Towards an Access Control in a Smart Manufacturing context

Björn Leander
ABB Industrial Automation, Process Control Platform,
Mälardalen University,
Västerås, Sweden
bjorn.leander@mdh.se

***Abstract*—In the ongoing 4^{th} industrial revolution a new paradigm of modular and flexible manufacturing factories powered by IoT devices, cloud computing, big data analytics and Artificial Intelligence is emerging. It promises increased cost efficiency, reduced time-to-market and extreme customization. However, there is an increasing risk that technical assets within such systems will be targeted by cybersecurity attacks. A compromised device in such an environment could cause significant damage, not only economically for the factory owner, but also physically on humans, machinery and the environment.**

This paper discuss one of the main mitigation strategies against compromised devices, namely access control. Until today inter-device communication within a manufacturing environment has had limited need for privilege handling, but due to connectivity requirements and the dynamic properties of smart manufacturing that is no longer the case. Furthermore, the access control models that are widely used within IT-environments today do not provide sufficient granularity and dynamicity for the needs of smart manufacturing. This article derives requirements on access control in such systems and provides an assessment of one of the novel access control models, Attribute Based Access Control, in the context of a smart manufacturing use case scenario.

I. Introduction

Smart manufacturing [1], [2] is a development of the traditional manufacturing industry implying a shift from production of big batches of identical units toward a highly dynamical manufacturing environment where production is tuned to extreme customization, fluctuating markets, and specific customer needs. The goal is to reach a highly re-configurable manufacturing system that can easily adapt to the changing requirements. The technology to enable this dynamic behaviour includes an increasing amount of interconnected sensors, actuators and related services in the manufacturing environment in combination with e.g., cloud technologies, data lakes, artificial intelligence etc. for inference and aid to decision-makers [3].

In the traditional manufacturing environment communication paths between devices were predefined and hard-wired, therefore the access control for inter-devices activities was not seen as an issue. Which devices could read data or execute operations on other device was defined by the wiring schemes and process descriptions. Furthermore, the control network was seen as being air-gapped in relation to the outside world. In the dynamic smart manufacturing environment of today and tomorrow, this is no longer the case [4]. Considering that a great number of the devices introduced in smart manufacturing have wireless connectivity, are living on the edge of the network, possibly with direct connections to unprotected networks, it is an increasing risk that any of the devices are compromised by a cybersecurity attack. This has been illustrated in a number of attacks targeting industrial systems over the last ten years. For protection of the manufacturing environment against compromised devices, there is therefore a need for a number of security measures, e.g in the form of Intrusion detection systems, end-to-end security for sensitive data, malware detection and inter-device access control.

This article is focusing on Access Control, as one of the basic security functions in any system. It aims to restrict access to operations on resources only to legitimate authorized subjects. The models for access control that are currently in use are focused on authorizing human subjects performing operations on digital assets. These models do not scale well with the dynamic and heterogeneous scenarios of smart manufacturing. A novel access control model is Attribute Based Access Control (ABAC), which has been suggested as a good match for machine-to-machine authorization [5], [6], [7]. This paper examines the implications of using ABAC in smart manufacturing systems, based on a number of requirement derived from a literature study and a simplistic use-case scenario.

The remainder of this paper is structured as follows: Research questions and methodology is described in section II, and necessary background is presented in section III. The data related to the literature review is described in section IV. In section V a compilation of requirements on access control, being the result of the literature review, is listed. In section VI a use cases scenario for smart manufacturing is described, followed by a discussion on how the use cases relate to access control requirements in section VII. Scientific work related to our findings is presented in section VIII. Finally the work is summarized and some remaining challenges and future areas of research are described in section IX.

II. Research Questions and Methodology

The research questions driving this work are:

Q1 What are the requirements on access control for smart manufacturing systems?

Q2 What are the implications of using Attribute Based Access Control (ABAC) as a model for privilege handling in a smart manufacturing system?

To get information on the current state-of-the art for requirements on smart manufacturing, a literature survey is performed. The survey is loosely based on the guidelines for a structured literature review presented by Kitchenham [8], with the following exceptions:

- Only one researcher was involved in the review.
- No quality instrument has been developed and used in the study, as the number of articles to review were at a manageable number after initial inclusion / exclusion completed.
- As the resulting articles have been very different in their form, structured data extraction was difficult. The data synthesis is therefore a result of combined notes from reading each of the articles, i.e., a narrative line of argument synthesis.
- A number of additional studies and standards are included in the study, indicating that the initial search criteria may be too narrow.

The result of the literature survey is an enumeration of requirements on access control in smart manufacturing systems. (Q1)

To address the second research question a exploratory case study method has been used, based on the checklist for case study design in [9]. The study is looking at three embedded units of study, being access control situations typical for a smart manufacturing scenario. Due to the simplicity of the studied scenario, the following exceptions from the method are done:

- No formal protocol is constructed.
- Only one case is studied with only one method, so no triangulation.
- The collection and analysis of data is performed in conjunction and resulting in a direct analysis, so there is no raw data available for further analysis.

The scenario is an illustrative example on how access control policies can be formulated using ABAC. The scenario is also used to corroborate the validity of the requirements inferred from the literature study. Implications of using the ABAC model for privilege handling in smart manufacturing are discussed in the light of the use case and the derived requirements. (Q2)

III. Background

A. Smart Manufacturing concepts

The term ”Smart manufacturing” is initially used for describing the 4^{th} industrial revolution from a manufacturing perspective, and it originates from joint work by several agencies in the USA [3]. There are several similar terms covering parts of the same area, e.g., Cyber Physical Production Systems (CPPS) [10] and Intelligent Manufacturing Systems (IMS) [1]. Smart manufacturing can be seen as a subset of the Industrial Internet [11] and the Industrial Internet of Things (IIoT) as defined by Boyes et al. [12]. Modular Automation [13] is another term, used for smart manufacturing in the process industries, e.g., chemical and pharmaceutical industries.

Smart manufacturing encompasses the whole manufacturing chain, from supply chain to shop floor production and logistics. Huge amounts of data collected from sensors within the manufacturing process is used for advanced data analytics in order to improve the overall operations of the process. One key aspect of smart manufacturing is to provide flexibility and dynamicity in the manufacturing environment by modularization of process steps, meaning that different process steps should be able to be combined and re-combined based on current production requirements [14]. An open framework for describing and integrating process steps in the manufacturing system also enables the idea of Workflow as a Service (WfaaS), meaning that vendors of production equipment could sell pre-fabricated process-steps as a service, allowing the factory owners to more easily adapt to increasingly fluctuating market demands. How different components in a smart manufacturing system should cooperate is still unclear, but at least two variants are described in the literature. Choreography, were the overall objective is defined, but it is up to the components to collectively solve the objective, which is the basis of many use cases described in the literature [2]. The other alternative is orchestration were one device has as only task to order all the other devices what to do, which is currently the main trend in modular automation [13].

B. Cybersecurity Threats to Smart Manufacturing Systems

Looking at smart manufacturing from a cybersecurity perspective, the increasing amount of connected and interconnected devices required for the data acquisition together with external stakeholders needing access to the data, considerably increases the attack surface of the system. Furthermore, as the different modules within the system is dynamically connected to each other, the authorization of privileges between devices and services also must be equally dynamic to allow continuous secure operation. The alternative of allowing any actor within the manufacturing system to execute any action would severely expose the system to internal attackers as well as to mistakes made during configuration or operation of the system. As pointed out by Tuptuk et al. [4], cybersecurity is seen rather as a characteristic than as a design principle within the development of smart manufacturing systems, a misconception that may leave many systems insufficiently protected.

An attack on a smart manufacturing system may have severe implications, depending on the objective of the attacker. The CIA-model is often used to describe the desired security characteristics of a system, CIA meaning **C**onfidentiality, **I**ntegrity and **A**vailability. In smart manufacturing we can use the following translations for these characteristics:

[1] http://ims.org

- Confidentiality: Intellectual Properties with regards to the manufacturing process (IP), along with sensitive information with regards to customer orders, credentials of operators and contractors, etc.
- Integrity: Ensuring that data used for analysis is unaltered, ensuring that a production ordered received is accurate and comes from the indicated source, etc.
- Availability: Up-time and reliability of production equipment, etc.

A cybersecurity attack may breach any of these characteristics, e.g., leading to possible loss of IP, costly errors in production due to unreliable or faulty data and, most seriously, down-time or potentially safety-related threats to production machinery.

C. Attacks on comparable industrial systems

There are currently few reported attacks on smart manufacturing systems, due to the fact of the novelty of such systems - there are almost no fully operational sites using smart manufacturing. As these systems becomes more of a commodity and the standardization efforts for the used technology is more mature, the systems will become more lucrative targets for hacker activity. However, there are an increasing number of attacks on industrial systems using the same kind of technology as is being used in smart manufacturing scenarios. One example is the TRISIS attack: in 2017 malware was detected on a number of Schneider Triconex safety instrumented system units, granting the attacker full control over safety critical PLCs in a petrochemical facility. A cybersecurity attack on the Ukrainian power grid in December 2015 is another example, where attackers were able to compromise and disrupt power distribution [15], affecting approximately 250.000 Ukrainian citizens, using a combination of several technologies, including lateral movement from IT-network to operational network using privilege escalation weaknesses.

D. Access Control definitions

There are a number of guiding principles for authorization, the most notable ones being [16]:

1) **Least privilege**, requires that a subject should only have the least privileges possible to perform its tasks.
2) **Separation of duties**, meaning that different subjects should have different tasks, e.g., an administrator should not also be a application user.
3) **Complete mediation** requires that any access to a resource must be monitored and verified.

These principles can be interpreted as: i) different subjects shall have different privileges, based on their current task with ii) an existing mechanism enforcing authorization of these privileges, and iii) each request of privilege securely tied to a subject identity. Following these principles for communication within a smart manufacturing environment will help minimize the harm an attacker can do after gaining an initial foothold within the system, and even shorten the detection time, since failed access attempts typically is logged and monitored, e.g., in accordance with IEC 62443-3-3, foundational requirements 2 (use control) and 6 (timely response to events) [17], [18].

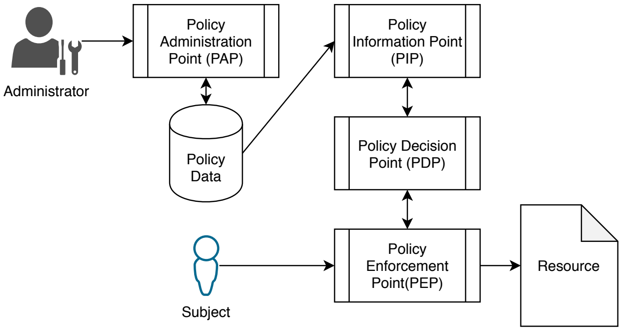
Administrator
Policy Administration Point (PAP)
Policy Data
Policy Information Point (PIP)
Policy Decision Point (PDP)
Subject
Policy Enforcement Point(PEP)
Resource

Fig. 1: Authorization Policy Enforcement Architecture

In Figure 1 an architecture for Authorization Policy Enforcement is depicted, using the standard nomenclature from the literature, see e.g., [19], [20], [7]. When a subject requests a resource, this request is mediated through a Policy Enforcement Point (PEP). The PEP request an authorization decision from the Policy Decision Point (PDP), which reads policy information from the Policy Information Point (PIP), reading Policy Data. An administrator maintains the Policy data through a Policy Administration Point (PAP).

Historically, Mandatory Access Control (MAC) and Discretionary Access Control (DAC) have been the two main paradigms within access control [21]. MAC is 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. 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 a development building both on principles from DAC and MAC, where subjects have one or several roles, and roles can be hierarchically ordered. Privileges are derived from the roles rather than from the subject. Roles are a natural concept for humans, but may not be the best fit for information objects. Furthermore, in a number of studies it has been found that the traditional access control schemes are not sufficient for, e.g., cloud-connected cyber physical systems [22] and Industrial Internet of Things (IIoT) [23].

E. Attribute Based Access Control

A novel scheme in access control is Attribute Based Access Control (ABAC), which was introduced by Yuan and Tong [24]. The initial use case was for access control in web services, where the granularity of the traditional RBAC scheme was not fine enough, or at least - the amount of configuration needed for the RBAC was unfeasible compared to the simple requirements. One such example was about granting a user access to movies in an online streaming service, based on movie R rating (R, R-13, G) and freshness F (New release, normal), which mapped to the user age A and subscription category C (Budget, Premium), lead to an explosion of user roles and permissions. With ABAC a much more elegant solution was presented, which in principle can be summarized as: Subject s right to perform operation o on resource r in environment e is calculated based on attributes of the subject, resource and environment A_s, A_r, A_e:

$$allow_o(s, r, e) \leftarrow f(A_s, A_r, A_e) \tag{1}$$

For the example with the movie streaming service, the following policy rules can be used for access control, based on the viewer and movie attributes:

$$f_1(s, r, e) = (R_r = \text{G}) \vee (A_s > 12 \wedge R_r = \text{R-13}) \vee (A_s > 17) \tag{2}$$

$$f_2(s, r, e) = (F_r = \text{normal}) \vee (C_s = \text{premium}) \tag{3}$$

Then the rules can be combined:

$$allow_{view}(s, r, e) = f_1(s, r, e) \wedge f_2(s, r, e) \tag{4}$$

Furthermore, an ABAC authorization architecture was suggested, with the following entities, in addition to the subject, resource and operation:

- Attribute Authorities (AA) - create and manage attributes for subjects, resources and environment.
- Policy Authority (PA) - creates and manages access control policies (in principle formalizes function $f(...)$ above).
- Policy Decision Point(s) (PDP) - evaluates applicable policies and makes the authorization decision. Will request attributes from AA, and policies from PA
- Policy Enforcement Point(s) (PEP) - requests authorization decision from PDP, and enforces received decision.

IV. Literature Review

The survey of the current state of the art for smart manufacturing and access control was conducted using the following search-phrase:

("SMART MANUFACTURING" OR "CYBER PHYSICAL PRODUCTION SYSTEM" OR "INTELLIGENT MANUFACTURING SYSTEMS") AND ("ACCESS CONTROL" OR "AUTHORIZATION" OR "PRIVILEGE HANDLING")

Selected resources for search were: IEEE Xplore, Scopus and Web of Science. The initial searches resulted in quite a small number of hits in the selected sources (IEEE Xplore: 5, Scopus: 10, Web of Science: 3). When removing doublets the number of unique hits amounted to 14, published between 2004 and 2019. The selected inclusion criteria for papers were: "any study describing smart manufacturing from the perspective of access control". Checking titles and abstracts for all the unique hits against the inclusion criteria excluded six more articles, leaving a total of eight articles. The small number of articles, which of six are from 2018-2019, and only two having more than two citations indicates that (1) this area of research is quite unexplored, and (2) there is a need to look at additional sources to be able to reach the research objectives. A reading of the articles left only two of them as providing value to the research question.

This lead to the inclusions of a number of seminal articles and standards:

- The IEC 62443 Standard is an cross-industry standard used for cybersecurity within industrial automation and control systems [17].
- The Industrial Internet Consortium Ref. Architecture [25].
- The work by Salonikas et al. [23] provides an evaluation of access control models within the larger scope of the Industrial Internet.
- Lopez et al. [22] looks at requirements on access control from the perspective of cloud-connected cyber physical systems.
- The article by Ladiges et al. provides information on the current state of Modular Automation [13].

The two articles from the structured review were the works by Faller et al.[26] and Ayatholli et al. [27].

The result of the literature study is synthesized into a number of access control requirements on smart manufacturing systems, presented in the following section.

V. Access Control Requirements on Smart Manufacturing

Through the literature study, guided by the basic principles for access control the following requirements are formulated:

A. Requirements related to dynamic systems

A number of requirements are shared with other dynamic systems of interconnected cyber-physical systems [22], [14]:

1 Dynamic: Several different kinds of applications could be integrated for the whole product life-cycle, implying multiple categories of users and usages of services and production related data.

2 Scalable with regards to users and policies. Management of a huge amount of devices, services and users must be simple and cost efficient, still providing necessary transparency.

3 Flexible: The access control mechanism must provide an easy way of defining new policies, what privileges can be transferred, definitions of trust-relationships between subjects, etc.

4 QoS: The computational cost of inferring privileges cannot negatively impact the performance of the system as a whole.

B. Requirements related to traditional automation

A number of requirements are originating from the traditional automation domain [17], [25]:

5 The manufacturing system should be operable also in island-mode, i.e., a disruption in network connectivity between shop floor and cooperate network should not interfere with production.

6 During critical events the manufacturing system must stay operable: operator lockout cannot happen due to a security related policy e.g., failure of entering correct password three times.

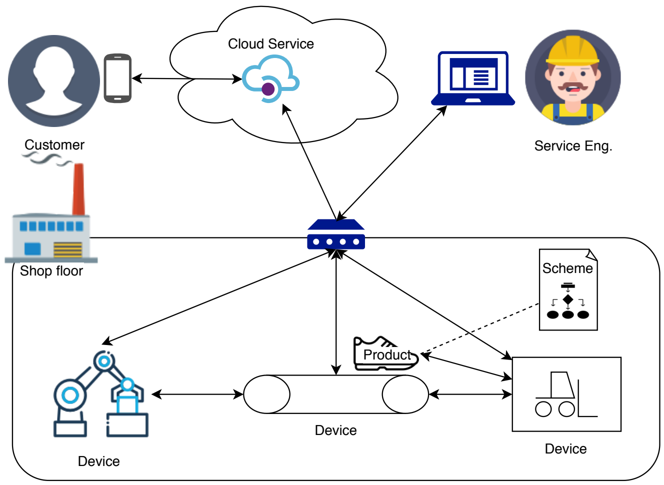

Fig. 2: Illustration of smart manufacturing scenario

C. Requirements related to smart manufacturing and the Industrial Internet

Properties specific to the smart manufacturing domain include [13], [26], [23], [27]:

7 Temporal policies: The policy may shift between each batch, or even between each produced unit, leading to potentially quick shifts in policies.

8 Logical ordering: Performing actions in a manufacturing environment is usually described as a workflow, meaning that the order of the actions, and the number of times an action can be executed also could be limited by an access control policy.

D. Requirements related to transparency

Generic access control requirements:

9 Transparency: At least from an administrator perspective, it must be easy to deduce current state of granted privileges, and historical changes to privileges.

VI. A Smart manufacturing Scenario

In this section we construct a generic smart manufacturing scenario to analyze from a access control perspective, and discuss how ABAC can be applied in this scenario. The scenario in principle follows the set-up of a service-driven architecture for manufacturing, described in [14] and [26], rooted in the IEC 61499 [28] standard.

An illustration of the scenario is provided in Figure 2. The illustration is limited to the different entities mentioned in the scenario, and therefore hugely simplified. Assume product p is to be manufactured. p is associated to a set of devices $d \in \mathbf{D}$ that must perform tasks on p for it to be finalized. In order to perform the actions there is a need for the devices d to share information, or even execute operations on each other, according to the manufacturing scheme defined for p.

Onto that, the customer c wants to read information from the system for data related to product p via a cloud service, and the 3rd party service organization s who is responsible for maintaining some of the devices in $\mathbf{D}$ must be able to read and possibly perform actions on the devices, e.g. reading health records and performing firmware upgrades.

Note that the devices in $\mathbf{D}$ is allowed to cooperate based on their assignment to the manufacturing scheme related to the specific product. The customer is only allowed to read data specific to the product it has ordered, the service organization can only read and perform actions on devices they currently maintain, something that may change at the end of a contract etc.

This is a simplified scenario, however, it is enough to show some interesting characteristics with regards to access control in smart manufacturing systems:

1) m2m cooperation limited by current product/batch attribute.
2) Customer outside organization read rights limited by purchase.
3) Service organization personnel (possibly 3rd party) having read and e.g. firmware-update rights limited by a contract.

It would be possible to describe these properties using RBAC, e.g., for (1), the devices and services related to the current batch could be assigned a new role, allowing them to access a list of resources, as defined by the manufacturing scheme. However, this would lead to an explosion of roles as new batches appear in the system, and the roles will have to be quickly disposed of as soon as the batch is completed. Instead using ABAC, policy (1) could be expressed as:

$$allow_{op}(s,r,e) = (batch_{id}(s) = batch_{id}(r)) \wedge id \in batches(e) \tag{5}$$

Meaning that the privilege to perform the operation will be granted only if the subject and resource have the attributes batch assigned with the same id, and that id is among the active batches in the environment.

Similarly for policy (2) the customer could be granted privileges based on a combination of attributes of the data and attributes of the customer, which would allow a very fine-grained model for authorization. Typically this information is currently retrieved through filtering in the application, meaning that the privilege is enforced by the application or API implementation rather than being part of the access control mechanism, which will grant access to the read-function to any valid customer.

The privileges of personnel from the service organization (3) is an interesting issue, since there may be many factors within the manufacturing environment that should prevent interruption or additional load on devices or services related to direct operation. In a classical service operation scheme, privileges to perform maintenance related operations may not be allowed except when the production unit is halted for planned maintenance or similar. However, in a smart manufacturing environment, this may very well be possible, especially for WfaaS scenarios - it is up to the service organization to make sure that the workflows are running as needed. In these cases an attribute based access control scenario could also be of help to minimize the risk of disturbing ongoing operations. For example, attributes indicating that the device is currently in use could inhibit right to perform disruptive actions, attributes indicating a need to perform an update or a similar disruptive maintenance action could inhibit the device from being assigned to a batch, etc.

VII. Discussion

What we can see with regards to ABAC is that it is highly flexible and supports dynamic use cases (**requirement 1 and 3**), except perhaps discretionary properties. It is not clear that the management effort of ABAC scales well with increasing complexity (**requirement 2**), and it is not a general property of ABAC that it has low computational cost (**requirement 4**).

Requirement 5 stipulates that there must be a federated or distributed architecture for access control in smart manufacturing applications. This characteristic is uncommon in most available access control implementations. For example, in RBAC, a central domain controller is usually required. Also for the classical ABAC it would seem as this is a difficult requirement to fulfill, mainly due to the central policy authority. However, it is quite possible to imagine an implementation of local caches for attributes and policy authorities that can be used in isolation in cases of loss of connectivity to the central authorities. There are research looking at federated access control, not specifically for ABAC but e.g., for inter-cloud environments [29], [30], Capability Based Access Control in IIoT [31], etc.

Requirement 6 could possibly be met by ABAC, if using an environment attribute indicating the ”danger level” within the plant. However, this will inadvertently add an incentive for an attacker to provoke the system until it reaches a high such level and then, e.g., perform a dictionary based password guessing attack.

For **requirement 7** it was illustrated in the scenario description how to reach this kind of temporal policy, providing a robust mechanism for attribute assignments.

Requirement 8 is currently not supported by ABAC, nor by any other access control model known by the author.

A generic requirement on an access control model is to provide transparency (**requirement 9**). For ABAC it is not clear that such functionality is available neither with regards to an administrator, nor to an user. Possibly a clever implementation could be able to answer to the transparency needs of an administrator, but it is not intrinsic to the access control scheme, as is the case with e.g., access control list (ACL) ability to perform per-resource review, or RBAC ability to perform a per-subject review.

A. Threats to validity

For the literature review, the low amount of matching articles is a clear threat to the validity of the results. The inclusion of additional sources is one action done to mitigate this threat. However, a more broadly formulated search criteria could have elicited a better result.

For the case study, the idea was mainly to illustrate and exemplify, but the case itself is hugely simplified, making it a threat to the validity. The lack of mature real-life implementations of Smart Manufacturing systems makes validity-checking of the model rather difficult.

VIII. Related Work

There are a number of earlier works discussing access control requirements in dynamic industrial systems, e.g. by Salonikas et al. for the wider concept of IIoT [23] and Lopez et al. for cloud connected cyber physical system [22]. Both these articles discuss different access control model on the policy level, similarly as in our work, but none of them look at the modular characteristics specific for smart manufacturing.

In the work by Watson et al. [5], the use of different access control models in conjunction with OPC UA is discussed. The authors are advocating ABAC or a combination of ABAC and RBAC as a good match for protection against privilege escalation on both inside and outside attackers within Industrial Automation and Control Systems. Their work can be seen as a suggestion in the enforcement layer, whereas our guidance is in the policy layer.

There are several works were variants of ABAC are presented, e.g., Lang et al. [7] is suggesting proximity based access control, being a good match especially for logistics systems, Park and Sandhu [6] describes Usage Control (UCON) being a good match for e.g., handheld IoT devices. Next Generation Access Control (NGAC) [19] is the NIST suggestion for how ABAC should be described, differing from traditional ABAC in that the attributes are hierarchical labels (similar to RBAC group hierarchies), rather than properties with values. All these variants of ABAC could be investigated in detail to see if they provide the same or a better match to the requirements on smart manufacturing.

IX. Conclusions

Smart manufacturing is an emerging technology within the manufacturing industry, having a huge economical and transitional potential. However, the technologies that smart manufacturing systems are built upon brings new challenges to the system, especially the increasing attack surface expose the system to additional cybersecurity threats. As we have argued in this paper, one of the looked over mechanisms for security within manufacturing systems is access control between devices and services. This area needs additional attention, the dynamic properties of smart manufacturing requires a similarly dynamic model for access control.

In this article we have derived a number of requirements on access control within smart manufacturing systems, and using a simple scenario, mapped these requirements on ABAC. Clearly ABAC is one interesting candidate for usage in Smart Manufacturing systems. It provides highly flexible and dynamic properties which aligns well with the derived requirements. There are however still several open questions to answer, such as:

1) How well does ABAC scale with regards to management?
2) Is there a way to prove QoS for ABAC privilege deduction?
3) How to provide necessary transparency?
4) Does ABAC work well in a federated architecture?
5) Can ABAC be implemented to allow the temporal properties of smart manufacturing?

One way forward for answering at least a few of these questions would be to conduct a simulation or experiment using use-cases from the smart manufacturing domain together with e.g., the Policy Machine, which is the reference implementation of NGAC from NIST [2]. The management issue of security policy generation could possibly be handled using model driven security, as discussed by Lang et al. [7]. The feasibility of such solution could be investigated, e.g., in conjunction with modular automation where the idea of a formal recipe description is already quite mature.

References

[1] S. Mittal, M. A. Khan, and T. Wuest, "Smart manufacturing: Characteristics and technologies," in *Product Lifecycle Management for Digital Transformation of Industries* (R. Harik, L. Rivest, A. Bernard, B. Eynard, and A. Bouras, eds.), (Cham), pp. 539–548, Springer International Publishing, 2016.

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

[3] K.-d. Thoben, S. Wiesner, and T. Wuest, ""Industrie 4.0" and Smart Manufacturing – A Review of Research Issues and Application Examples," *International Journal of Automation Technology*, no. January, 2017.

[4] N. Tuptuk and S. Hailes, "Security of smart manufacturing systems," *Journal of Manufacturing Systems*, vol. 47, no. April, pp. 93–106, 2018.

[5] V. Watson, J. Sassmannshausen, and K. Waedt, "Secure granular interoperability with opc ua," in *INFORMATIK 2019: 50 Jahre Gesellschaft für Informatik – Informatik für Gesellschaft (Workshop-Beiträge)* (C. Draude, M. Lange, and B. Sick, eds.), (Bonn), pp. 309–320, Gesellschaft für Informatik e.V., 2019.

[6] J. Park and R. Sandhu, "The UCON$_{ABC}$ usage control model," *ACM Transactions on Information and System Security*, vol. 7, no. 1, pp. 128–174, 2004.

[7] U. Lang and R. Schreiner, "Proximity-based access control (pbac) using model-driven security," in *ISSE 2015* (H. Reimer, N. Pohlmann, and W. Schneider, eds.), (Wiesbaden), pp. 157–170, Springer Fachmedien Wiesbaden, 2015.

[8] B. A. Kitchenham, "Procedures for Undertaking Systematic Reviews," tech. rep., Keele University, 2004.

[9] P. Runeson and M. Höst, "Guidelines for conducting and reporting case study research in software engineering," *Empirical Software Engineering*, vol. 14, p. 131, Dec 2008.

[10] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," *Proceedings of the 52nd Annual Design Automation Conference on - DAC '15*, pp. 1–6, 2015.

[11] J. Q. Li, F. R. Yu, G. Deng, C. Luo, Z. Ming, and Q. Yan, "Industrial Internet: A Survey on the Enabling Technologies, Applications, and Challenges," *IEEE Communications Surveys and Tutorials*, vol. 19, no. 3, pp. 1504–1526, 2017.

[12] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial internet of things (IIoT): An analysis framework," *Computers in Industry*, vol. 101, no. June, pp. 1–12, 2018.

[13] 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*, vol. 54, pp. 1870–1880, March 2018.

[14] Y. Lu and F. Ju, "Smart Manufacturing Systems based on Cyber-physical Manufacturing Services (CPMS)," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 15883–15889, 2017.

[15] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid," tech. rep., SANS, 2016.

[16] J. Saltzer and M. Schroeder, "The Protection of Information in Computer Systems," in *proceedings of the IEEE*, vol. 63, pp. 1278–1308, September 1975.

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

[18] B. Leander, A. Causevic, and H. Hansson, "Applicability of the IEC 62443 standard in Industry 4.0 / IIoT," in *14th International Conference on Availability, Reliability and Security*, ACM, August 2019.

[19] D. Ferraiolo, R. Chandramouli, R. Kuhn, and V. Hu, "Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC)," pp. 13–24, 2016.

[20] "eXtensible Access Control Markup Language (XACML) version 3.0 plus errata 01," standard, OASIS, 2017.

[21] R. S. Sandhu and P. Samarati, "Access control: Principles and Practice," *IEEE Communications Magazine*, vol. 32, no. September, pp. 40–48, 1994.

[22] J. Lopez and J. E. Rubio, "Access control for cyber-physical systems interconnected to the cloud," *Computer Networks*, vol. 134, pp. 46–54, 2018.

[23] S. Salonikias, A. Gouglidis, I. Mavridis, and D. Gritzalis, "Access control in the industrial internet of things," in *Security and Privacy Trends in the Industrial Internet of Things* (C. Alcaraz, ed.), pp. 95–114, Springer International Publishing, 2019.

[24] E. Yuan and J. Tong, "Attributed Based Access Control (ABAC) for web services," in *Proceedings - 2005 IEEE International Conference on Web Services, ICWS 2005*, vol. 2005, pp. 561–569, 2005.

[25] Industrial Internet Consortium, "Industrial Internet of Things Volume G4 : Security Framework," Tech. Rep. IIC:PUB:G4:V1.0:PB:20160919, 2016.

[26] C. Faller and M. Höftmann, "Service-oriented communication model for cyber-physical-production-systems," *Procedia CIRP*, vol. 67, pp. 156–161, 2018.

[27] I. Ayatollahi, J. Brier, B. Mörzinger, M. Heger, and F. Bleicher, "SOA on smart manufacturing utilities for identification , data access and control," *Procedia CIRP*, vol. 67, pp. 162–166, 2018.

[28] "IEC 61449 function blocks," standard, Internation Electrotechnical Commission, Geneva, CH, 2012.

[29] Y. Demchenko, C. Ngo, C. De Laat, and C. Lee, "Federated access control in heterogeneous intercloud environment: Basic models and architecture patterns," pp. 439–445, IEEE, 2014.

[30] A. A. Almutairi and M. I. Sarfraz, "Access Control Architecture for Cloud Computing," *IEEE computer Society*, pp. 36–44, 2012.

[31] B. Anggorojati, P. N. Mahalle, N. R. Prasad, and R. Prasad, "Capability-based access control delegation model on the federated IoT network," pp. 604–608, IEEE, 2012.

[2] https://csrc.nist.gov/Projects/Policy-Machine