Evolving a Use Case for Industry 4.0 Environments Towards Integration of Physical Access Control

Stephan Seifermann
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
stephan.seifermann@kit.edu

Maximilian Walter
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
maximilian.walter@kit.edu

***Abstract*—Industry 4.0 digitalizes the production process by collecting and sharing information of Internet of Things (IoT) devices to improve the production process. Sharing information in a supply chain, however, requires trust between all participants that access control policies have to establish. Static policies limited to information systems are not sufficient for dynamically changing production processes because they change frequently. However, linking such virtual and physical access control and keeping them consistent is not well understood. In this paper, we want to discuss the challenges of such scenarios by presenting a use case to evaluate approaches that link physical and virtual access control.**

***Index Terms*—Industry 4.0, access control, use case**

I. Introduction

Industry 4.0 [1] is about digitalization of production processes. Companies expect technologies such as the Internet of Things (IoT) or Big Data [2] to improve the overall efficiency of the production. For instance, companies can mitigate shortcomings in the supply chain if supplying companies share information about production output timely. Another example is a supplying company that shares log information of machines with external service contractors. The contractors analyze issues and send appropriate workers to fix the issue.

Besides the benefits of sharing data, there are several issues that have to be considered. Extensive data sharing can easily violate confidentiality of critical business information. For instance, the log file of a machine could leak information such as temperatures and pressures that can be considered business secrets. Competitors can gather information about the production schedule from log files or a production output value that is too fine grained. Therefore, access control is vital for constraining data sharing in a secure way. Static rules are, however, not sufficient to cover dynamically changing production processes and data requirements. For instance, the log file of a machine might only be shared after an error occurred. The access control system has to be aware of the error and has to update policies accordingly. Besides the policies for the information systems (virtual access control), policies of the physical access control system (PACS) are affected as well. A sub-contractor that shall repair the machine now needs access to the production hall the defective machine is located. The maintenance person, however, shall only have access to this single production hall. Determining the specific policies required in a certain scenario can be complex if complex software systems or production areas are involved.

The coupling of such a dynamic access control system with PACS is not well understood yet. While we are aware of approaches that consider the context of a system, we could not find approaches that exploit this information to keep PACS policies up-to-date. This would, however, be useful because Industry 4.0 targets connecting the physical to the virtual world. In our opinion, this involves addressing security challenges as well: People that have physical access to a facility can leak information as well as people that have access to the information system.

In this paper, we want to discuss some key challenges for a system evolution step that integrates physical and virtual access control. We derived the challenges from a use case involving virtual and physical access control in Section II. The use case stems from discussions about confidentiality affecting scenarios in the production process with our two industrial partners CAS Software AG (Germany) and IMA sro (Czech Republic). We want to use the use case to evaluate future solution approaches. Discussing such solution approaches is, however, out of scope of this paper. Anyway, we aim for finding a solution as part of the Trust 4.0 project [3], in which we investigate the confidentiality in Industry 4.0 supply chains. In the project, we already created different use cases for developing an example system [4] but they lack the integration of PACS. We discuss the challenges that we derived from the use case in Section III and give an overview of related work in Section IV. Section V concludes the paper.

II. Use Case Description

We expect combining physical and virtual access control to be beneficial in Industry 4.0 scenarios. In such scenarios, it is crucial to link the real with the virtual world, which includes at least monitoring real-world entities but might include enforcing access control policies in real world as well.

The description is structured as follows: First, we describe the basic requirements. Afterwards, we describe the overall

This work was supported by the German Federal Ministry of Education and Research (grant numbers 01IS17106A and 01IS17106B), the Technological Agency of the Czech Republic (project no. 2017TF04000064), and by Charles University institutional funding SVV. We would like to thank our project partners from CAS Software AG (Germany), IMA sro (Czech Republic), and Charles University in Prague (Czech Republic) for fruitful discussions.

setting of the use case that we defined in discussions with our industrial partners. In Subsection II-C, we describe a first version that only contains virtual access control. Subsection II-D describes a system evolution step that integrates PACS.

A. Requirements for the Use Case

The overall goal of the use case is to demonstrate the interplay between virtual and physical access control, as well as to serve as source for reasoning about challenges for such integrations. In addition, we want to use the use case to evaluate solution approaches in the future. For a sake of brevity, we do not list all requirements for establishing trust in supply chains, which are definitely the foundation for every use case in this field. We already elicitated such requirements from our industrial partners in the Trust 4.0 project [3] and made them available in a technical report [4].

The use case shall be focused on the confidentiality and data-sharing aspect in Industry 4.0 (R1). We do not want to cover other aspects like performance or usability. Based on the requirements of the technical report, the use case shall also cover dynamic context information such as locations or shift assignments (R2). Also, the data shall only be shared with other organizations if their privacy levels allow this (R3). A privacy level is a classification of information for one data-object. Additionally, it is important for us to include physical and virtual access control. On the physical side, there shall be at least one access to a building (R4). On the virtual access control side, at least one data sharing operation shall exist (R5).

B. Use Case Setting

The use case is settled in an Industry 4.0 supply chain with two participants A and B. A is an engine manufacturer, and B is a supplier, who delivers parts for the engines of A. The topic of the use case is handling a defective part, which is used by A during the production of an engine but has been produced by B. Figure 1 illustrates the use case as an activity diagram. The gray activities and participants (Worker, Shift Supervisor, QA A, QA Inspector A) belong to company A. The black activities belong to company B. The black and gray striped fields belong to the evolutionary extension of the approach described later in Subsection II-D. First, Subsection II-C covers the virtual access control in the information system. If we refer to a dynamic change in the text, we visualize this using an italic font. For a sake of brevity, we omit several process steps that do not affect confidentiality but would be important for modeling reality more accurately. One example is that we directly start the investigation of a defective part instead of recording defective parts and triggering the investigation after a certain threshold.

C. Virtual Access Control

The trigger of the use case is a worker detecting a defective engine part, which has been produced by B. Therefore, the worker informs the shift supervisor. This should only be possible if the worker works actively in a shift, i.e. *executing a business process step*, and the worker is at the working place *location*. The shift supervisor runs a first initial analysis to check whether the item is indeed defective. The shift supervisor then informs the quality assurance department (QA) of A about this incident by an incident report. Shift supervisors are always allowed to contact the QA department of their organization. The QA A department performs an analysis and informs the QA B department about the incident. Informing QA B should only be possible if the *privacy level* of the incident report is *internal use* according to the information classification guide of Georgia Tech [5]. QA A reduces the privacy level by removing confidential information about the product, production process, and customer that is not necessary to investigate the incident.

QA B performs an analysis, which requires requesting additional information about the problem from QA A. QA A answers the information requests of QA B. Again, the privacy level has to be at most *internal use* in order for QA A to answer the request of QA B. Afterwards, QA B sends a progress report to QA A. QA B performs a detailed analysis using the available data and sends the final report to QA A if the investigation is finished. If not, the process is repeated. In order to share the progress report and final report, the privacy level has to be at most *internal use*. After this, the incident report is closed.

D. Adding Physical Access Control

The previous version of the use case did not consider sending an inspector of A to support or supervise the inspection. Because A wants to certify the quality of its products and production processes, the certification authority, however, now requires audits of suppliers. Therefore, A sends inspectors to B on a regular basis and in case of low quality of supplied products. Physical access control becomes necessary. Previously, the visitors had to register at the reception and got a guest card to enter the production area. However, in our extension the inspector can enter the production side with his own company card and a specific set of accessible locations. In a complex production side where a supplier produces parts for different companies, this might be useful, so that the inspector can only enter buildings, in which parts for company A are produced. The changes regarding the previously defined use case are as follows: Besides informing QA B about the incident, QA A sends an inspector to manufacturer B. The inspector enters the production area of manufacturer B and investigates the incident. The inspector of A is only allowed to enter the facilities of B if there is an open incident report of A for B. The inspector is always allowed to send a report to QA A.

III. Challenges

While creating the previously described use case, we discovered several challenges during the definition as well as during reasoning about a possible solution approach. We do not consider the following list to be complete but to be a starting point for further investigations.

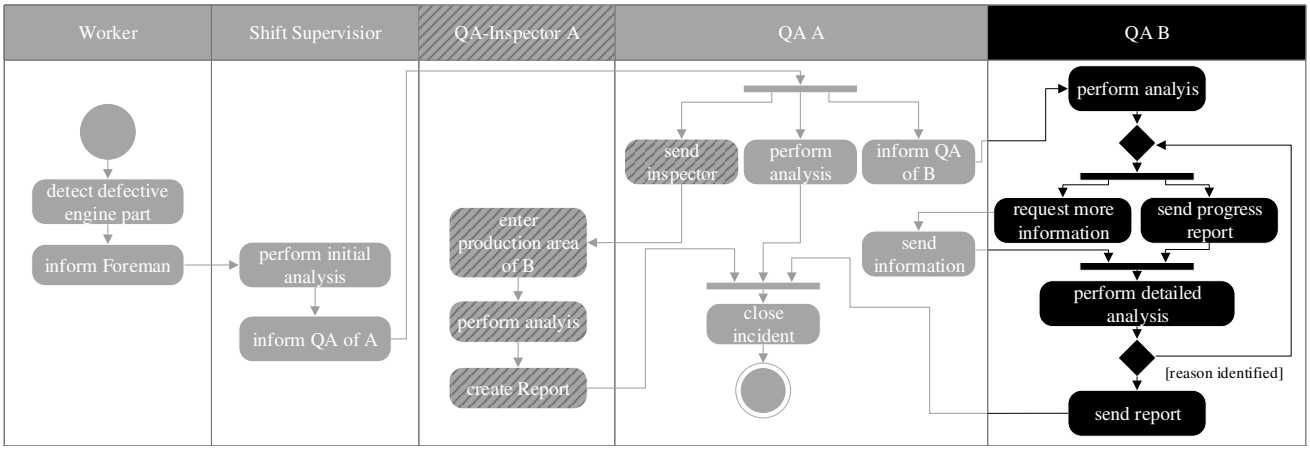

Figure 1. Overview of the complete use case including the extension of the physical access control step

The first major challenge is consistency of policies and the policy enforcement in both access control systems. The consistency of policies means that policies in both systems serve the intended purpose. While this seems to be trivial, it becomes challenging as soon as policies do not only have to be created but modified and adjusted. If dependencies between policies are not clear, the systems might end up with conflicting or at least unintended policies. Consistency in enforcement means that the decision components have to use the same version of the policies after an update. Otherwise, business processes might not be executable anymore.

The second challenge is the consideration of dynamically changing context information. Gathering required information requires combining multiple monitoring solutions that are challenging to setup and combine. Even if the information can be gathered, the policy definitions have to incorporate them. Attribute-based access control provides a framework for integrating context information but physical access control systems usually do not consider such information. Instead, they rely on static configurations and reconfigurations by humans.

The third challenge is gathering the required information securely and legally, which directly connected to the previous challenge. For instance, the continuous tracking of worker might be forbidden in some countries.

IV. Related Work

We identified related work in the fields of dynamic changes and use cases combining virtual and physical access control.

Hu et al. [6] mention dynamically changing environments in the definition of ABAC but do not describe changes that affect policy decisions. Organization based access control (OrBAC) [7] is a dynamic virtual access control system. It allows setting access rights over contexts [8], which describe the environment for accessing data. However, it lacks the support for PACS.

There are plenty of use cases and case studies for information systems. CoCoME [9] is one example that also provides evaluation scenarios. Pilipchuk et al. [10] discussed extending CoCoME with security including access control but do not consider physical access control. To the best of our knowledge, there is not yet a case study that combines virtual and physical access control for Industry 4.0 scenarios.

V. Conclusion

Access control of exchanged information is vital for a cooperation of manufacturers in a supply chain to improve distributed production processes. Industry 4.0 complicates access control because of frequent changes such as the amount of available data, or the context data is used in. Because the information systems are connected with real-world entities such as workers, virtual access control is not sufficient. We created a use case that incorporates physical access control and collected some initial challenges. Both use case and challenges can be a foundation for further research in combining virtual and physical access control.

References

[1] M. Hermann, T. Pentek, and B. Otto, "Design principles for industrie 4.0 scenarios", in *HICSS'16*, IEEE, 2016, pp. 3928–3937.

[2] R. Schmidt, M. Möhring, R. C. Härting, C. Reichstein, P. Neumaier, and P. Jozinović, "Industry 4.0 - Potentials for creating smart products: Empirical research results", in *Lecture Notes in Business Information Processing*, vol. 208, 2015, pp. 16–27.

[3] R. Al-Ali, R. Heinrich, P. Hnetynka, A. Juan-Verdejo, S. Seifermann, and M. Walter, "Modeling of dynamic trust contracts for industry 4.0 systems", in *Companion Proceedings (ECSA '18)*.

[4] R. Al-Ali, T. Bures, B. Hartmann, J. Havlik, R. Heinrich, P. Hnetynka, *et al.*, "Use cases in dataflow-based privacy and trust modeling and analysis in industry 4.0 systems", Karlsruhe, Tech. Rep. 9, 2018, 43 pp.

[5] Georgia Tech, *Data access*, http://policylibrary.gatech.edu/data-access, accessed 04.01.2019.

[6] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, *et al.*, "Guide to Attribute Based Access Control (ABAC) Definition and Considerations", National Institute of Standards and Technology, Tech. Rep. NIST SP 800-162, 2014.

[7] A. A. E. Kalam, R. E. Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, *et al.*, "Organization based access control", in *POLICY'03*.

[8] F. Cuppens and A. Miège, "Modelling contexts in the Or-BAC model", in *ACSAC '03*, IEEE, pp. 416–425.

[9] S. Herold, H. Klus, Y. Welsch, C. Deiters, A. Rausch, R. Reussner, *et al.*, "Cocome-the common component modeling example", in *The Common Component Modeling Example*, 2008, pp. 16–53.

[10] R. Pilipchuk, S. Seifermann, and E. Taspolatoglu, "Defining a security-oriented evolution scenario for the cocome case study", in *EMLS'17*, vol. 37, 2017, pp. 60–77.