A Questionnaire Study on the Use of Access Control in Industrial Systems

Björn Leander[‡][†], Aida Čaušević[†], Tomas Lindström[‡], and Hans Hansson[†]
[‡] ABB Process Automation, Process Control Platform,
[†] Mälardalen University,
Västerås, Sweden
{bjorn.leander, aida.causevic, hans.hansson}@mdh.se, tomas.lindstrom@se.abb.com

***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.

I. Introduction

In our daily lives we depend on industrial communication systems being reliable, e.g., power and water supply, goods manufacturing, transportation of raw materials and goods. These systems are undergoing a transformation towards higher level of connectivity and complexity, as well as growth in size, related to the Industry 4.0 evolution. This development has great implications on the security characteristics of the systems, with e.g., expanding attack surfaces and less predictability of system behavior.

There are several initiatives related to increasing the overall cybersecurity posture of industrial networks, often with the focus on securing the network traffic. Limited work has been done in the area of access control related to industrial systems. Access control is one of the major security mechanism in any information system, used to uniquely identify actors and resources and enforce rules describing which users can access which resources. Functionality related to access control are of course already present in many industrial systems, but to what extent different methods are used, reasons for their use, and the general preparedness for the on-going evolution of industrial systems in general has not been investigated.

In this work we aim to study how different aspects of access control are used in industrial systems, and to understand the challenges in this area, based on responses from cybersecurity experts actively working with industrial systems. To that avail, we designed and performed a questionnaire study aimed at precisely that target population. The study focuses on three main topics: i) demographic properties as well as the cybersecurity process used within the organization, ii) authentication related aspects, and iii) use control. In this paper we will analyze only the first two topics.

A major source for guidance and certifications for cybersecurity used within Industrial Automation and Control Systems (IACS) is the IEC 62443 [1], [2] standard series. Sections 4-2 and 3-3 of the standard contain requirements and guidance related to system resp. component design, based on seven foundational requirements:

1) Identification and Authentication Control (IAC)
2) Use Control (UC)
3) System Integrity (SI)
4) Data Confidentiality (DC)
5) Restricted Data Flow (RDF)
6) Timely Response to Events (TRE)
7) Resource Availability (RA)

The focus of this paper is on the first of these foundational requirements (IAC), and its respective System Requirements (SR). Specifically we look at *SR 1.1 - Human user identification and authentication*, *SR 1.2 - Software process and device identification and authentication*, *SR 1.3 - Account management* and *SR 1.5 - Authenticator management*.

Several other standards are also available, related to different types of industrial system, e.g., [3], [4], [5], [6]. They all include similar requirements and guidelines related to identification and authentication. In this paper we choose to use the IEC 62443 standard as the main reference, as it is the most used standard among the respondents.

The rest of this article is organized as follows. In Section II related work is described. Section III summarizes the methodology and survey instrument design. In Section IV the results of the study are presented, while in Section V the implications of these results are discussed. Finally, in Section VI, we conclude the paper and indicate plans for future iterations.

II. Related Work

A. Questionnaire studies on cybersecurity in industrial systems

There are few survey studies related to cybersecurity in industrial settings. Both Prins *et al.* [7], and Ani *et al.* [8] investigate the cybersecurity awareness and capacity of employees working with industrial control systems, while Alcaide *et al.* [9] starts with similar questions, but puts focus on the maritime sector. Morris *et al.* [10] performs a combined survey and face-to-face study on cybersecurity knowledge-sharing in the automotive industry. All surveys investigate 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.

Franke *et al.* [11] look at the general state of cybersecurity within the Swedish manufacturing industry, partly overlapping the target population of our work. However, their study is on a very high level, not looking at any details with regards to technical solutions or future challenges. Moreover, respondents are typically not cybersecurity experts, but rather high-level managers or IT responsible.

This study is focusing on a specific category of the workforce, the appointed cybersecurity experts, and the questions are related to a rather narrow area of cybersecurity, i.e., access control. With this approach we are able to answer much more specific questions, related to what is actually used in Swedish industry, and what is the state of practice according to the practitioners. As far as the authors are aware, no such study has previously been conducted.

B. Access control in industrial systems

Access control is one of the basic security functions in any system, enabling access restriction to operations on resources only to legitimate authorized subjects. Access control can be split into three main subjects: identification, authentication and use control.

Quite a lot is written on the subject of access control in industrial systems, with recent works mainly focusing on evolving technologies and foreseen challenges related to the Industry 4.0 and Industrial Internet of Things (IIoT). The current state of the art for access control in IoT systems is surveyed by Ouaddah *et al.* [12], contrasting and evaluating available techniques. Similarly, Salonikias *et al.* [13] discuss the techniques, models and foreseen challenges related to IIoT systems.

Enforcement architectures for access control in modern industrial systems are discussed in a few articles, e.g., by Martinelli *et al.* [14] and Watson *et al.* [15], both discussing shortcomings and extensions of the Open Process Consortium Unified Architecture (OPC UA) [16], a communication protocol developed for component interactions in modern industrial systems with increasing popularity.

Policy models for industrial control systems are discussed in a few published articles, e.g., by Leander *et al.* [17], in relation to smart manufacturing and Bhatt *et al.* [18] related to the emerging Secure Smart Communities.

Works related specifically to access control in traditional industrial systems are not numerous, but e.g., the book by Knapp *et al.* [19] as well as the article by Dzung *et al.* [20] contain information on the subject.

However, none of the above listed works makes an attempt at describing what is actually used in industry based on the perception of practitioners. This study makes a clear contribution to this topic by providing some clarity on used standards and techniques, reasoning behind why they are used, and what the challenges are, from the practitioners perspective.

III. Research Methodology

When conducting this study, the guidelines provided by Linåker *et al.* [21] have been used as the main source for method on how to design the survey instrument, identify target population, and sample from that population.

A. Survey instrument design

The survey instrument is designed as an on-line web questionnaire using the QuestionPro website[1].

The instrument is separated into three main parts, the first one is related to demographic properties, e.g., a respondent role, primary business activity, and cybersecurity standards used. The second part focuses on questions related to authentication, i.e., methods for proving credentials, how unique identification of digital entities are done, etc. The last section contains questions related to use control, e.g., policy models used, enforcement methods used. In total the study consists of 41 questions, with an estimated time to complete of 15 minutes.

None of the questions are mandatory, allowing respondents to skip questions, but still complete the study. This strategy is used to minimize drop-outs due to difficult or sensitive questions.

B. Sampling strategy

The target population in this study is limited to engineers and managers working with cybersecurity in Swedish industry. Using a public database[2] of companies, 825 organizations have been identified as being potentially of interest, using the filtering criteria "category = industry AND no. of employees $>$ 100". Using a combination of available public contact information (cold-calls) and personal network connections (accidental sampling), respondents at 350 of these companies have been contacted. Invitations to participate in the study has been distributed using e-mails.

There are several weaknesses with this sampling strategy:

1) Since the target population is personnel working with cybersecurity in Swedish industry, not companies, it is impossible to say how large amount of the population is sampled, and if the sampled population is representative.

[1] Link: www.questionpro.com

[2] Link: www.allabolag.se

2) The database categorization “industry” has a quite imprecise definition, which includes some companies of no interest, and excludes a number of potentially interesting companies, e.g., service providers are not well represented in this register.
3) Using the threshold of companies with at least 100 employees also filters out several potentially relevant respondents, e.g., expert consultants are often employed in smaller companies. However, a limit is necessary to get a manageable base population.

The goal of the study is however not to do a quantitative analysis, but rather to get indications on the breadth and depth of used techniques and perceived challenges.

C. *Quality assurance*

To increase the quality of the survey instrument, a pilot group comprising six cybersecurity experts from both the academic and industrial field has been formed. This group has previewed the survey instrument and provided feedback in a number of areas, aiming for construct and content validity. The instrument design has been updated based on these comments, before being used on the sampled population.

IV. Results

In this section we present the results of the questionnaire, collected between 26th of February and 30th of March 2021. From the 350 invited organizations, 40 respondents have been reached, out of which 19 dropped out before finalizing the questionnaire, i.e., a 6% rate of complete responses, and replies from 2.5% of the total population of companies. As respondents have been allowed to skip questions, there are several cases of questions where the total number of responses are less than 21.

A. *Demography of respondents*

To be able to separate the received results into meaningful groups, and to analyze the composition of the group of respondents, the following questions related to demography have been asked:

Q1 What is the primary business activity of your organization?[3]
Q2 How many are employed in your organization?
Q3 In what country are you employed?
Q4 What is the main technical activity of your part of the organization?
Q5 What is your role within the organization?

Size and business activity (**Q1** and **Q2**) of the respondents' organizations are summarized in Figure 1. All respondents are, as expected, employed in Sweden (**Q3**), but several of these organizations most probably operate internationally.

The technical activity of the respondents organization (**Q4**) has been organised as a multi-select question, where 8 participants have indicated *owning or operating industrial systems*, 6 *developing components for industrial or vehicular system*, 6 *developing system solutions for industrial control systems or vehicles* and 5 *supplying services to industrial systems*. In the following diagrams we categorize respondents into the groups “Operation”, containing respondents that own industrial systems, and “Products and Services” for respondents providing services to industrial systems or are active in system or components development. In two cases there has been an overlap in this categorization, i.e., a respondent indicated both operating and developing or providing services to an industrial system. These two cases were categorized as “Operation”.

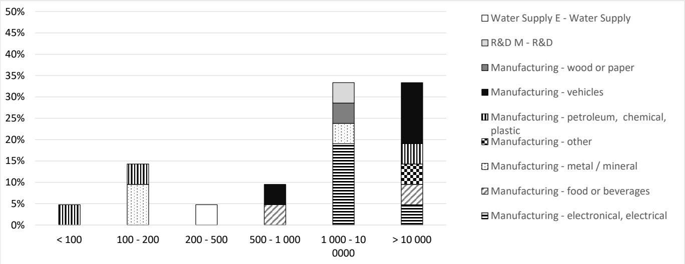

Fig. 1: Size of companies, grouped by business activity (**Q2**).

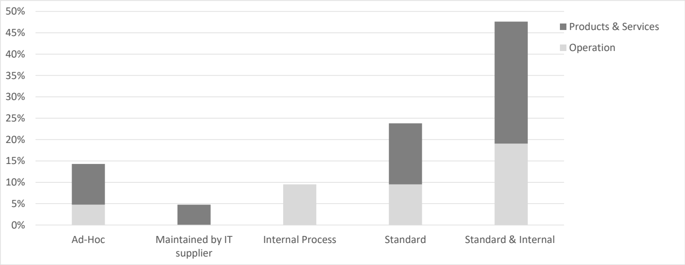

Fig. 2: Source for process used for systematic cybersecurity management (**Q6**).

The result of **Q5** shows that respondents are managers (8), cybersecurity experts (9), and engineers (4).

B. *Cybersecurity processes*

Cybersecurity is a continuous and iterative task, implying a need for a structured methodology when working with the subject in an industrial setting. To capture how and why respondents organizations are working with cybersecurity, the following questions are asked:

Q6 How does your organization work systematically with cybersecurity?
Q7 Which, if any, industrial standards / guidelines for cybersecurity do you use in your organization?
Q8 Why is this specific standard chosen?

Results for question **Q6** are illustrated in Figure 2, with a majority of respondents indicating that a standard or a combination of standard and internal processes is used for guiding systematic work with cybersecurity (approximately 70%). Around 10% of the respondents are using internal processes, but without connection to a well-defined standard or a guideline. Out of the all respondents, 15% indicated that

[3] Based on the EU RAMON Statistical Classification of Economic Activities in the European Community, NACE Rev. 2 https://ec.europa.eu/eurostat/ramon/nomenclatures/

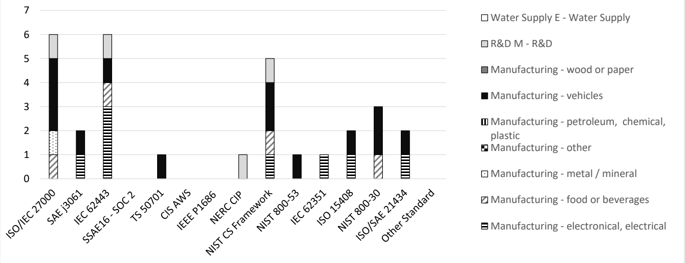

Fig. 3: Use of specific standard (**Q7**).

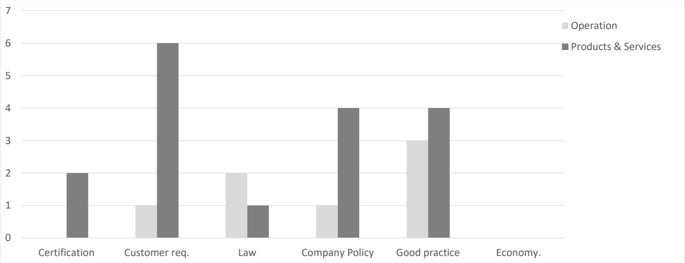

Fig. 4: Indicated reasons for selecting a standard (**Q8**).

they do not follow defined process when working with cybersecurity. In some of the following diagrams the responses are grouped based on respondents utilization of a standard, with the category "Standard" representing respondents indicating using a standard or a combination of a standard and an internal process, and the category "No standard" representing all other respondents.

The respondents indicating using a standard or a combination of standard and internal process could answer the follow-up questions related to used standard (**Q7**) and the reason for using a standard (**Q8**). Results for **Q7** are summarized in Figure 3, and for **Q8** in Figure 4. 45% of respondents that confirmed working with standards indicated using several of the listed standards, 20% use one of the listed standards and the remaining 35% have not indicated which standard is used.

Question **Q8** allowed multiple answers, so each respondent could pick several reasons for choice of standard / guideline.

C. Identification and Authentication

Questions related to identification and authentication have been partitioned in three parts: (1) likelihood and impact related to privilege escalation attacks, (2) identification and authentication of human users, and (3) identification and authentication of digital entities. Questions and corresponding answers are illustrated in the following.

1) Likelihood and impact of a privilege escalation attack:

Q9 What impact could a privilege escalation attack potentially have on your system/product(s)?
  a) From a safety perspective.
  b) From a security perspective.

Q10 How likely do you consider such a privilege escalation attack to be?

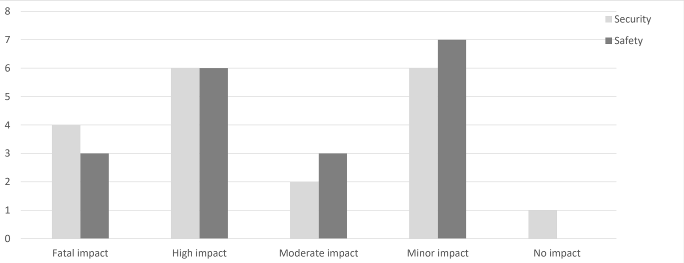

Fig. 5: Perceived impact of a successful privilege escalation, on security and safety respectively (**Q9**).

Results of this section are illustrated in Figure 5. The respondents have been asked to grade on a scale from "Fatal" to "No impact" the seriousness of a potential privilege escalation attack, from security and safety perspectives, respectively. In Table I and Table II the impact on security and safety are correlated with the respondents perception of the likelihood of a successful attack.

Likelihood / Impact	Fatal	High	Moderate	Minor	No Impact
High Risk	1	1	0	0	0
Medium Risk	3	2	0	2	0
Low Risk	0	3	2	4	1

TABLE I: Impact on cybersecurity vs. likelihood of an attack.

Likelihood / Impact	Fatal	High	Moderate	Minor	No Impact
High Risk	0	2	0	0	0
Medium Risk	3	1	3	0	0
Low Risk	0	3	0	7	0

TABLE II: Impact on safety vs. likelihood of an attack.

2) Identification and authentication of human users: Two questions have been asked in this section:

Q11 Does your system or component use unique identification of human users?

Q12 What method(s) are used for authentication of human users?

Results for question **Q11** are illustrated in Figure 6. In question **Q12**, the respondents answering "Yes" to the previous question (**Q11**) have been able to indicate which methods are used for authentication, see Figure 7. Available choices included *Username/Password*, *Physical key or token*, *Self-signed certificates*, *PKI-based certificates*, *Biometric methods*, *Multi Factor Authentication (MFA)*, *Single Sign On (SSO) - identity proven by external system*, and *Other*.

3) Identification and authentication of digital entities: The following questions have been asked within this survey section:

Q13 Do your product(s)/system use unique identification for digital entities, e.g., devices, software services, etc.?

Q14 What type of digital entities are identified?

Q15 What method(s) are used for authentication of digital entities?

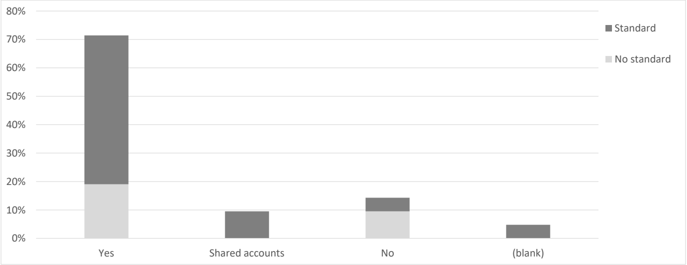

Fig. 6: Usage of unique user identification (**Q11**).

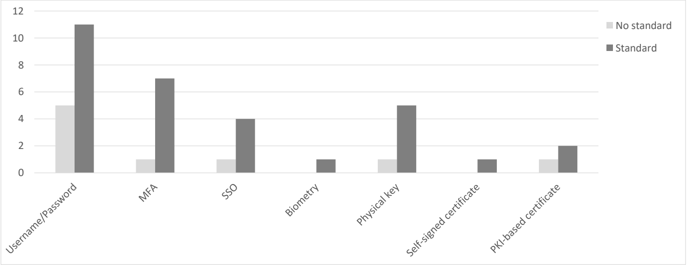

Fig. 7: Methods used for user authentication (**Q12**).

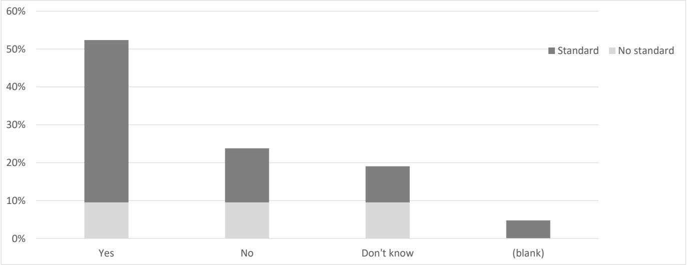

Fig. 8: Usage of unique identification for digital entities (**Q13**).

Only respondents answering "Yes" on question **Q13** could answer the follow-up questions. For both of the questions **Q14** and **Q15** multiple answers could be selected.

Results for question **Q13** are illustrated in Figure 8. Question **Q14** results are shown in Figure 9, with Devices, Applications, Application Endpoints and Other being the possible options. Results for question **Q15** are illustrated in Figure 10, with the options Shared secret (e.g., password), Self-signed certificate, PKI-certificate and Other. No respondent indicated "Other" on any of the two follow-up questions.

D. Perceived challenges in the area of identification and authentication

Related to future challenges that respondents see in the area of identification and authentication, we have asked the following question:

Q16 What challenges do you see in your field/industry related to identification and authentication?

The respondents have been able to answer in a free-text form, where 10 of them have answered to this question. For respondents privacy reason, the results are reported in an aggregated form. The following common themes have been identified (number in the brackets represent number of respondents answering within that theme):

T1 Cost related to inclusion of secure HW components. (2)
T2 Cost of account management. (2)
T3 Increasing system complexity. (2)
T4 Lack of technical support and standardization. (3)
T5 Improper use of methods. (3)
T6 Regulations related to open market making implemented methods ineffective. (1)
T7 Increasing amount of cyber-attacks. (3)

V. Discussion

One hypothesis generated from this work is that the adaption and use of a standard or well defined guidelines could be a determinant for cybersecurity maturity, specifically in the case of authentication. To define cybersecurity maturity in a form identifiable in the results of this questionnaire is not straightforward, but some indicators are quite obvious. Using unique identification for human users and digital entities respectively are two such indications. The use of some of the more advanced techniques is another indicator, such as certificate-based and multi-factor authentication.

Secondly, related to preparedness for the evolving IIoT, the hypothesis is that the systems and components that the respondents refer to in their replies use no or a very limited set of IIoT technologies. To infer this from the results of the survey is not possible, but there are some indications pointing in that direction, which will be discussed in the following.

A. Cybersecurity Management, used standards

The underlying rule-book being used in an organizations' cybersecurity process could have an impact on which and how techniques are used within the products or systems that the organization own or produce. There are several well defined cybersecurity standards useful in industrial settings.

Among the respondents a majority (approximately 70%) indicate using a standard, or the combination of a standard and an internal framework as part of their cybersecurity management system. One expectation has been that the business activity would reflect which standard is used, as different standards are oriented towards different types of systems. However, this is not clearly visible in the data, e.g., respondents from manufacturing of vehicles indicate using 9 out of the 14 listed standards and guidelines. One trend is however clear: no respondent was aware of using any of the two listed guidelines related to cloud security (SSAE16 SOC 2 [22] and CIS AWS [23]). This is traditionally out of scope for an industrial system, but with the currently evolving IIoT, cloud interactions and cloud services are increasingly important parts of these systems.

The most popular standards among the respondents are the ISO/IEC 27000-series (a collection of several related standards) and IEC 62443 [1], being equally popular, followed by the NIST Cybersecurity Framework [24].

Several of the respondents confirm using a standard, without selecting any of the listed alternatives. This might indicate that some of the used standards have been left out of the list, e.g., relating to the petrochemical industry, where the majority of respondents replied they were using a standard, but no one indicated which one. The option to enter additional standards in a free-text field was however not used by any of the respondents, so possibly some respondents just did not know which of the standards they use.

The answers on question **Q8**, reasons for selecting a specific standard or guideline, indicate an expected difference between organizations operating a system compared to organization providing products or services. For products and services providers, the indicated reasons are mainly related to customer requirements, followed by internal company policies and as an aid assuring usage of well known and tested practices. For operations of industrial systems, following a good practice and adherence to law are the two top reasons, among the respondents active in that category.

Certification is used only by a small number of respondents as a reason to follow a standard. A trend that we have anecdotal experience of is that customers within specific sectors are increasingly requiring adherence to a standard, and that certification (e.g., CSA [25] for IEC 62443-4-2) according to the standard is a prerequisite to be able to sell products in these businesses. The indication that customer requirements are the most important reason for products and services suppliers choice of a standard may be related to this trend. This is, however, not possible to infer from this study. An in-depth study into organizations reasons for using a standard could provide evidence strengthening or weakening this assumption.

Three respondents indicated that usage of the standard has been mandated by law. This is an interesting result, as in Sweden there are no such laws, mandating adherence to specific standards. The only standard among the listed ones that is mandated by a law in any country, as far as the authors are aware of, is the NERC CIP, required for systems being used together with power transmission in the USA. However, there is no overlap between respondents using the NERC CIP standard, and respondents being mandated to follow a standard because of law requirements.

In the European Union, there is a directive on Network and Information Security (NIS)[4], corresponding to laws in the member states, mandating organizations operating critical infrastructure to work with cybersecurity in a structured way, to e.g., allow coherent incident reporting. This directive does not require adherence to a specific standard, but following a standard may be used to demonstrate compliance. Investigation of the potential connection between the adaption of standards among organizations operating critical infrastructure, and the NIS-directive could be an interesting continuation of this work.

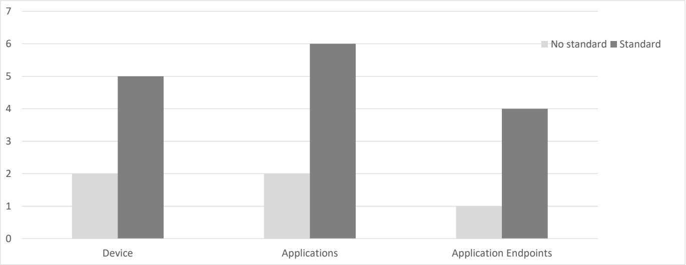

Fig. 9: Type of digital entities that are identified (**Q14**).

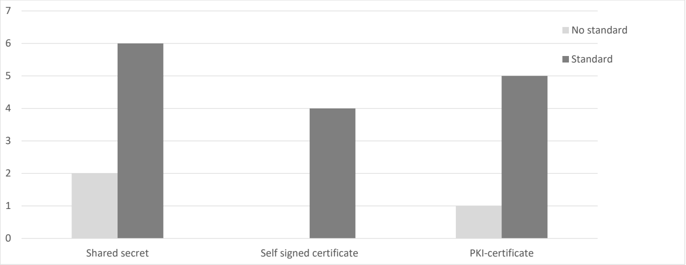

Fig. 10: Methods used for digital entity authentication (**Q15**).

B. *Identification and Authentication*

A fundamental requirement for use control in any system is that involved parties can be uniquely identified and that there is a method for providing proof of identity, i.e., authentication. The authenticated subject is granted privileges in the system, meaning that the impact of an privilege escalation attack could be substantial, as indicated by the respondents. 12 out of 19 participants in the study indicate moderate to fatal impact on safety as well as security measures of a successful privilege escalation attack. However, the likelihood of a successful attack is perceived as being low by the majority of the respondents (10 out of 19).

Looking at the combination of likelihood and impact, there is some correlation (see Tables I, II) between respondents indicating moderate to fatal impact to also indicate a higher likelihood of an attack. Among the 12 indicating moderate to fatal impact, 9 indicated a medium to high likelihood, while all of the 7 indicating a minor impact also indicated a low likelihood of an attack.

According to *SR 1.1 - Human user identification and authentication*, the system shall provide the capability to identify and authenticate all human users, however, allowing for use of shared accounts in systems where human users functions as a single group for lower security levels.

A clear majority of respondents indicate using unique identification of human users (more than 70%). One out of the 15 study participants using a standard answered “No”, while the number of those not using a standard is 2 out of 6, indicating a slightly higher adaption of unique human user identification in the group of respondent working according to a standard. The use of shared accounts are indicated as being common practice by approximately 10% of the respondents. This would typically be the case for systems with no cen-

[4] DIRECTIVE (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union

tral user management. Worth noticing is that no respondent answered *Don't know* on this question.

Similar to the previous requirement on human user identification, *SR 1.2 - Software process and device identification and authentication* stipulates identification and authentication of all software processes and devices, required for security level 2. For security level 3 and 4, unique identification of all software processes and devices is required.

About 50% of the respondents answered that they use unique identification for digital entities. What is meant by unique identification in this case may be a bit unclear, which can explain this relatively low number. For example, most digital devices in an industrial system will hold an unique identity based on e.g., the serial number of the device or its logical (e.g., IP address) or physical location. However, these identities may be impossible to authenticate.

A much higher level of uncertainty can be seen among the respondents related to the question of unique identity for digital entities, as almost 20% answered *Don't know*. There seems to be a skew toward the participants using a standard having a slightly higher level support for identification of digital entities, with 9 out of 15 in that group answering *Yes*, compared to 2 out of 6 in the group not using a standard.

The methods used for authentication is related to *SR 1.5 - Authenticator management*. Authenticators include tokens, certificate-based keys, biometrics, password, physical tokens etc. For the highest security levels, there is a requirement on hardware mechanisms for protection of authenticators.

Among the techniques used for authentication of human users, *Username/Password* is an expected top candidate. The full breadth of methods for authentication is found in the group of respondents using standards. *Multi-Factor Authentication (MFA)*, is indicated as being used for human authentication by several of respondents' systems or components. According to SR 1.1, MFA is a requirement enhancement for security level 3, for untrusted networks, and level 4 for all networks. It is uncertain to what extent MFA is actually used by the respondents' components, on what interfaces, etc.

The techniques used for authentication of digital entities, as well as types of identifiable digital entities are quite evenly spread among the respondents. Usage of *shared keys* is the most common technique for entity authentication among the respondents, and *applications*, *application endpoints* and *devices* being almost equally common as identifiable entities. The usage of hardware mechanisms for safeguarding the authenticators used for digital entities could be a possible area of further inquiry, which is not measured in this study.

C. Perceived challenges

Analyzing the perceived challenges indicated by the respondents, it becomes clear that they see increasing costs related to components (theme **T1**) as well as management effort (**T2**, **T3**) in relation to identification and account management. This may be an effect of increased system complexity driven by the Industry 4.0 evolution, but also requirements related to evolving best practices. E.g., the cost for changing from shared user accounts to unique user accounts puts a significant additional burden on the account management process.

The heterogeneity of the future industrial systems is seen as a big challenge (theme **T4**), with different component manufacturers choosing incompatible technical solutions. A lack of standardization is mentioned by several respondents as an issue hampering effective account management in industrial systems. Interestingly, there are several on-going efforts aiming for convergent and operable standards being used in industrial system, e.g., the Open Process Automation Standard[5]. Possibly the respondents have limited knowledge of these efforts, or are skeptical to their level of success.

Three of the themes implies direct threats to the integrity of the industrial systems. Theme **T5** indicates a lack of technical maturity leading to improper usage of the available methods. Theme **T6** indicates that "right to repair"-regulations may force manufacturers to include mechanisms which could make authentication less secure. The theme **T7** related to cybersecurity attacks on industrial systems are possibly worsened by the previous two, as the likelihood of a successful attack will increase with improperly configured systems or inherently vulnerable mechanisms. Cybersecurity attacks and information leakages in other seemingly unrelated systems may have collateral impact also on industrial systems using unique user identifications, as password re-use over several platforms is a common issue.

The perceived challenges illustrate the on-going technical shift from isolated to increasingly interconnected systems, with a resulting complexity and heterogeneity that currently used solutions cannot handle, requiring investments both related to technical components and system solutions for account management. The fear is that lack of standardization and improper usage of technical solutions may lead to more vulnerable systems, consequently increasing the likelihood of successful cybersecurity attacks.

D. Discussion on validity and reliability

Validity concerns about whether the study measured what it meant to measure. In this case, the study is hypothesis generative, meaning no *a priori* hypothesis has been formulated. However, the questionnaire is formulated with a clear target population in mind, experts within the area of cybersecurity in industrial systems, and with a clear subject, that of access control within industrial systems. The questionnaire has been evaluated using a pilot study to minimize the risk of bad formulations, missing alternatives, etc., as a way of lowering the potential threats to content and construct validity of the questionnaire instrument.

The results of a questionnaire study are reliable if the results can be generalized to the whole population, i.e., if performing the same study on another sample of the population, a similar distribution of answers would be the result [21]. In this study a clear threat to reliability is the low response rate, and the skew among the respondents towards working mainly in large

[5] Link: publications.opengroup.org/c19f

companies. The low number of participants and the unbalance among the participants constrain any generalized claims from this study.

VI. Conclusions

Cybersecurity is of growing concern for industrial systems, and access control is one of the fundamental mechanisms for providing security in these systems. However, access control is relatively immature in the traditional industrial systems, as compared to modern IT systems. In this paper we have provided the results of a questionnaire study on the usage of access control within industrial system being developed, serviced or operated by Swedish organizations.

Standards and guidelines are used by many of the respondents, with 11 out of the 14 listed standards in use by one or more of the respondents, essentially only leaving the guidelines related to cloud-security out. The number of different standards covering similar topics may seem redundant, but the fact that so many are used by practitioners indicates their relevance. Different needs are covered by different standards.

For identification and authentication of human and digital entities, the full breadth of techniques is used by the respondents. There is a skew towards the respondents following a standard that is more mature in this sense, as these respondents to a higher degree have indicated using and adapting the more advanced techniques to a higher degree.

The respondents acknowledge that a successful privilege escalation attack may have dire consequences on security as well as safety measures, but rate the likelihood of such attack occurring as rather low. The reasoning may be that industrial systems are still seen as quite isolated. Looking at the perceived challenges, this assessment is likely to change in the future.

As this study is hypothesis generative, the natural continuation is to investigate the hypotheses in more detail. We plan to perform an in-depth interview study with a selection of cybersecurity experts related to reasoning behind selecting usage of standards, some of the specific techniques used and the perceived development of challenges related to the evolving characteristics of future industrial systems.

A. Limitations

As already discussed, the low and unevenly distributed response rate hampers generalization on the results of this study. Engaging people in on-line surveys are difficult. The area of the study is quite technical and seen as sensitive, indicated as a reason for non-participation by some respondents. Consequently, the results presented are based on a rather small percentage of the total population. The sampled population is limited to industrial systems being developed, serviced or operated by Swedish companies.

Despite the limitations, this study provide indications on the breadth of used technologies and standards, and present challenges from the perspective of practitioners in the field of industrial systems security, which was the goal of this work.

Acknowledgements

This work is supported by ABB AB; the industrial postgraduate school Automation Region Research Academy (ARRAY), funded by The Knowledge Foundation; and the European Union's Horizon 2020 ECSEL JU project InSecTT under grant agreement No 876038[6]. The authors would like to acknowledge Judith Rossebø and Oliver Lindberg for their feedback.

References

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

[2] 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.

[3] "SAE j3061, cybersecurity guidebook for cyber-physical vehicle systems," standard, SAE International, 2016.

[4] NERC, "NERC CIP Standards." http://www.nerc.com/pa/Stand/pages/cipstandards.aspx, 2019. [Online; accessed May 9, 2019].

[5] NIST, "Security and Privacy Controls for Information Systems and Organizations," tech. rep., National Institute of Standards and Technology, Gaithersburg, MD, sep 2020.

[6] "IEC 62351 - power systems management and associated information exchange," standard, Int. Electrotechnical Commission, Geneva, 2021.

[7] 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*, vol. 2020-June, 2020.

[8] 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*, vol. 21, no. 1, pp. 2–35, 2019.

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

[10] D. Morris, G. Madzudzo, and A. Garcia-Perez, "Cybersecurity threats in the auto industry: Tensions in the knowledge environment," *Technological Forecasting and Social Change*, vol. 157, no. May, 2020.

[11] 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.

[12] 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*, vol. 112, pp. 237–262, 2017.

[13] 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 IoT*, Springer Int. Publishing, 2019.

[14] 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.

[15] 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)*, 2019.

[16] "IEC 62541 OPC unified architecture," standard, Internation Electrotechnical Commission, Geneva, CH, 2016.

[17] B. Leander, A. Čaušević, H. Hansson, and T. Lindström, "Access control for smart manufacturing systems," in *Software Architecture*, pp. 463–476, Springer Intl. Publishing, 2020.

[18] S. Bhatt and R. Sandhu, "Convergent Access Control to Enable Secure Smart Communities," pp. 148–156, 2020.

[19] E. D. Knapp and J. T. Langill, *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Syngress, 2014.

[20] D. Dzung, M. Naedele, T. P. Von Hoff, and M. Crevatin, "Security for industrial communication systems," *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1152–1177, 2005.

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

[22] "SOC2 - SOC for Service Organizations: Trust Services Criteria." https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html, 2021. [Online; accessed April 29, 2021].

[23] CIS, "CIS AWS Benchmark." https://www.cisecurity.org/benchmark/amazon_web_services/, 2019. [Online; accessed May 4, 2021].

[24] NIST, "NIST Cybersecurity Framework." https://www.nist.gov/cyberframework, 2020. [Online; accessed April 29, 2021].

[25] "IEC 62443-4-2 - Component Security Assurance (CSA)." https://www.isasecure.org/en-US/Certification/IEC-62443-CSA-Certification, 2021. [Online; accessed May 7, 2021].

[6] The document reflects only the author's view and the Commission is not responsible for any use that may be made of the information it contains.