 391

DYNAMIC ACCESS CONTROL FOR INDUSTRIAL SYSTEMS

Björn Leander

Akademisk avhandling

som för avläggande av teknologie doktorsexamen i datavetenskap vid
Akademin för innovation, design och teknik kommer att offentligen försvaras
fredagen den 8 december 2023, 13.00 i Beta, Mälardalens universitet, Västerås.

Fakultetsopponent: Doctor Marina Krotofil, ISSP

Akademin för innovation, design och teknik

Abstract

Industrial automation and control systems (IACS) are taking care of our most important infrastructures, providing electricity and clean water, producing medicine and food, along with many other services and products we take for granted. The continuous, safe, and secure operation of such systems are obviously of great importance. Future iterations of IACS will look quite different from the ones we use today. Modular and flexible systems are emerging, powered by technical advances in areas such as artificial intelligence, cloud computing, and motivated by fluctuating market demands and faster innovation cycles. Design strategies for dynamic manufacturing are increasingly being adopted. These advances have a fundamental impact on industrial systems at component as well as architectural level.

As a consequence of the changing operational requirements, the methods used for protection of industrial systems must be revisited and strengthened. This for example includes access control, which is one of the fundamental cybersecurity mechanisms that is hugely affected by current developments within IACS. The methods currently used are static and coarse-grained and therefore not well suited for dynamic and flexible industrial systems. A transition in security model is required, from implicit trust towards zero-trust, supporting dynamic and fine-grained access control.

This PhD thesis discusses access control for IACS in the age of Industry 4.0, focusing on dynamic and flexible manufacturing systems. The solutions presented are applicable at machine-to-machine as well as human-to-machine interactions, using a zero-trust strategy. An investigation of the current state of practice for industrial access control is provided as a starting point for the work. Dynamic systems require equally dynamic access control policies, why several approaches on how dynamic access control can be achieved in industrial systems are developed and evaluated, covering strategies for policy formulations as well as mechanisms for authorization enforcement.

ISBN 978-91-7485-616-3
ISSN 1651-4238

Abstract

Industrial automation and control systems (IACS) are taking care of our most important infrastructures, providing electricity and clean water, producing medicine and food, along with many other services and products we take for granted. The continuous, safe, and secure operation of such systems are obviously of great importance. Future iterations of IACS will look quite different from the ones we use today. Modular and flexible systems are emerging, powered by technical advances in areas such as artificial intelligence, cloud computing, and motivated by fluctuating market demands and faster innovation cycles. Design strategies for dynamic manufacturing are increasingly being adopted. These advances have a fundamental impact on industrial systems at component as well as architectural level.

As a consequence of the changing operational requirements, the methods used for protection of industrial systems must be revisited and strengthened. This for example includes access control, which is one of the fundamental cyber-security mechanisms that is hugely affected by current developments within IACS. The methods currently used are static and coarse-grained and therefore not well suited for dynamic and flexible industrial systems. A transition in security model is required, from implicit trust towards zero-trust, supporting dynamic and fine-grained access control.

This PhD thesis discusses access control for IACS in the age of Industry 4.0, focusing on dynamic and flexible manufacturing systems. The solutions presented are applicable at machine-to-machine as well as human-to-machine interactions, using a zero-trust strategy. An investigation of the current state of practice for industrial access control is provided as a starting point for the work. Dynamic systems require equally dynamic access control policies, why several approaches on how dynamic access control can be achieved in industrial systems are developed and evaluated, covering strategies for policy formulations as well as mechanisms for authorization enforcement.

Sammanfattning

Vi tar för givet att det alltid ska finnas el, rent dricksvatten, mat och läkemedel. Många av våra grundläggande behov tillgodoses tack vare produkter som är beroende av industriella styrsystem. Att skyddas dessa system ifrån störningar är följaktligen ytterst viktigt.

Vi är mitt i ett teknikskifte som brukar kallas "Industri 4.0" och som innebär att framtidens industriella system kommer skilja sig avsevärt ifrån dagens. Förändringen drivs bland annat av nya krav och förväntningar, exempelvis på kortare tid mellan idé och produktion, möjlighet att anpassa produktionen till snabba marknadsförändringar och tillverkning av individuellt anpassade produkter. Flexibla och skalbara lösningar krävs för att kunna uppfylla dessa krav, till skillnad från dagens system som i allmänhet är utvecklade för massproduktion av en specifik produkt.

Detta påverkar såväl hur produktionssystemen konstrueras som designen av varje ingående komponent. En konsekvens är att metoderna som används för att skydda dagens system måste anpassas och stärkas för att möta framtidens utmaningar. En grundläggande sådan säkerhetsfunktion är behörighetshantering. Nuvarande behörighetshantering är inte tillräckligt flexibel och därmed dåligt anpassad till morgondagens dynamiska system.

I denna doktorsavhandling undersöks behörighetshantering för framtidens industriella system, med fokus på de dynamiska produktionssystem som behövs för att uppfylla kraven kopplade till Industri 4.0. Med utgångspunkt från en enkätundersökning analyseras dagsläget. Förslag på flera olika tillvägagångssätt för dynamisk behörighetshantering presenteras och utvärderas, såväl med avseende på hur sådana regler kan formuleras som på hur de ska kunna upprätthållas.

Acknowledgments

First, to my family, Linnea, Hugo, Nike and Teo, thank you for your patience, and for making my life interesting and fun! Siv and Lars, my dear parents, thank you for guidance, advice and your life-long support.

I want to express my greatest gratitude toward my supervisors Hans Hansson, Aida Čaušević, and Tomas Lindström, thank you for unwavering support, invaluable guidance and trust in my abilities. You have shared your knowledge and helped me to grow as a researcher.

Pursuing a PhD is quite a lonely job - most of the work is done by and for yourself. I have had the luck of having a lot of great colleagues at ABB and MDU, many of you are also co-authors and teachers. Bjarne, Tijana, Sasi, Bahar, Miguel, Adnan, Van-Lan, Åsa, Abbas, Shamoona, Robbert, Anders, Henrik, Mohammad, Saad, Ines, Mats, Thomas - thank you for friendship, good discussions, company, ideas, and the joint work.

I have had the privilege of supervising four master students through their thesis projects. Both thesis projects ended up as published scientific articles, one of which is included in this PhD thesis. Selma, Lejla, Enna, and Ivan, thank you for your curiosity and contributions! Similarly awarding were the three seasons of summer internships which I supervised, and which all provided tangible technical contributions to the *Modular Ice-cream Factory*. Abhinav, Gloria, Andreas, Filip, Ivan and Enna, thank you for the good cooperation!

Aside from work and family, a lot of my life revolves around music - and the vast majority of my friends (and family) are also co-musicians or otherwise engaged with music. Playing or listening to music is the best way to relax, remove stress, etc - which has aided me in staying focused and sane throughout this PhD project. Linnea, Tommy, Erik, Jenny, Anton, Mats E, Leo, Mats H, Anders, Helena, Hugo, Thomas, Jan, Claes, all in VBB and VSMK, etc., thank you so much for joining my music projects, and letting me join yours. I hope

for a lot of great joint musical experiences in the future!

My research has been conducted as an industrial PhD project, supported by ABB Process Automation, with the academic support from Mälardalen university through the industrial postgraduate program Automation Region Research Academy (ARRAY) funded by the Swedish Knowledge foundation (KKS). Further funding is provided by the Horizon 2020 project Intelligent Secure Trustable Things (InSecTT), funded by the European Commission and Vinnova under grant agreement No 876038.

The usual disclaimer: This thesis reflects only my view, and the Commission is not responsible for any use that may be made of the information it contains.

Björn Leander
Västerås, November 2023

List of Publications

Publications included in thesis[1]

Paper A: *A Questionnaire study on Access Control for Industrial Systems*, **Björn Leander**, Aida Čaušević, Hans Hansson, Tomas Lindström, 26th International Conference on Emerging Technologies and Factory Automation, ETFA, Västerås, Sweden, Sept. 2021.

Paper B: *Towards an ideal Access Control Strategy for Industry 4.0 Manufacturing Systems*, **Björn Leander**, Aida Čaušević, Hans Hansson, Tomas Lindström, In IEEE Access journal, Aug. 2021.

Paper C: *Access Control Enforcement Architectures for Dynamic Manufacturing Systems*, **Björn Leander**, Aida Čaušević, Hans Hansson, Tomas Lindström, 20th IEEE International Conference on Software Architecture, ICSA, L'Aquila, Italy, March 2023.

Paper D: *Simulation Environment for Modular Automation Systems*, **Björn Leander**, Tijana Marković, Aida Čaušević, Tomas Lindström, Hans Hansson, Sasikumar Punnekkat, 48th Annual Conference of the Industrial Electronics Society, IECON, Brussels, Belgium, Oct. 2022.

Paper E: *Evaluation of an OPC UA-based Access Control Enforcement Architecture*, **Björn Leander**, Aida Čaušević, Tomas Lindström, Hans Hansson, 28th European Symposium on Research in Computer Security, ESORICS, 9th CyberICPS Workshop, Hague, Netherlands, Sept. 2023.

Paper F: *An Authorization Service supporting Dynamic Access Control in Manufacturing Systems*, Ivan Radonjić, Enna Bašić, **Björn Leander**, Tijana Marković, IEEE 9th World Forum on Internet of Things, Aveiro, Portugal Oct. 2023.

[1]The included publications have been reformatted to comply with the thesis layout.

Publications not included in thesis

Paper X1: *Classification of PROFINET I/O Configurations utilizing Neural Networks*, Bjarne Johansson, **Björn Leander**, Aida Čaušević, Alessandro Papadopoulos, Thomas Nolte, 24th International Conference on Emerging Technologies and Factory Automation, ETFA, Zaragoza, Spain, Sept. 2019 [28].

Paper X2: *Anomaly Attack Detection in Wireless Networks Using DCNN*, Van-Lan Dao, **Björn Leander**, IEEE 8th World Forum on Internet of Things, Yokohama, Japan, Oct. 2022 [13].

Paper X3: *Ice Cream Factory Dataset and Performance of Machine Learning Algorithms for Fault Detection*, Tijana Markoivć, Miguel Leon, **Björn Leander**, Sasikumar Punnekkat, In IEEE Access journal, Feb. 2023 [45].

Paper X4: *Developing and Evaluating MQTT Connectivity for an Industrial Controller*, Selma Opačin, Lejla Rizvanović, **Björn Leander**, Saad Mubeen. 8th IEEE Cyber Physcal Systems & Internet of Things conference CPS&IoT, Budva, Montenegro, June 2023 [53].

Paper X5: *Dependability and Security Aspects of Network-Centric Control*, **Björn Leander**, Bjarne Johansson, Tomas Lindström, Olof Holmgren, Thomas Nolte, Alessandro Papadopoulos. 28th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Sinaia, Romania, Sept. 2023 [41].

Paper X6: *Enhanced Simulation Environment to Support Research in Modular Manufacturing Systems*, **Björn Leander**, Tijana Markoivć, Miguel Leon. 49th Annual Conference of the Industrial Electronics Society, IECON, Singapore, Oct. 2023 [42].

Book chapter: *InSecTT technologies for the enhancement of industrial security and safety*, The InSecTT Book, 2023, Sasikumar Punnekkat, Tijana Markoivć, Miguel Leon, **Björn Leander**, Alireza Dehlaghi-Ghadim, Per Erik Strandberg.

Patent Application 1: *Access Control Within A Modular Automation System*, (EU EP20171980.4, US20210341894A1, 2021), **Björn Leander**.

Patent Application 2: *Fine-grained access control enforcement for industrial control systems using tokens, combining static roles with explicit permissions*, (EU EP22155487.6, 2022, US20230254320A1, 2023), **Björn**

Leander, Tomas Lindström.

Licentiate Thesis: *Access Control Models to secure Industry 4.0 Industrial Automation and Control Systems*, **Björn Leander**, Licentiate Thesis no. 296, Mälardalen University, 2020 [39].

Contents

Part I

Thesis

Chapter 1

Introduction

Industrial automation and control systems (IACS)[1] are used to operate a wide range of industrial applications including critical infrastructure, such as power plants and clean water supplies [75]. The safe and secure operations of these systems are crucial for system owners from a business perspective, for private persons relying on reliable services and safe products, and for the society as a whole for supply of critical resources and as a basis of economic growth and stability.

Since the beginning of industrialization, the manufacturing systems have gone through several revolutionary developments, from the steam-powered spinning machine in the 18th century to computerized automatic control in the 1990s, further described in Chapter 2.1. Today, many people talk about the fourth industrial revolution, which is a collective name for a number of trends and emerging characteristics defining the future of industrial manufacturing.

The envisioned technical manufacturing systems are expected to be dynamic and flexible to support a market- and innovation-driven production. When a plant is constructed, it needs to be prepared for changing functionality over time to fulfill shifting production requirements. Different design strategies on the technical system level are currently emerging to support this, with many of the solutions taken from the IT-domain, e.g., using a service-oriented approach both for manufacturing modules and digital services. Allowing these kinds

[1] Industrial Systems we define as any computerized system used for industrial purposes, e.g., including vehicular systems, telecommunication systems, etc. IACS is a subset of industrial systems, and includes systems for automation and control of physical industrial processes. In some of the included papers the terms *industrial automation system* and *industrial control system* is used almost interchangeably with IACS.

of flexible and dynamic scenarios requires novel solutions for the industrial systems, with availability and interoperability of networked industrial services as key requirements. Technical trends in industrial system architectures and design patterns are further described in Chapter 2.2.

Safe and secure operation of IACS is of great importance, and the selection of protective mechanisms must be aligned with the system requirements as well as with the current threat landscape. When automated factories emerged at the 70s, the major threats against the system were in the form of physical sabotage, and therefore the physical security in the form of locked gates, fences, etc., have been introduced as the most effective protective mechanisms (chap. 3 in [29]). Since then, the systems have evolved and become more networked and connected, resulting in threats on the digital plane being increasingly important to handle and counter. Current threats and security mechanisms for IACS are further described in Chapter 2.3.

As the industrial systems and the context in which they operate are changing, there is a need to investigate which protective mechanisms are required to counter the current threats. The security model used within IACS has for several years mainly been based on implicit trust, meaning that an entity (physical or digital) is trusted based on an implicit property such as being connected to a certain network and able to communicate using a specific protocol. The model works if everyone behaves well on the network but provides little protection against insider threats, malware, lateral movements, etc. To handle the reality of a more complex and cyber-hostile world, the *zero-trust* [62] model starts to be adopted to industrial systems. Using the zero-trust model, any interaction between entities are considered potentially malicious, and must therefore be validated. Access control is an important method for achieving this.

Access control is one of the fundamental security mechanisms of digital systems, and encompasses identification, authentication, and authorization, i.e., methods for establishing identities, methods for proving identities, and methods for enforcement of rules on interactions between identified entities. These disciplines progressively depend on each other, authentication requires established identities, and authorization usually requires an authenticated user. The *principle of least privilege* is one of the main guidelines for access control [65] and stipulates that entities should hold no higher privileges than required to fulfill their tasks in the system. More background on access control is provided in Chapter 2.4.

The implicit trust model used in IACS of today emphasize identification, and some level of authentication, while authorization is often very coarse-grained.

This is not a viable approach for the envisioned dynamic manufacturing systems of the future, following from the principle of least privilege. Since these systems are dynamic to their nature, the access control solutions must be equally dynamic.

Several challenges arise related to including dynamic access control in industrial systems: (1) we need to know how to define rules that follow the dynamic behavior of the system, (2) we need to make sure that these rules are enforced within a complex and distributed system, and (3) we need to understand what impact these mechanisms have on the behavior of the system, so that the system still can perform its intended task. These are the challenges tackled in this PhD thesis.

1.1 Thesis scope & contributions

The scope of the thesis is to investigate solutions towards zero-trust in IACS. Specifically we focus on access control for dynamic and flexible manufacturing scenarios requiring fine-grained and flexible access control.

The PhD contributes with the following:

- A study of state of the practice and perceived challenges in access control in industrial systems, with the purpose to understand the industrial perspective and relevance of the research topic.
- An investigation of access control strategies for policy formulations in dynamic manufacturing systems, aiming to provide basis for selecting a suitable approach fit for the principle of least privilege.
- Definitions, approaches, and evaluations of enforcement architectures in dynamic manufacturing systems, with aim to implement efficient enforcement mechanisms in support of dynamic access control.
- Development of a testbed based on the modular automation design strategy, with the main goal to provide a demonstration environment for access control policy strategies and enforcement architectures.
- Implementation and evaluation of policy strategies as well as an enforcement architecture using the developed testbed, with the aim to quantify and compare quality metrics for suggested approaches.

Even though the presented approaches are developed with dynamic manufacturing in mind, they are using available industrial protocols and standards.

Therefore, they are applicable for other scenarios requiring fine-grained access control within industrial automation and similar systems.

Chapter 2

Background

This chapter provides background on the topics covered by this thesis. We start with a brief history on industrialization, followed by a description of current technical trends in industrial control system design and development, which are the main motivations behind the work of the thesis. As our goal is to provide solutions to improve the security of industrial automation and control systems, we summarize some aspects of state of the art in the area of industrial cybersecurity as part of the background. Lastly, as background to the specific focus on the thesis we introduce the basic concepts of the access control.

2.1 History of industrialization - evolution & revolutions

There is a distinction between the notion of a "revolution" as compared to a mere evolutionary development. A revolution is characterized by a stepwise fundamental change occurring under a relatively short amount of time, typically due to an accumulated amount of mutually reinforcing conditions.

Industry-scale manufacturing started in England during the 18th to early 19th century, with production of, e.g., cast iron and textiles. The introduction of steam engines for driving the manufacturing plants as well as a the transportation (e.g., steam ships and trains), were some of the driving factors behind *the first industrial revolution*. There were also economical changes driving the revolution such as accumulation of wealth from colonies which turned into capital to production plant owners. The industrial revolution was largely fueled by exploiting underpaid labor working in the factories and slaves producing the raw

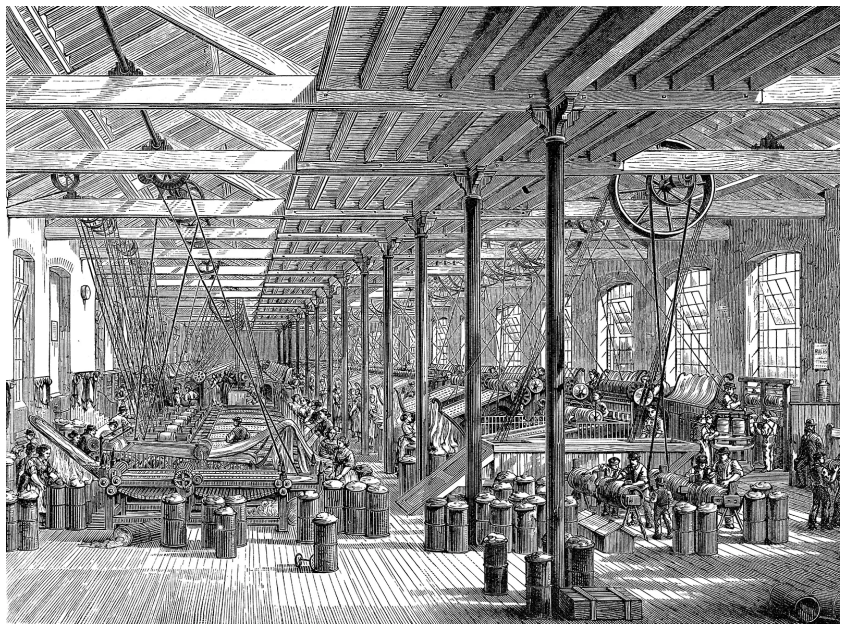


Figure 2.1: Engraving showing the factory floor of the spinning room in Shadwell Rope, 1878 [51]

materials, e.g., in the case of cotton fabrication, being an important branch of Britain's industrialization (in 1840 cotton fabric provided approximately 50% of Brittish exports [74]).

The second industrial revolution was a technical transition from steam to electrical powered machinery, occurring in the early 20th century, and was related to advances within steelmaking (e.g., the Bessemer process, patented 1856), the invention of electrical generators (by Siemens in 1867) and the hydro electric power station (the first public one in 1896, on the Niagara river). Power generation as well as propulsion using the internal-combustion engine implied a shift away from steam and coal.

The invention of the conveyor belt increased the manufacturing efficiency, first for cars and then for other products. In this era, true mass production of a range of goods has been introduced, making them cheaper and more easily accessible. The manufacturing machinery became increasingly complex during this period, implying a need for more qualified workforce, which increased the number of scholars and engineers involved in the production process.

Several technical advances were developed as part of the industrialization of

Figure 2.2: Workers on the first moving assembly line put together magnetos and flywheels for 1913 Ford autos, Unknown photographer, Highland Park, Michigan, National Archives, Records of the U.S. Information Agency (306-PSE-73-1534).

the military sector, due to the first and second world wars. However, in many places, the aftermath of the second world war initially implied an economical decrease, with a focus on rebuilding and restoring war-torn economies and preventing another depression. During this time the European domination on the global arena was largely diminished, with the liberation of the most of old colonies. The U.S became the largest economy, and much of the industrial achievements were driven by huge corporations seated there [74].

The third industrial revolution is related to the introduction of automation using computers and robotics in the production plants, with dirty, dull, and dangerous jobs no longer being performed by human labor. This revolution occurred in the mid 20th century, and implied a globalization of production, where a complete product contains components produced at one site, designed at another site and assembled at the third one. This revolution further decreased the need for blue-collar workers and changed the work requirements for the engineering staff. The technical systems of the third industrial revolution are the predominant ones currently in use.

If we can learn anything from this summary, it is that development in the industrial sector is very closely related to other trends and events in society, such

as the growth and decline of colonialism, war, politics, technical advances in seemingly unrelated sectors, etc. “History is merely a list of surprises. It can only prepare us to be surprised yet again.”[1]

2.2 Industrial control systems trends and characteristics

The fourth industrial revolution is expected to occur during the first half of the 21st century and implies a shift from automatic to autonomous control. The technological shift is fueled by introduction of internet technology, artificial intelligence, etc., in manufacturing facilities. Mass production is transformed into mass customization, and everything in production facilities is networked, including the products being produced. Industry 4.0 [38, 23, 44] is shaping the future of IACS, implying huge changes both from a business and technological perspective.

Dynamic manufacturing is a trend for supporting production systems with a high level of adaptability to shifting market demands. Industry 4.0 manufacturing systems rely on ubiquitous access to data - both on the distributed control level to be able to adapt and customize production, on supervisory level to be able to foresee maintenance needs, and up to the enterprise level to predict and adapt production to market requirements.

The Purdue Enterprise Reference Architecture (PERA) [78], illustrated in Figure. 2.3, was introduced in the early 1990s as a reference and methodology for computer integrated manufacturing systems. The hierarchical levels of the PERA architecture are widely used in current industrial automation and control systems, often referred to as the automation triangle. Level 0 represents the physical process including all physical, chemical, or spatial transformations. Level 1 represents basic control, including the sensors and actuators Input/Output signal connections to the controllers. Level 2 represents supervisory control and level 3 operations management. On the top of the pyramid, level 4, represents the enterprise systems.

In PERA, information and data flow accumulates one hierarchy level at a time, with real-time requirements increasing with a decreasing level, and amount of data increase with increasing level.

Network-centric control is a design strategy for Distributed Control Systems (DCS) which transitions away from the hierarchical architecture of PERA. It

[1] Kurt Vonnegut, from the novel *Slapstick*.

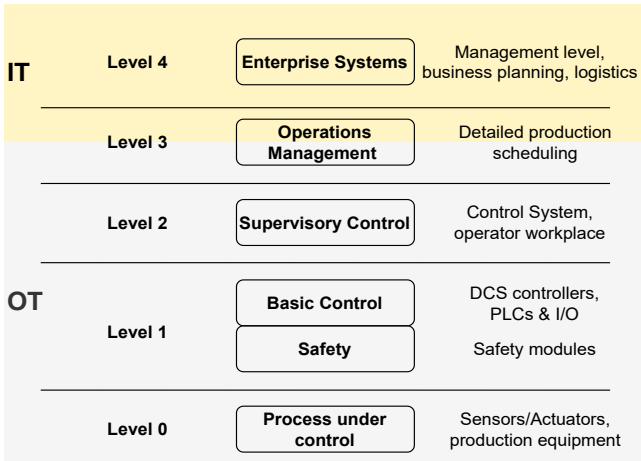
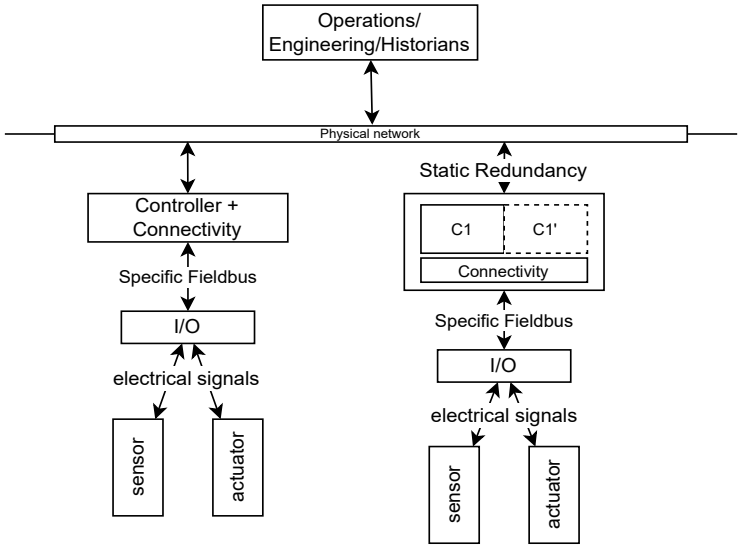


Figure 2.3: Illustration of the hierarchical levels of the Purdue Enterprise Reference Architecture (PERA)

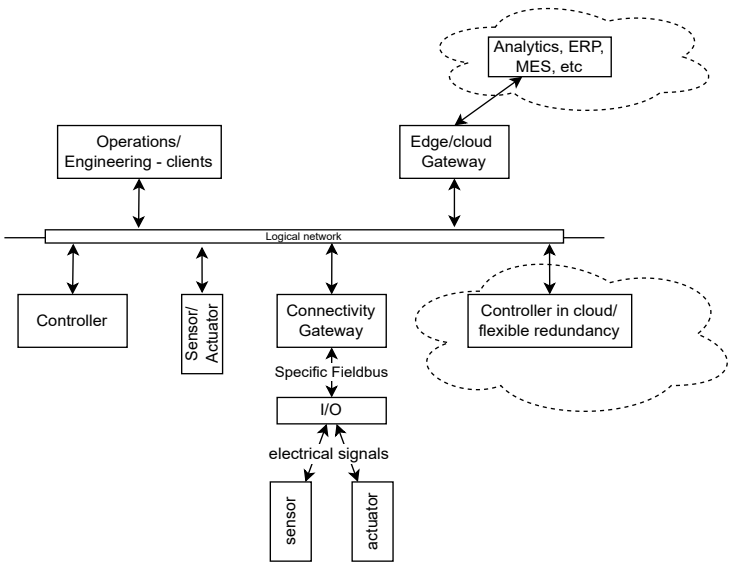
is partly described in the Open Process Automation standard (OPAS) [52], and [41]. In the predominant controller-centric architecture, illustrated in Figure. 2.4a, access to process signals is only possible through a controller, i.e., a controller *owns* a set of Input/Output (I/O) signals. This allows for very strict real-time requirements, but puts limitations on flexibility, e.g., when it comes to redundancy solutions. In a network-centric control, illustrated in Figure. 2.4b, a service-oriented approach is used, all the way down to access to I/O, which allows a high flexibility on deployment of control, connectivity, redundancy, as well as the high level functionalities of the PERA architecture.

Dynamic manufacturing is a production systems development related to Industry 4.0. Current manufacturing systems are typically static and have been largely optimized for high-volume production to a low per-item cost. This has led to highly specialized and optimized factories with a high complexity. These factories are difficult and expensive to retrofit for changing demands or requirements.

Smart manufacturing [48, 14] and modular automation [84, 36, 68] are examples of system types/design strategies for dynamic manufacturing. These systems are optimized for being adaptable and customizable, in order to easily ramp up or decrease production, adapt to new innovations or specific customer requirements, etc. The resulting systems are dynamic manufacturing environments, which exhibit different levels of dynamicity, e.g., for modular automation:



(a) A controller-centric architecture.



(b) A network-centric architecture.

Figure 2.4: Example architectures for network- and controller-centric design models respectively, from [41].

1. Dynamic system composition - available physical processing modules and how they are interconnected will change over time, due to changing

high-level production requirements.

2. Dynamic production schemes - available and active recipes describing the production workflow and daily synchronization change, based on business requirements.

3. Dynamic operations - during recipe execution, different steps of the recipe-workflow are activated, implying execution of different processing operations.

Dynamic manufacturing is easier to achieve by using the network-centric approach described above, since with this approach the flexibility and dynamicity required on the manufacturing level is supported by a service oriented and flexible architecture.

2.3 Cybersecurity in industrial control systems

As mentioned, traditional industrial automation systems of the third industrial revolution are being built based on strict hierarchical segregation between levels (in PERA) and zones in the network [2]. In this architecture, physical and logical perimeter protection and security zoning are the main cybersecurity mechanisms, especially at the lower levels (0-1), i.e., close to the physical process. Used protocols at this level, such as Manufacturing Message Specification (MMS) [67], PROFINET [58], MODBUS TCP[2], etc., are developed without much security functionality. At these levels, an entity is basically trusted based on its location, e.g., what network it is connected to. At the middle levels (2-3), including, e.g., operations and engineering, the client layer of applications are typically where security functions are implemented, i.e., authentication and authorization. The top levels, (4 and part of 3), are part of office networks, and therefore security functionality and mechanisms from Information Technology (IT) are being used there.

A clear separation between Operational Technology (OT) (levels 0-3), and IT (level 3-4) used to be the norm (chap. 3 and 9 in [29]). There is an ongoing trend toward convergence between IT and OT [31], with the introduction of IT components within the OT network, and a growing amount of interconnections between the IT and OT networks. This convergence is accelerated by the Industry 4.0 paradigm.

[2] `modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf`

Among industrial communication protocols there are several examples of secure variants, mainly Ethernet-based protocols, e.g., MODBUS TCP Security[3] and Open Process Communication Unified Architecture (OPC UA) [27]. OPC UA supports service-oriented architectures, include certificate-based authentication and secure communication, and provides solutions for authorization, making it a very interesting protocol for future IACS.

Cybersecurity legislation and standardization: When developing, deploying and operating IACS, standardization plays an important role for utilization of cybersecurity mechanisms [17, 59]. For certain industries, asset owners are required to follow a specific cybersecurity regulation (e.g., NERC CIP[4]), product suppliers may be requested to fulfill specific certifications (e.g., SDLA[5], CSA[6], Common Criteria[7], etc.), usually prescribed by industrial standards, such as IEC 62443 [26].

Within the European Union, the second iteration of the directive on security of network and information systems (NIS2)[8] is coming into effect during 2024. The directive implies legislative requirements on cybersecurity management and incident handling for critical infrastructure and services, covering a wide range of industrial systems such as energy, health, drinking water, chemical and food manufacturers.

Emerging threats, trends in attacks: A cybersecurity attack, a failure or a threat related to an industrial automation and control system can have severe impact. It may cause economic harm, it could have safety implications on equipment and personnel, it could have environmental impact, and it may pose a threat to the society in the form of outage of, e.g., power or clean water supply.

All these scenarios have materialized in the form of different attacks [22], and in recent years, there has been a steady trend of increasing amounts of cyber-attacks on IACS [73, 47]. Many incidents and attacks are never discovered, and only a few are publicly disclosed, so there is likely a considerable amount of hidden statistics regarding the magnitude of this problem. A few attacks are well described, with *Stuxnet* [19, 34] being a wake-up call for the existence of targeted cyber-attack inflicting physical harm on industrial systems, although

[3] `modbus.org/docs/MB-TCP-Security-v21_2018-07-24.pdf`
[4] North American Electric Reliability Corporation, Critical Infrastructure Protection
[5] ISASecure certification - Secure Development Lifecycle Assessment
[6] ISASecure certification CSA - Component Security Assessment
[7] Common Criteria for Information Technology Security Evaluation ISO/IEC 15408
[8] `digital-strategy.ec.europa.eu/en/policies/nis2-directive`

not being the first such example. The *Wannacry* [49] ransomware attack (collateral effects on industrial systems), *Maroochy* [72] waste-water incident and the *BlackEnergy3* and *Crash Override* [47] attacks on the Ukrainian energy sector are other examples of known attacks having a tangible impact on industrial systems.

The Zero-trust model is originally a response to the Bring Your Own Device (BYOD) trend in enterprise networks, embodied by the widespread use of e.g., personal cellphones, tablets and smart watches at work [62], connected to office networks, and has had a big impact on the IT world in general, especially related to protection of cloud-hosted services and other internet-facing solutions.

Zero-trust implies that trust is never granted implicitly but must be evaluated continually, with the goal to prevent unauthorized access to resources. For example, this implies:

- Interaction between digital entities shall be checked both on sending and receiving side, to securely identify and authenticate communicating parties.
- Access to resources must be intelligently evaluated for permissions.
- Communication between authenticated parties must be at least integrity-protected, and possibly encrypted, as the threat-actor may be located in intermediate network nodes.

The technological advances and evolving characteristics of IACS, as well as the increasingly hostile environment with regards to cyber-threats, imply the need of redefining the trust-models used, with zero-trust as viable model also for these systems [83]. Minimizing the implicit trust-zones makes fine-grained access control a necessity.

2.4 Access Control

Access Control Fundamentals: Access control is one of the most prominent security mechanisms in an information system and aims to limit what is allowed to be done in a system based on a set of well-defined rules. Access control can be separated into three major disciplines: identification, authentication and authorization. Identification covers the practice of establishing identities for subjects and resources in the system, authentication provides the mechanisms for providing proof of identity, and authorization is concerned

with describing rules for if, how, and when a certain subject can access a certain resource. These three disciplines are incrementally dependent on each other, i.e., identification is prerequisite for authentication and authentication is a prerequisite for authorization.

The focus of this thesis is mainly on authorization, implying that there are already sufficiently trustworthy methods of identification and authentication implemented in the system. Several rather well-established mechanisms for identification and authentication are starting to be used in industrial control systems, e.g., based on device certificates, user identity tokens, etc. However, it is still an area of active research and development, e.g., related to certificate distribution [24, 61], and secure device provisioning [16, 33].

Some basic guidelines of authorization, as defined by Saltzer *et al.* [65], are:

- *Principle of least privilege*: No subject should hold higher privileges in a system, than what is required for it to perform its required tasks.
- *Principle of full mediation*: All operations related to accessing a resource shall be mediated by a resource monitor that makes and enforces policy decisions.
- *Separation of duties*: Different subjects should have different tasks, e.g., an administrator should not also be an application user.

Sandhu *et al.* [66] describe authorization as being comprised of models at three different layers, **P**olicy, **E**nforcement, and **I**mplementation (PEI). The PEI-model is illustrated in Figure. 2.5. Policy models are used to formalize high level access control requirements, enforcement level models describe how to enforce these policies from a systems perspective, and the implementation level models show how to implement the components and protocols described by the enforcement model. In short, we can say that P-models decide what requirement can be described, whereas the E- and I-models describe how to enforce the requirements.

Policy Enforcement Architecture: A policy enforcement architecture is useful when describing what mechanisms are needed, where they are placed and how they interact. One of the most used reference architectures for policy enforcement is the one described in the specification for the eXtensible Access Control Markup Language [79, 25], illustrated in Figure. 4.2c.

Policy Models: Historically, Mandatory Access Control (MAC) and Discretionary Access Control (DAC) have been the two main policy models within access control. MAC is traditionally connected with Multi-Level Security,

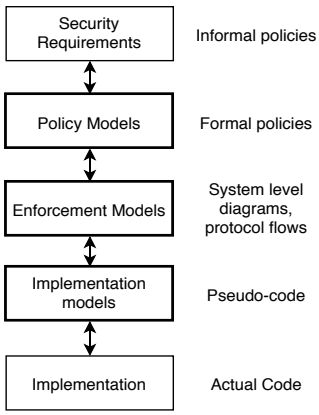


Figure 2.5: A PEI-model [66]

based on security classifications on resources, combined with security clearances for subjects, e.g., top-secret content only readable for subjects with the highest security clearance. MAC used in operating systems or database management implies centrally controlled policies for system resources. In DAC on the other hand, the privileges are defined as a relation between the resource and subject, often with the subject allowed to transfer its privileges. Role-Based Access Control (RBAC) is building on principles from both DAC and MAC, where subjects have one or several roles that may be hierarchically ordered. Privileges are derived from the roles rather than from the subject. Currently RBAC is the most widely used model for access control [12], being used e.g., in the Windows Active Directory.

Dynamic Access Control: There are two main branches for policy model families that support dynamic access control: Attribute Based Access Control (ABAC) [82] and Task Based Access Control (TBAC) [76].

In ABAC, the dynamic behavior is achieved by expressing the policy rules as logical functions of attributes of the subject, resource, and environment respectively. For example, it is possible to express a rule that says a person has the right to control and supervise signals related to a section of a plant if the person is in the team of operators responsible for this section, given that it is during working hours and the person is on premise.

In TBAC, the policy decisions are instead based on knowledge of active workflows within the system, so that only actions in line with available workflows are allowed. This requires the entity making policy decisions to also execute a model of workflows to understand what actions can be taken, and what transi-

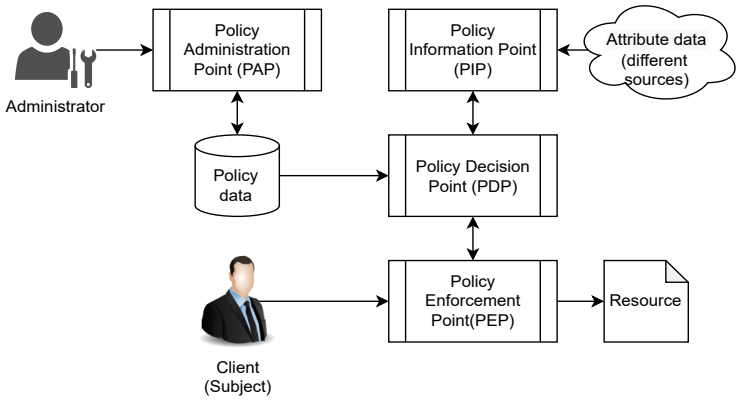


Figure 2.6: Elements of the XACML reference enforcement architecture [79]

tions taking this action implies in the workflow. TBAC is applied only in rather specialized systems, i.e., document handling systems or similar Process Aware Information Systems (PAIS) [77].

There are other flavors of access control models which could be used in workflow contexts. Boughrous *et al.* [8] provide a comparative study where PAIS is the main use case, but aspects related to the industrial domain are not discussed.

Access control for industrial automation and control systems: A major source for guidance and certification for cybersecurity used within IACS is the IEC 62443 [26, 40] standard series, which contains requirements and guidance related to system and component design. The top two of the foundational requirements described in the standard are *Identification and Authentication Control* and *Use Control*, underlining the importance and laying out guidelines for access control within IACS.

It is difficult to know the current state of practice for access control within IACS with any certainty as many different generations of industrial control systems are being used, all with different properties. Looking at state of the art of access control in industrial systems, the recent publications are focusing on novel approaches and new problems, such as the Industrial Internet of Things [54, 64], smart communities [7], etc. The literature describing current practices related to access control are quite old, e.g., the book by Knapp *et al.* [29] from 2015, or the articles by Dzung *et al.* [18] from 2005, and Alcaraz *et al.* [2] from 2012.

The strategies currently used for access control in industrial automation and control systems are typically optimized for the static and strictly hierarchical systems of the third industrial revolution, implying a differential approach to access control at different levels, with detailed use control at upper levels, and a rather coarse-grained access control at the lower levels, mainly relying on network separation. The trend towards increased connectivity of devices and a usage of common network back-bones within industrial systems, points towards the need of a *zero-trust* [62] strategy for industrial networks, i.e., that all actions within the system must be checked at all times. This requires a common strategy for access control spanning all interactions, for human users as well as digital services and devices.

To follow the principle of least privilege [65], the dynamic properties of the emerging manufacturing systems should ideally be mirrored by the access control mechanisms. This could be achieved using different methods of dynamic access control [30, 15] that provide active permissions adaptable to system changes over time, following, e.g., active workflows or environmental conditions.

Currently, dynamic access control is not widely adopted in manufacturing systems, but for evolving system types, such as dynamic manufacturing, it is highly relevant.

Chapter 3

Research Summary

In this chapter the main research goal is formulated, along with accompanying research questions. We also briefly describe the process used when working towards the identified goal.

3.1 Problem description

Industrial automation and control systems are currently developed toward being increasingly modular, flexible, and dynamic. As a consequence, the requirements on the protective mechanisms of these systems are also evolving. Access Control is one of the major cybersecurity mitigating mechanisms, but it has traditionally been an underdeveloped function in industrial systems. With a zero-trust approach and a network-centric control strategy, there is an obvious need for more fine-grained access control at all levels in industrial control systems, aiming towards the principle of least privilege.

3.2 Research goal

The overarching goal of this thesis is to improve industrial automation and control system security by providing robust solutions for access control which support fine-grained, flexible and dynamic scenarios, and that are practically useful in such systems.

3.3 Research questions

In support of the research goal, a number of research questions are formulated, covering different areas of dynamic access control for industrial automation and control systems.

Investigate state of the practice: To understand in what direction to proceed toward a certain goal, you need to know your current position. To provide some clarity on the current state of the practice, the following research question is stated:

RQ1 *What are the current state of the practice and perceived challenges related to access control in industrial systems?*

The question aims to support the research goal by providing some indication of the starting position with regards to what is used, and also to provide some indication of direction, related to the perceived challenges.

Policy formulations: Access control prescribes allowed interactions within a system, based on a set of formalized rules. We need to understand how to describe rules that are meaningful in the context of dynamic manufacturing, prompting the following research question:

RQ2 *How to formulate access control policies sufficiently close to the principle of least privilege in flexible industrial systems?*

The question supports the research goal by providing guidance on strategies for expressing rules that are fine-grained and supports dynamic scenarios.

Policy enforcement: The defined policies must be possible to enforce, to have meaningful impact on the system. The mechanisms needed to support enforcement of the rules discussed in **RQ2** must be defined, leading to the following research question:

RQ3 *How can dynamic access control policies efficiently be enforced in an industrial control system?*

The question supports the research goal by providing architectures, methods, and mechanisms able to enforce the fine-grained and dynamic rules, which are suitable for industrial control systems.

Performance implications of dynamic authorization: We need to understand if the suggested strategies and mechanisms are practically useful in industrial automation and control systems. Therefore the following question is formulated:

RQ4 *What are the performance and reliability implications of including dynamic access control in an industrial automation system?*

The question supports the research goal by adding a reality-check on the suggested approaches aiming at investigating whether they are practically useful in an industrial setting, and if so, what are the implications.

3.4 Research process

The scientific viewpoint used in the thesis is classical positivism, mainly collecting information using empirical methods, and in some cases formal logic. The method is used to provide the knowledge using observations of reality. However, the work is aiming towards improving existing or developing new approaches and mechanisms rather than gaining new knowledge on existing phenomena, which is the traditional goal of empirical sciences.

Because of this, the research is developed through a process inspired by the Design Science Research Process (DSRP) [56], which is an iterative process using approaches from design science applied to information system design (Figure. 3.1). The studies included in the thesis are conducted with this process in mind, even though all studies do not complete all process steps.

The DSRP process is split into six different steps. The first step focuses on problem identification and motivation, aiming towards definition of a research problem along with a justification of the potential value of solving the problem. In the second step, qualitative or quantitative objectives for a solution of the research problem are defined. In the third step, a solution is designed and developed, and in the fourth, the efficacy of the developed artifact is demonstrated. In the fifth step the developed artifact is observed and measured in relation to the defined research problem. Finally, the results are communicated, in step six, typically in the form of one or more scientific publications.

Iterations in the process sequence is possible either after an evaluation, or as a starting point for a follow-up study. The goal of the iteration is to refine some aspects of the proposed solution, either by improving the design to increase the fulfillment of previously defined objectives, or to redefine the objectives, and adapt the design accordingly.

Depending on the approach of the study, it can start at different process steps, e.g., a problem-centric approach starting at the first step, while a development-centric approach may start at the third step. In Figure. 3.1, all articles included in the thesis are aligned with the respective approach. Article A is not using the

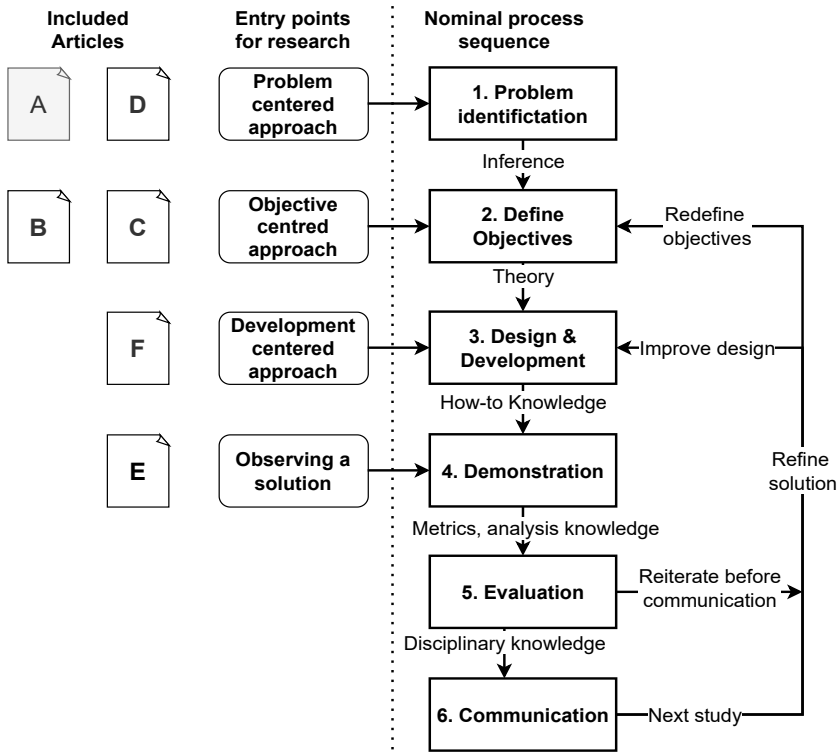


Figure 3.1: The Design Science Research Process, with each included article mapped to resp. approach (adapted from [56]). Articles are briefly presented in Chapter 4 and provided in full in Part II of the thesis.

process completely, as it does not contain any artifact development. However, it contributes to problem identification for design and development done in the following studies.

3.5 Industrial perspective

The overall goal of the PhD thesis is related to developing methods for solving foreseen problems. To some extent this means that it is difficult to claim general applicability of the contributions, as they are designed for systems that dot not exist yet. Therefore, it is not possible to study the developed method or approach in real life. Instead, to evaluate the solution in a more or less realistic context we need to reason about why the proposed solution is useful, or try to simulate a system the way we think it may look.

Being an industrial PhD research project, this situation is a bit of a dilemma, as the aim is to contribute to practically applicable solutions to real industrial problems. To keep industrial relevance of the research in a systematic way, the following method have been followed:

- Close collaboration and discussions with industrial supervisor and colleagues at ABB related to selection of orientation and ideas to further investigate. I have been the main driver of this work, though influenced by ongoing industrial projects.
- Intellectual Property screenings before publications, resulting in two patent applications.
- Targeting compatibility with available industrial standards for implementations.

This ambition to keep industrial relevance may have put limitations on the directions and methods used, but has on the other hand been a driving force behind some of the research contributions.

3.6 Relationship to Licentiate Thesis

The research work done in this PhD thesis is preceded and a continuation of prior work in the scope of a licentiate thesis, which in the Swedish academic system is a thesis presented half-way through the PhD studies. The licentiate thesis, titled *Access Control Models to secure Industry 4.0 Industrial Automation and Control Systems* [39], was successfully defended in November 2020.

Similarly to this PhD thesis, the licentiate thesis is a compilation of the following publications:

1. *Cybersecurity Challenges in Large IIoT Systems*, Björn Leander, Aida Čaušević, Hans Hansson, 24th International Conference on Emerging Technologies and Factory Automation (ETFA), Zaragoza, Spain, September 2019.
2. *Applicability of the IEC 62443 standard in Industry 4.0 / IIoT*, Björn Leander, Aida Čaušević, Hans Hansson, 14th International Conference on Availability, Reliability and Security (ARES), Canterbury, United Kingdom, August 2019.
3. *Access Control for Smart Manufacturing Systems*, Björn Leander, Aida Čaušević, Hans Hansson, Tomas Lindström, 14th European Conference on Software Architecture, Virtual, Italy, September 2020.

4. *A Recipe-based Algorithm for Access Control in Modular Automation Systems*, Björn Leander, Aida Čaušević, Hans Hansson, MRTC Report, MDH-MRTC-333/2020-1-SE, Mälardalen Real-Time Research Centre, Mälardalen University, 2020

As the title indicates, the focus of the licentiate thesis is on access control in industrial systems in general. That work provides the basis and motivates the research presented in this PhD thesis. Although none of the publications included in the licentiate thesis are part of this PhD thesis, the algorithm presented in the last publication of the licentiate thesis (4), is further described and evaluated in contributions related to **RQ2**.

Chapter 4

Contributions

This chapter presents the research results. The contributions of the thesis are described, along with a mapping between the formulated research goals and contributions. Furthermore, the articles included in the thesis are described, and each article is mapped to one or more of the listed contributions.

4.1 Thesis contributions

This PhD thesis includes the following contributions:

C1 A study of current state of the practice with regards to access control mechanisms used in industrial systems.

C2 A study of industrial practitioners perceived challenges on access control in industrial systems.

C3 A description and evaluation of access control strategies for workflow-based production systems.

C4 A description and validation of mechanisms for enforcement of fine-grained flexible access control in industrial automation and control systems.

C5 A testbed in the form of a simulation environment for the modular automation architecture.

C6 Evaluation of strategies and mechanisms from **C3** and **C4** respectively, performed in the system defined by **C5**.

A mapping between research questions, contributions and included articles is provided in Table 4.4.

In the following, we describe these contributions in more detail, and outline how they contribute to the overall research goals and the answers to the research questions.

4.1.1 Contributions C1 and C2

These two contributions together target **RQ1** and contribute to the overall research goal by defining a baseline for the current state of affairs in industrial systems with regards to access control. This helps in providing directions for the subsequent contributions.

The contributions are based on a questionnaire study of the current state of the practice with regards to access control mechanisms used in industrial systems, and of the perceived challenges from the view of industrial practitioners. The questionnaire was sent out to practitioners actively working with cybersecurity in the Swedish industry.

The questionnaire study is executed and evaluated using the guidelines for surveys in software engineering set out by Linåker *et al.* [43].

Contributions **C1** and **C2** are presented in detail in Paper A: *A Questionnaire study on Access Control for Industrial Systems.* The study could be seen as using a problem centered approach, but as no design or development is performed, we see it more as a traditional qualitative descriptive study.

Cybersecurity is an area where it is not unusual that practitioners are reluctant to share detailed information, which made recruiting respondents to the study difficult. We received enough responses to analyze the data and give a broad picture of "what is out there", but not enough to claim any statistical significance. Therefore, **C1** and **C2** cannot provide a complete answer to **RQ1**, but rather provide indications, and showcase the difficulties in fully answering this type of question.

One example of a result from the study is on the question related to which methods are generally applied for user authentication, grouped by if the respondent organization is following a cybersecurity standard or not (Figure. 4.1). 72% of the respondents indicate that they have applied a unique user identification, while the rest use shared accounts or no unique user identification.

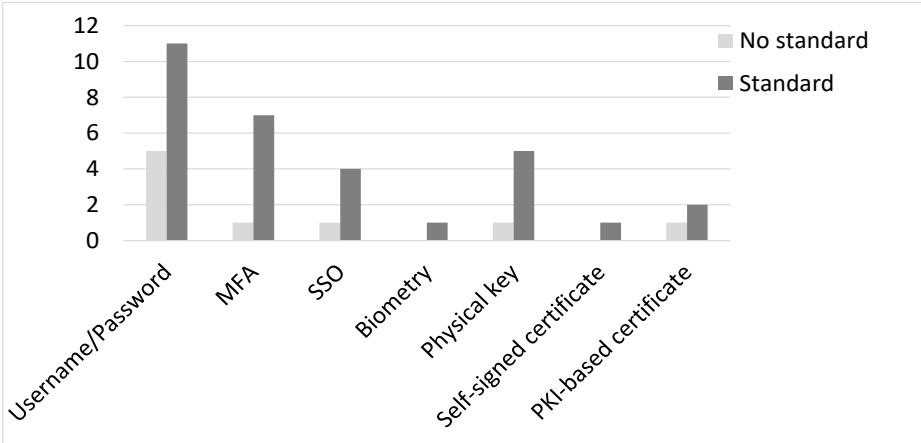


Figure 4.1: Methods used for user authentication, from Paper A

4.1.2 Contribution C3

This contribution is provided in the form of a description and evaluation of a set of access control strategies which can be used in workflow-based production systems. In total five strategies are evaluated, where three are commonly used in industry, and two are novel suggested approaches towards a perceived ideal as defined by the principle of least privilege. Furthermore, in line with one of the novel approaches, a method for automating policy rule formulations is suggested. The method is based on available engineering data, thereby allowing fine-grained and dynamic policies with a minimal management effort.

The contribution provides answers related to **RQ2** and supports the overall research goal by describing and evaluating strategies for formulating access control policies towards an ideal policy satisfying the least-privilege principle in a workflow-based production system.

The contribution is presented in Paper B: *Towards an ideal Access Control Strategy for Industry 4.0 Manufacturing Systems*, and for the method of automating policy rule inference based on engineering data a patent application has been submitted: “Access Control Within A Modular Automation System”.

The paper provides an evaluation of access control strategies that are currently used in industrial manufacturing systems and includes suggestions on further strategies progressing toward the least-privilege principle. The strategies evaluated are:

A Anyone within the network is trusted.

B Anyone with trusted credentials is trusted.

C Access is allowed to entities within a certain group.

D Entities assigned to a certain workflow are allowed to perform operations contained by the workflow.

E Entities assigned to a certain workflow are allowed to perform operations, in accordance with the sequence of the workflow.

Simulation results that evaluate the strategies against a set of attack scenarios, are summarized in Table 4.1. The article aims to provide an answer to the question on how to formulate access control policies sufficiently close to the principle of least privilege in manufacturing systems with a minimal management effort.

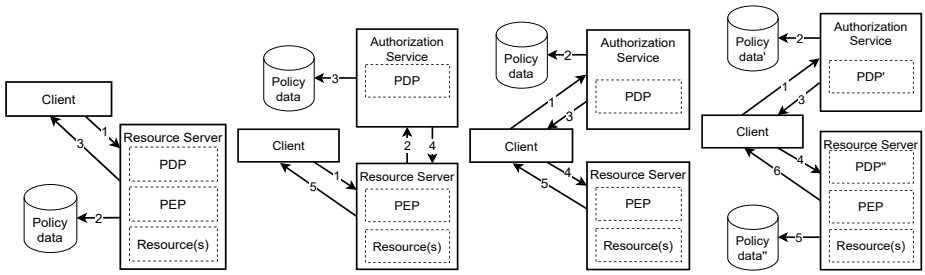
Table 4.1: Average percentage of successful attacks per strategy and scenario, standard deviation (σ)=0 unless otherwise stated. Results are based on 7-10 executions of each combination of strategy and attack scenario. From Paper B.

Strategy	Attack Scenario			
	S1	**S2**	**S3**	**S4**
A	100%	100%	100%	100%
B	100%	100%	100%	0%
C	100%	100%	0%	0%
D	58% $\sigma = 2.4\%$	0%	0%	0%
E	19% $\sigma = 2.7\%$	0%	0%	0%

In relation to the DSRP, the study uses an objective-centered approach. The focus is on the design and development. Different solutions' efficacy are demonstrated and to some extent evaluated using simulation experiments.

4.1.3 Contribution C4

C4 is a description and validation of architectures for enforcement of fine-grained flexible access control in dynamic manufacturing systems. The contribution investigates four architecture models, derived using the XACML reference enforcement architecture, and discusses these models' suitability for dynamic access control in manufacturing scenarios. Four ways of formulating access tokens in support of policy delegation mechanisms for the most promising architecture models are described, along with a feasibility study in the form



(a) Traditional client-server model. All logic in resource server.

(b) COPS-model. Resource server communicates directly w. PDP.

(c) OAuth2-model. PDP in authorization service, PEP in resource server, client mediates.

(d) OPC UA-model. PDP distributed over authorization- and resource-server, client mediates.

Figure 4.2: Four authorization architecture models. The numbers indicate the order of messages in respective protocols, from Paper C.

of an implementation. The work provides answers to **RQ3** and contributes to the overall research goal by describing how existing industrial standards can be used for achieving dynamic access control enforcement in industrial systems.

The contribution is described in Paper C: *Access Control Enforcement Architectures for Dynamic Manufacturing Systems*. The included policy delegation mechanism for fine-grained access control policy decisions resulted in the patent application "Fine-grained access control enforcement for industrial control systems using tokens, combining static roles with explicit permissions".

The article aims at answering how dynamic access control policies can be enforced in a manufacturing system by providing a high-level evaluation of a set of enforcement architectures in the context of dynamic manufacturing. The architectures are presented in Figure. 4.2, with the evaluation provided in Table 4.2.

Table 4.2: An Evaluation of architectures, from Paper C.

Architecture	**Workload**	**Network load**	**Flexibility**
(a)	High	Low	Low
(b)	Medium	High	High
(c)	Low	Low	Medium-High
(d)	Medium-Low	Low	Medium-High

The study is, from a DSRP perspective, quite similar to the one presented in Article B, as it also uses an objective-centered approach, with focus on the

design and development. Several different solutions are described, but only one is implemented and demonstrated.

4.1.4 Contribution C5

The contribution is a testbed in the form of a modular automation system simulator, exemplified with a modular ice-cream factory. The environment consists of a configurable physical environment simulator, a set of controllers, orchestration functionality, etc. The simulator is providing behavior and actuator/sensor interfaces to the controllers so that each module can be individually controlled, a key feature missing in comparable simulators.

The testbed can be used for various purposes, e.g., it is used for anomaly injection and detection experiments in the article [45], as the motivating use case in another article [53], and as one of two demonstrators in the InSecTT use case on secure and resilient collaborative manufacturing environments[1]. For the scope of this thesis, the contribution represents a realistic dynamic manufacturing system for performing evaluations of the mechanisms developed in **C3** and **C4**, thereby indirectly contributing to **RQ2**, **RQ3** and **RQ4**.

The contribution is detailed in Paper D: *Simulation Environment for Modular Automation Systems*, with further enhancements of the testbed described in [42]. This study is using a problem centered approach, and thus contains components from all steps in the DSRP, with a focus on developing an artifact supporting experimentation on a realistic modular automation system. The artifact is demonstrated by using it to create an ice-cream factory configuration. An architecture overview of the simulation environment is provided in Figure. 4.3, showing the simulation of a modular ice-cream factory.

4.1.5 Contribution C6

C6 is an evaluation of selected strategies and mechanisms from **C3** and **C4** respectively, performed in the system defined by **C5**. The evaluation is in the form of controlled experiments, where different quality properties are measured, specifically related to performance and scalability metrics. **C6** therefore provides answers to **RQ4**.

In Paper E: *Evaluation of an OPC UA-based Access Control Enforcement Architecture*, the authorization protocol and resulting enforcement architecture

[1] Intelligent Secure Trustable Things (InSecTT), a research project within the EU Horizon 2020 research and innovation programme, under grant agreement 876038 (`www.insectt.eu/use-cases/`)

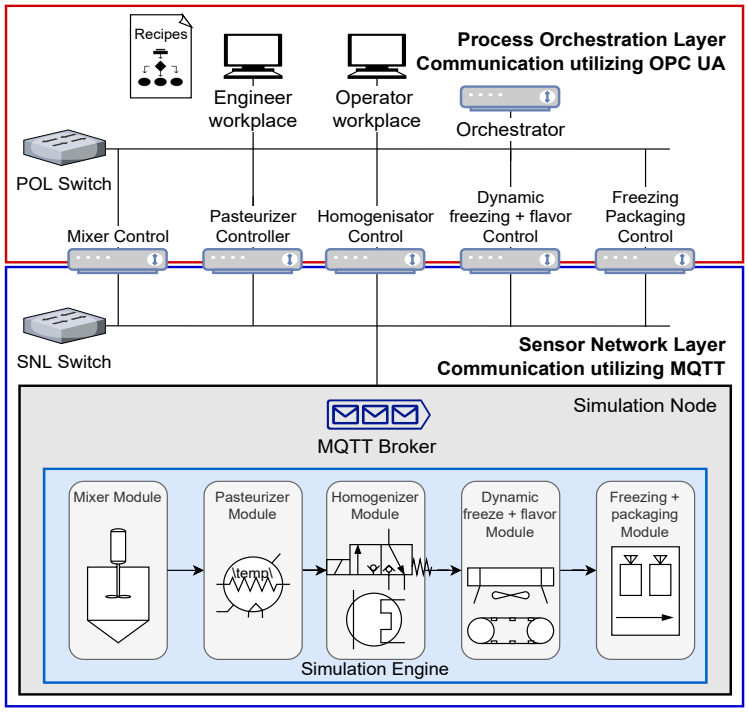


Figure 4.3: Simulation environment exemplified with a modular ice-cream factory use case, from Paper D.

(d), as described in **C4** are evaluated by investigating the completion time for different parts of the protocol. Connection establishment proved to be the critical part of the protocol with regards to added overhead. Experimental results are provided in Table 4.3. The connection establishment time using the architecture can be compared to using no authorization, both for high and low load scenarios.

Paper E does not include the authorization service in the experiments, which instead is provided separately in Paper F: *An Authorization Service supporting Dynamic Access Control in Manufacturing Systems*. In this paper the policy decision function suggested as part of **C3** in line with strategy **E** is implemented in the architecture, and different algorithms for policy decision encoding are evaluated. An overview of the implemented authorization protocol is provided in Figure. 4.4.

Table 4.3: Results from connection establishment experiments, with completion time divided by the main protocol steps. All results are given in milliseconds where μ is the average value and σ the standard deviation, adapted from Paper E.

Authorization	No authorization		Using arch. **(d)**	
	μ	σ	μ	σ
Low load				
Open session	15.0	3.3	15.1	3.3
Request Token	0	0	115.2	12.8
Activate session	100.0	12.3	193.9	12.9
Total	115.0	13.2	324.3	19.3
High load				
Open session	17.0	10.5	18.7	14.4
Request Token	0	0	213.8	69.0
Activate session	124.8	23.2	223.1	25.1
Total	141.6	29.0	455.6	88.6

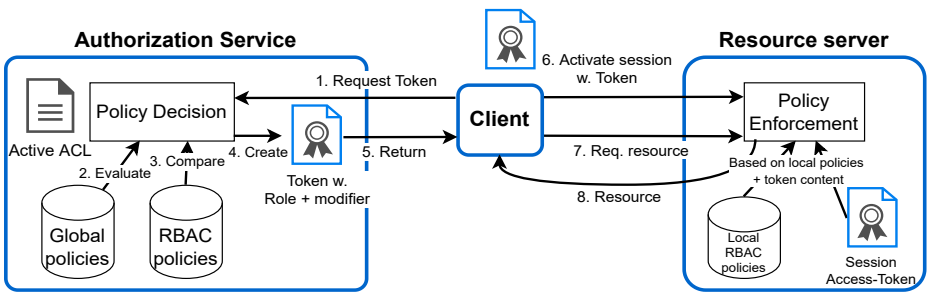


Figure 4.4: Illustration of the authorization protocol, from Paper F.

4.2 Included publications

The following publications are included in this thesis.

4.2.1 Paper A

Title: A Questionnaire study on Access Control for Industrial Systems
Authors: Björn Leander, Aida Čaušević, Hans Hansson, Tomas Lindström
Publication venue: IEEE 26th International Conference on Emerging Technologies and Factory Automation, ETFA, Västerås, Sweden, Sept. 2021.
Abstract: Industrial systems have traditionally been kept isolated from external networks. However, business benefits are pushing for a convergence between the industrial systems and new information technology environments such as cloud computing, as well as higher level of connectivity between different systems. This makes cybersecurity a growing concern for industrial systems. In strengthening security, access control is a fundamental mechanisms for providing security in these systems. However, access control is relatively immature in traditional industrial systems, as compared to modern IT systems, and organizations' adherence to an established cybersecurity standard or guideline can be a deciding factor for choices of access control techniques used.

This paper presents the results of a questionnaire study on the usage of access control within industrial system that are being developed, serviced or operated by Swedish organizations, contrasted to their usage of cybersecurity standards and guidelines. To be precise, the article focuses on two fundamental requirements of cybersecurity: identification and authentication control, and presents related findings based on a survey of the Swedish industry. The goal of the study is breaching the gap between the current state and the requirements of emerging systems with regards to access control.

My role: I was the main driver of the work, under supervision of the co-authors, who provided guidance and feedback on drafts of the manuscript. I formulated the on-line questionnaire, invited respondents, analyzed the results, and wrote the article.

4.2.2 Paper B

Title: Towards an ideal Access Control Strategy for Industry 4.0 Manufacturing Systems
Authors: Björn Leander, Aida Čaušević, Hans Hansson, Tomas Lindström
Publication venue: Published in IEEE Access, August 2021

Abstract: Industrial control systems control and supervise our most important and critical infrastructures, such as power utilities, clean water plants and nuclear plants, as well as the manufacturing industries at the base of our economy. These systems are currently undergoing a transformation driven by the Industry 4.0 evolution, characterized by increased connectivity and flexibility.

Consequently, the cybersecurity threat landscape for industrial control systems is evolving as well. Current strategies used for access control within industrial control systems are relatively rudimentary. It is evident that some of the emerging cybersecurity threats related to Industry 4.0 could be better mitigated using more fine-grained access control policies.

In this article we discuss and describe a number of access control strategies that could be used within manufacturing systems. We evaluate the strategies in a simulation experiment, using a number of attack-scenarios. Moreover, a method is outlined for automatic policy-generation based on engineering-data, which is aligned with one of the best performing strategies.

My role: I was the main driver of the work, under supervision of the co-authors, who provided guidance and feedback on drafts of the manuscript. I formulated the strategies, implemented the simulation experiments, did the formal modeling of the strategies, and wrote the article.

4.2.3 Paper C

Title: Access Control Enforcement Architectures for Dynamic Manufacturing Systems
Authors: Björn Leander, Aida Čaušević, Hans Hansson, Tomas Lindström
Publication venue: IEEE 20th International Conference on Software Architecture, ICSA, L'Aquila, Italy, March 2023.
Abstract: Industrial control systems are undergoing a transformation driven by business requirements as well as technical advances, aiming towards increased connectivity, flexibility, and high level of modularity, that implies a need to revise existing cybersecurity measures. Access control, being one of the major security mechanisms in any system, is largely affected by these advances.

In this article we investigate access control enforcement architectures, aiming at the principle of least privilege in dynamically changing access control scenarios of dynamic manufacturing systems. Several approaches for permission delegation of dynamic access control policy decisions are described. We present an implementation using the most promising combination of archi-

tecture and delegation mechanism for which available industrial standards are applicable.

My role: I was the main driver of the work, under supervision of the co-authors, who provided guidance and feedback on drafts of the manuscript. I formulated the architectures, did the proof-of-concept implementation, and wrote the article.

4.2.4 Paper D

Title: Simulation Environment for Modular Automation Systems
Authors: Björn Leander, Tijana Marković, Aida Čaušević, Tomas Lindström, Hans Hansson, Sasikumar Punnekkat
Publication venue: IEEE 48th Annual Conference of the Industrial Electronics Society, IECON, Brussels, Belgium, Oct. 2022.
Abstract: When developing products or performing experimental research studies, the simulation of physical or logical systems is of great importance for evaluation and verification purposes. For research-, and development-related distributed control systems, there is a need to simulate common physical environments with separate interconnected modules independently controlled, and orchestrated using standardized network communication protocols.

The simulation environment presented in this paper is a bespoke solution precisely for these conditions, based on the Modular Automation design strategy. It allows easy configuration and combination of simple modules into complex production processes, with support for individual low-level control of modules, as well as recipe-orchestration for high-level coordination. The use of the environment is exemplified in a configuration of a modular ice-cream factory, used for cybersecurity-related research.

My role: I was the main driver of the work, doing the majority of the implementation and design, except the visual parts of the user interface, which was developed as a project course in distributed software development, with me acting product owner. Co-author, Tijana Marković developed parts of the study related to the user interface (II.C) and data extraction (II.E), for all other parts I was the main contributor. All co-authors contributed through high-level discussions on the topics and reviewing/commenting drafts of the article.

4.2.5 Paper E

Title: Evaluation of an OPC UA-based Access Control Enforcement Architecture

Authors: Björn Leander, Aida Čaušević, Hans Hansson, Tomas Lindström
Publication venue: 28th European Symposium on Research in Computer Security, ESORICS, 9th CyberICPS Workshop, the Hague, Netherlands, Sept. 2023.
Abstract: Dynamic access control in industrial systems is becoming a concern of greater importance as a consequence of the increasingly flexible manufacturing systems developed within the Industry 4.0 paradigm. With the shift from control system security design based on implicit trust toward a zero-trust approach, fine grained access control is a fundamental requirement.

In this article, we look at an access control enforcement architecture and authorization protocol outlined as part of the Open Process Communication Unified Automation (OPC UA) protocol that can allow sufficiently dynamic and fine-grained access control. We present an implementation, and evaluates a set of important quality metrics related to this implementation, as guidelines and considerations for introduction of this protocol in industrial settings. Two approaches for optimization of the authorization protocol are presented and evaluated, which more than halves the average connection establishment time compared to the initial approach.

My role: I was the main driver of the work, under supervision of the co-authors, who provided guidance and feedback on drafts of the manuscript. I did the implementations, performed the experiments, analyzed the results, and wrote the article.

4.2.6 Paper F

Title: An Authorization Service supporting Dynamic Access Control in Manufacturing Systems
Authors: Ivan Radonjić, Enna Bašić, Björn Leander, Tijana Marković
Publication venue: IEEE 9th World Forum on Internet of Things, Aveiro, Portugal Oct. 2023.
Abstract: Cybersecurity is of increasing importance in industrial automation systems. The use of fine-grained and intelligent access control is paramount in emerging manufacturing systems as implicit trust is no longer a viable assumption for interactions within industrial systems. An authorization service is a central component of an access control enforcement architecture, to which resource servers may outsource parts of the policy decision functionality.

This paper investigates how to create and integrate an authorization service in an industrial manufacturing system, which uses workflow descriptions combined with operational system states for policy decisions. The implementation

is demonstrated in the use case of recipe orchestration in a modular automation system, and a few key quality metrics of the authorization service are evaluated.

My role: This work was executed as a master thesis work, in which Ivan Radonjić and Enna Bašić was supervised by me and Tijana Marković. The ideas behind the work and many of the suggestions driving the work were mine. One of the suggested algorithms for token encoding is adapted from Paper E, but the other algorithms, as well as the related evaluation are the work of the students, who also provided the basic content of the article, which was then re-worked by me and Tijana.

4.3 Mapping between publications and contributions

A mapping between research questions, contributions and publications are presented in Table 4.4.

Table 4.4: Mapping between publications, research contributions, and research questions.

RQ	**RQ1**		**RQ2**	**RQ3**	**RQ4**	
Contribution	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**
Paper A	X	X				
Paper B			X			
Paper C				X		
Paper D					X	
Paper E						X
Paper F						X

Chapter 5

Related Work

Three main areas are covered in this thesis: empirical cybersecurity research, access control in industrial systems, and the evaluation of quality metrics of communication protocols. In this chapter we describe relevant academic efforts within these areas, and how these previous works relate to the contributions of this thesis.

5.1 Questionnaires on industrial cybersecurity

Even though empirical studies in software engineering are a rather mature area of research, e.g., following guidelines from Linåker *et al.* [43] and Shull *et al.* [69], very few studies are related to cybersecurity in industrial settings, possibly due to the sensitivity of the subject.

Chowdry *et al.* [11] performs a combined questionnaire and interview study on cybersecurity training among cybersecurity professionals in Norwegian critical infrastructure, reaching the same type of respondents as our study.

Prins *et al.* [60], Ani *et al.* [4], and Alcaide *et al.* [1] investigate the cybersecurity awareness and capacity of employees working with industrial systems. Morris *et al.* [50] performs a combined survey and face-to-face study on cybersecurity knowledge-sharing in the automotive industry, Franke *et al.* [21] look at cybersecurity in Swedish industry. All these studies sample the knowledge of the workforce involved in the execution of different industrial systems, and all show that the level of knowledge related to cybersecurity is relatively low among employees.

No study is found which aims at investigating how access control is used in industry, which is the focus in our work.

5.2 Access Control in industrial systems

There are few academic works specifically investigating dynamic access control within industrial control systems, which have been the reason for us to additionally examine research related to access control for similar systems.

Policy models concern how access control rules are described in a computer system. For industrial automation and control systems, the state of practice is currently utilizing a role-based access control (RBAC) [12] at the higher levels, and implicit trust at the lower ones. Communication at higher levels, e.g., user access to the Human-Machine Interface (HMI), is governed by the role of the user, while trust further down in the system, e.g., between controllers, is in general allowed.

Solutions toward a more fine-grained access control policy models for industrial systems include variations of attribute-based access control (ABAC) suitable in different domains, e.g., Lang et al. [37] suggesting a Proximity Based Access Control (PBAC) suited for e.g., intelligent transportation systems, and Ruland et al. [63] use safety-specific attributes for access control in the smart grid.

There are some examples where task-based access control (TBAC) is used. The work by Knorr [30] suggests using access control matrices based on workflow-data utilizing Petri-Nets [57]. Uddin *et al.* [77] look at authorization using workflows in process-aware information systems, such as document handling or banking.

Some approaches include trust calculations and thresholds as part of the policy model, e.g., Yao *et al.* [80]. Applying such a model on industrial systems is proposed by Yu and Zhang [81] for a rail-transit data platform, and Atieh *et al.* [5] for industrial IoT devices' cloud connectivity. Both define different sets of metrics and calculations for evaluating the trust level for the given domain. The idea of adding metrics for trust levels, e.g., based on historical behavior, security threat level, etc., could add a complementary layer of defense which is not covered in our work. Especially for the interactions not described in formalized workflows, this is an interesting approach.

Access Control Enforcement Architectures describe how different software components interact in a computer system in order to enforce the rules de-

fined by the policy models [66]. There are works focusing on enforcement architectures for industrial systems, e.g., Alcaraz *et al.* [3] that discuss a policy enforcement system for distributed smart grid, using authentication tokens similarly as we do.

Federici *et al.* [20] describe a Zero-Trust architecture for industrial IoT, utilizing Software Defined Networks (SDN) and Trusted Execution Environments (TEE), in order to enable secure remote access manufacturing resources through unprotected network zones. The focus is on applying zero-trust to the edge-nodes of the industrial network. The described solution of partitioning access control on network level and data level, and using SDN for creating temporary virtual networks for sessions may be viable solution worth exploring for some scenarios also crossing the border to OT.

Martinelli *et al.* [46] describe an alternative enforcement architecture for OPC UA supporting the Usage Control (UCON) policy model [55], adding an extra protocol layer for handling the UCON policy decisions. The focus of this work is on the description and formalization of the enforcement architecture.

The previous works related to policy models and enforcement architectures are all looking at similar issues as our work. As far as we know, neither of them cover dynamic access control within industrial automation and control system, which is based on engineered workflow descriptions and uses available industrial standards, allowing adoption to real manufacturing environments, which is the aim of the work presented in this thesis.

5.3 Communication protocol evaluations

When evaluating the feasibility of a protocol, several dependability aspects may be interesting to look at, including for example availability, reliability, integrity and maintainability [6]. In our work, the focus is on some aspects of availability, namely response-time measurement paired with scalability investigations. The response-time analysis aims at revealing the conditions and limitations for using the protocol or software in real-time constrained contexts, and the scalability measurements could tell how well the proposed solution can be adopted to a complex or growing system.

There are many previous works looking into response-time scalability analysis, e.g., Cavalieri *et al.* [10], Kohnhäuser *et al.* [32] and Ladegourdie *et al.* [35] which experiment on the response-times of different aspects of the OPC UA protocol. Rocha *et al.* [71] and Burger *et al.* [9] evaluate the response-time performance of the OPC UA publish/subscribe mechanism. Silva *et al.*[70]

evaluate several communication protocols using response-time evaluation experiments.

All the above mentioned publications evaluate similar metrics of communication protocols as is done in our work, but none of them is looking at the performance cost of an enforcement architecture, which is the focus of our contribution.

Chapter 6

Conclusions

In this chapter the contributions of the thesis are summarized, and ideas on future directions are discussed.

This PhD thesis focuses on the need of dynamic and fine-grained access control for industrial automation and control systems (IACS), following the zero-trust security model required by network-centric control systems. Within the scope of the thesis, we have consulted industrial practitioners in cybersecurity on the current state of practice and foreseen challenges in the area of access control. Moreover, we have investigated different access control strategies, towards a perceived ideal of access control rules, strictly following the running workflows in a manufacturing system. Enforcement architectures which can support such dynamic policy rules are explored and the most promising approach is implemented and experimentally evaluated.

The overall aim of these contributions is to increase the resilience and operational integrity of the process, while reaping the benefits of the technical advances of the Industry 4.0 paradigm. When put together, they pose a good starting point for establishing access control towards a zero-trust approach in IACS. However, we are aware that this is just a starting point in this direction and a lot of work remains for the future.

Provided solutions focus on dynamic access control for inter-device communication. To include and combine dynamic access control for user-to-device interaction and device-to-device interactions would be an interesting follow-up work. The policy rule inference method presented in this thesis could be extended to include other sources of engineering and configuration data to provide a general solution for automatic access control rule generation in IACS.

Integration of the provided solutions into industrial products would be another potential continuation of the work. The focus could be on the components of the suggested enforcement architecture as they are technically mature and provide solutions to some of the current problems identified for industrial systems based on the network-centric architecture. However, further evaluations with regards to scalability are required, e.g., in order to provide guidance on distribution and balance of federated systems of authorization services.

Over the course of this thesis, we have generally assumed that device provisioning and public key infrastructure (PKI) solutions are in place and sufficiently secure, e.g., in order to distribute certificates in the system. Even though several techniques exist, they are mainly adopted from the IT world and may therefore not fit well in an industrial setting. Evaluating secure provisioning and PKI solutions for industrial systems could be an interesting area of research, and is a prerequisite for the solutions proposed in this PhD thesis.

One major challenge discussed in conjunction with authorization in network-centric control systems is the handling of ownership for output signals. A key requirement for sustaining deterministic behavior of a control system is that only one controller should be able to set a specific output signal. This property is inherent in the control-centric design strategy, but is lost in the network-centric paradigm, making it an important topic of research for access control in network-centric control systems.

Bibliography

[1] J. I. Alcaide and R. G. Llave. Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia*, 45, 2020.

[2] C. Alcaraz, G. Fernandez, and F. Carvajal. Security Aspects of SCADA and DCS Environments. In *Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense*, pages 120–149. Springer, Berlin, Heidelberg, 2012.

[3] C. Alcaraz, J. Lopez, and S. Wolthusen. Policy enforcement system for secure interoperable control in distributed Smart Grid systems. *Journal of Network and Computer Applications*, 59:301–314, 2016.

[4] U. D. Ani, H. He, and A. Tiwari. Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*, 21(1):2–35, 2019.

[5] A. Atieh, P. Nanda, and M. Mohanty. A Zero-Trust Framework for Industrial Internet of Things. In *2023 International Conference on Computing, Networking and Communications, ICNC 2023*, pages 331–335, 2023.

[6] A. Avizienis, J. . Laprie, B. Randell, and C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. *IEEE Trans. Dep. and Sec. Comp.*, Jan 2004.

[7] S. Bhatt and R. Sandhu. Convergent access control to enable secure smart communities. In *2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, pages 148–156, 2020.

[8] M. Boughrous and H. El Bakkali. A comparative study on access control models and security requirements in workflow systems. In *Advances in Intelligent Systems and Computing*, volume 735, pages 361–373. Springer International Publishing, 2018.

[9] A. Burger, H. Koziolek, J. Rückert, M. Platenius-Mohr, and G. Stomberg. Bottleneck identification and performance modeling of OPC UA communication models. *ICPE 2019 - Proceedings of the 2019 ACM/SPEC International Conference on Performance Engineering*, pages 231–242, 2019.

[10] S. Cavalieri and F. Chiacchio. Analysis of OPC UA performances. *Computer Standards and Interfaces*, 36(1):165–177, 2013.

[11] N. Chowdhury, E. Nystad, K. Reegård, and V. Gkioulos. Cybersecurity Training in Norwegian Critical Infrastructure Companies. *International Journal of Safety and Security Engineering*, 12(3):299–310, 2022.

[12] N. Condori-Fernandez, V. N. Franqueira, and R. Wieringa. Report on the survey of role-based access control (RBAC) in practice. Technical report, University of Twente, 2012.

[13] V.-L. Dao and B. Leander. Anomaly attack detection in wireless networks using dcnn. In *2022 IEEE 8th World Forum on Internet of Things (WF-IoT)*, pages 1–6, 2022.

[14] J. Davis, T. Edgar, J. Porter, J. Bernaden, and M. Sarli. Smart manufacturing , manufacturing intelligence and demand-dynamic performance. *Computers and Chemical Engineering*, 47:145–156, 2012.

[15] D. J. Dougherty, K. Fisler, and S. Krishnamurthi. Specifying and reasoning about dynamic access-control policies. In *International Joint Conference on Automated Reasoning*, pages 632–646. Springer, 2006.

[16] OPC unified architecture specification part 21: Device onboarding. Standard, OPC Foundation, 2022.

[17] Z. Drias, A. Serhrouchni, and O. Vogel. Analysis of cyber security for industrial control systems. In *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, pages 1–8, 2015.

[18] D. Dzung, M. Naedele, T. P. Von Hoff, and M. Crevatin. Security for industrial communication systems. *Proceedings of the IEEE*, 93(6):1152–1177, 2005.

[19] N. Falliere, L. O. Murchu, and E. Chien. W32. stuxnet dossier. *White paper, symantec corp., security response*, 5(6):29, 2011.

[20] F. Federici, D. Martintoni, and V. Senni. A Zero-Trust Architecture for Remote Access in Industrial IoT Infrastructures. *Electronics (Switzerland)*, 12(3), 2023.

[21] U. Franke and J. Wernberg. A survey of cyber security in the Swedish manufacturing industry. *Int. Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA*, 2020.

[22] K. E. Hemsley, E. Fisher, et al. History of industrial control system cyber incidents. Technical Report December, Idaho National Lab.(INL), Idaho Falls, ID (United States), 2018.

[23] M. Hermann, T. Pentek, and B. Otto. Design principles for industrie 4.0 scenarios. In *Proceedings of the Hawaii International Conference on System Sciences*, volume 2016-March, pages 3928–3937. IEEE, 2016.

[24] J. Höglund, S. Lindemer, M. Furuhed, and S. Raza. PKI4IoT: Towards public key infrastructure for the Internet of Things. *Computers and Security*, 89, 2020.

[25] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. Technical report, NIST, 2014.

[26] IEC 62443 security for industrial automation and control systems. Standard, Internation Electrotechnical Commission, Geneva, CH, 2009-2018.

[27] IEC 62541 OPC unified architecture. Standard, Internation Electrotechnical Commission, Geneva, CH, 2016.

[28] B. Johansson, B. Leander, A. Čaušević, A. V. Papadopoulos, and T. Nolte. Classification of profinet i/o configurations utilizing neural networks. In *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, pages 1321–1324, 2019.

[29] E. D. Knapp and J. T. Langill. *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Syngress, Boston, second edition edition, 2015.

[30] K. Knorr. Dynamic access control through petri net workflows. In *Proceedings 16th Annual Computer Security Applications Conference (ACSAC'00)*, pages 159–167. IEEE, 2000.

[31] W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso, and K. Jones. A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*, 9:52 – 80, 2015.

[32] F. Kohnhäuser, N. Coppik, F. Mendoza, and A. Kumari. On The Feasibility And Performance Of Secure OPC UA Communication With IIoT Devices. In *SAFECOMP 2022*, page 189–203, Berlin, Heidelberg, 2022. Springer-Verlag.

[33] F. Kohnhäuser, D. Meier, F. Patzer, and S. Finster. On the security of IIoT deployments: An investigation of secure provisioning solutions for OPC UA. *IEEE Access*, 9:99299–99311, 2021.

[34] D. Kushner. The real story of stuxnet. *IEEE Spectrum*, 50(3):48–53, 2013.

[35] M. Ladegourdie and J. Kua. Performance Analysis of OPC UA for Industrial Interoperability towards Industry 4.0. *IoT*, 3(4):507–525, 2022.

[36] J. Ladiges, A. Fay, T. Holm, U. Hempen, L. Urbas, M. Obst, and T. Albers. Integration of modular process units into process control systems. *IEEE Transactions on Industry Applications*, 54(2):1870–1880, March 2018.

[37] U. Lang and R. Schreiner. Proximity-based access control (PBAC) using model-driven security. In H. Reimer, N. Pohlmann, and W. Schneider, editors, *ISSE 2015*, pages 157–170, Wiesbaden, 2015. Springer Fachmedien Wiesbaden.

[38] H. Lasi, P. Fettke, H.-G. Kemper, T. Feld, and M. Hoffmann. Industry 4.0. *Business & information systems engineering*, 6(4):239–242, 2014.

[39] B. Leander. *Access Control Models to secure Industry 4.0 Industrial Automation and Control Systems*. Licentiate thesis, Mälardalen University, November 2020. ISBN: 978-91-7485-478-7.

[40] B. Leander, A. Čaušević, and H. Hansson. Applicability of the IEC 62443 standard in Industry 4.0/IIoT. In *Proceedings of the 14th International Conference on Availability, Reliability and Security*, 2019.

[41] B. Leander, B. Johansson, T. Lindström, O. Holmström, T. Nolte, and A. V. Papadopoulos. Dependability and security aspects of network-centric control. In *2023 IEEE 28th International Conference on Emerging Technologies and Factory Automation (ETFA)*, pages 1–8, 2023.

[42] B. Leander, T. Markovic, and M. L. Ortiz. Enhanced simulation environment to support research in modular manufacturing systems. In *49th Conference of the IEEE Industrial Electronics Society 2023*, October 2023.

[43] J. Linåker, M. S. Sardar, R. M. de Mello, and M. Höst. *Guidelines for conducting surveys in software engineering v. 1.1*. Lund University, 2015.

[44] Y. Lu. Industry 4.0: A survey on technologies, applications and open research issues. *Journal of Industrial Information Integration*, 6, 2017.

[45] T. Markovic, M. Leon, B. Leander, and S. Punnekkat. A modular ice cream factory dataset on anomalies in sensors to support machine learning research in manufacturing systems. *IEEE Access*, 11:29744–29758, 2023.

[46] F. Martinelli, O. Osliak, P. Mori, and A. Saracino. Improving security in industry 4.0 by extending OPC-UA with usage control. In *15th Intl. Conference on Availability, Reliability and Security*. ACM, 2020.

[47] T. Miller, A. Staves, S. Maesschalck, M. Sturdee, and B. Green. Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems. *International Journal of Critical Infrastructure Protection*, 35, 2021.

[48] S. Mittal, M. A. Khan, and T. Wuest. Smart manufacturing: Characteristics and technologies. In R. Harik, L. Rivest, A. Bernard, B. Eynard, and A. Bouras, editors, *Product Lifecycle Management for Digital Transformation of Industries*, pages 539–548, Cham, 2016. Springer International Publishing.

[49] S. Mohurle and M. Patil. A brief study of Wannacry Threat: Ransomware Attack 2017. *International Journal of Advanced Research in Computer Science (IJARCS)*, 8(5):1938–1940, 2017.

[50] D. Morris, G. Madzudzo, and A. Garcia-Perez. Cybersecurity threats in the auto industry: Tensions in the knowledge environment. *Technological Forecasting and Social Change*, 157(May), 2020.

[51] T. E. of Encyclopaedia Britannica. *Industrial Revolution*. Encyclopædia Britannica, Inc., 2022.

[52] O-PAS Standard, Version 2.0: Part 1 – Technical Architecture Overview. Open Group Preliminary Standard (P201-1), The Open Group, February 2020.

[53] S. Opačin, L. Rizvanović, B. Leander, S. Mubeen, and A. Čaušević. Developing and Evaluating MQTT Connectivity for an Industrial Controller. In *2023 12th Mediterranean Conference on Embedded Computing (MECO)*, pages 1–5, 2023.

[54] A. Ouaddah, H. Mousannif, A. Abou Elkalam, and A. Ait Ouahman. Access control in the Internet of Things: Big challenges and new opportunities. *Computer Networks*, 112:237–262, 2017.

[55] J. Park and R. Sandhu. The UCON$_{ABC}$ usage control model. *ACM Transactions on Information and System Security*, 7(1):128–174, 2004.

[56] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee. A design science research methodology for information systems research. *Journal of management information systems*, 24(3):45–77, 2007.

[57] J. L. Peterson. Petri nets. *ACM Comput. Surv.*, 9(3):223–252, sep 1977.

[58] PI Organisation. PROFINET. `https://www.profibus.com`. Online; Accessed: 2019-03-19.

[59] R. S. H. Piggin. Emerging good practice for cyber security of industrial control systems and SCADA. In *7th IET International Conference on System Safety, incorporating the Cyber Security Conference 2012*, pages 1–6, 2012.

[60] S. Prins, A. Marnewick, and S. von Solms. Cybersecurity awareness in an industrial control systems company. In *European Conference on Information Warfare and Security, ECCWS*, volume 2020-June, 2020.

[61] A. Ray, J. Åkerberg, M. Björkman, R. Blom, and M. Gidlund. Applicability of LTE Public Key Infrastructure Based Device Authentication in Industrial Plants. *Proceedings - International Computer Software and Applications Conference*, 2:510–515, 2015.

[62] S. Rose, O. Borchert, S. Mitchell, and S. Connelly. Zero Trust Architecture. Technical report, National Institute of Standards and Technology, Gaithersburg, MD, aug 2020.

[63] C. Ruland and J. Sassmannshausen. Access Control in Safety Critical Environments. In *Proceedings - 12th International Conference on Reliability, Maintainability, and Safety, ICRMS 2018*, pages 223–229. IEEE, 2018.

[64] S. Salonikias, A. Gouglidis, I. Mavridis, and D. Gritzalis. Access control in the industrial internet of things. In C. Alcaraz, editor, *Security and Privacy Trends in the Industrial Internet of Things*. Springer International Publishing, 2019.

[65] J. H. Saltzer and M. D. Schroeder. The protection of information in computer systems. *Proceedings of the IEEE*, 63(9):1278–1308, 1975.

[66] R. Sandhu, K. Ranganathan, and X. Zhang. Secure information sharing enabled by trusted computing and PEI models. *Proceedings of the*

2006 ACM Symposium on Information, Computer and Communications Security, ASIACCS '06, 2006:2–12, 2006.

[67] K. Schwarz. Introduction to the Manufacturing Message Specification (MMS, ISO/IEC 9506). `www.nettedautomation.com/standardization/ISO/TC184/SC5/WG2/mms_intro/`, 2000. Online; Accessed: 2020-08-15.

[68] T. Seifert, S. Sievers, C. Bramsiepe, and G. Schembecker. Small scale, modular and continuous: A new approach in plant design. *Chemical Engineering and Processing: Process Intensification*, 52:140–150, 2012.

[69] F. Shull, J. Singer, and D. I. Sjøberg. *Guide to advanced empirical software engineering*. Springer, 2007.

[70] D. Silva, L. I. Carvalho, J. Soares, and R. C. Sofia. A Performance Analysis of Internet of Things Networking. *Applied Sciences*, 11(4879):1–30, 2021.

[71] M. Silveira Rocha, G. Serpa Sestito, A. Luis Dias, A. Celso Turcato, and D. Brandao. Performance Comparison between OPC UA and MQTT for Data Exchange. *2018 Workshop on Metrology for Industry 4.0 and IoT, MetroInd 4.0 and IoT 2018 - Proceedings*, pages 175–179, 2018.

[72] J. Slay and M. Miller. Lessons learned from the Maroochy water breach. In *International conference on critical infrastructure protection*, pages 73–82. Springer, 2007.

[73] J. Slowik. Evolution of ICS Attacks and the Prospects for Future Disruptive Events. Technical report, Threat Intelligence Centre Dragos Inc, 2017.

[74] P. N. Stearns. *The industrial revolution in world history*. Routledge, 2020.

[75] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn. Guide to Industrial Control Systems (ICS) Security NIST Special Publication 800-82 Revision 2. *NIST Special Publication 800-82 rev 2*, pages 1–157, 2015.

[76] R. K. Thomas and R. S. Sandhu. Task-based authorization controls (TBAC): A family of models for active and enterprise-oriented authorization management. In *Database Security XI*, pages 166–181. Springer, 1998.

[77] M. Uddin, S. Islam, and A. Al-Nemrat. A Dynamic Access Control Model Using Authorising Workflow and Task-Role-Based Access Control. *IEEE Access*, 7:166676–166689, 2019.

[78] T. J. Williams. The purdue enterprise reference architecture. *Computers in Industry*, 24(2):141 – 158, 1994.

[79] eXtensible Access Control Markup Language (XACML) version 3.0 plus errata 01. Standard, OASIS, 2017.

[80] Q. Yao, Q. Wang, X. Zhang, and J. Fei. Dynamic access control and authorization system based on zero-trust architecture. In *Proceedings of the 2020 1st International Conference on Control, Robotics and Intelligent System*, CCRIS '20, page 123–127, New York, NY, USA, 2021. Association for Computing Machinery.

[81] W. Yu and L. Zhang. Research on Zero Trust Access Control Model and Formalization Based on Rail Transit Data Platform. In *2022 IEEE 10th International Conference on Information, Communication and Networks, ICICN 2022*, pages 689–695. IEEE, 2022.

[82] E. Yuan and J. Tong. Attributed Based Access Control (ABAC) for web services. In *Proceedings - 2005 IEEE International Conference on Web Services, ICWS 2005*, volume 2005, pages 561–569, 2005.

[83] C. Zanasi, F. Magnanini, S. Russo, and M. Colajanni. A zero trust approach for the cybersecurity of industrial control systems. In *2022 IEEE 21st International Symposium on Network Computing and Applications (NCA)*, volume 21, pages 1–7, 2022.

[84] ZVEI—German Electrical and Electronic Manufacturers' Association. Process INDUSTRIE 4.0: the age of modular production. White Paper, ZVEI, Frankfurt, 2019.