http://dx.doi.org/10.25673/39569

Secure Usage of Asset Administration Shells - An Overview and Analysis of Best Practises

Andre Bröring, Marco Ehrlich, Henning Trsek, Lukasz Wisniewski
Technische Hochschule Ostwestfalen-Lippe
inIT - Institute Industrial IT

Campusallee 6
32657 Lemgo, Germany
andre.broering@th-owl.de
marco.ehrlich@th-owl.de
henning.trsek@th-owl.de
lukasz.wisniewski@th-owl.de

The Asset Administration Shell (AAS) is a core element for Industrie 4.0. In addition, the security of industrial systems is a permanent topic that could be improved by the AAS and should have a high priority for future developments and implementations of the AAS. This paper evaluates the current threat landscape for Industrial Control Systems (ICS) communicating to the AAS, as well as for IT systems hosting the AAS. The relevance of these threats is evaluated for the AAS and the threats with the highest relevance, namely Basic Web Application Attacks and Malware Infections, are analysed in detail. The recommended countermeasures for these threats are compared with the state of the art of AAS security concepts and result in missing countermeasures and research gaps for an overall security of the AAS.

1 Introduction

The current progress within the developments of the Industrie 4.0 (I4.0) offer a great potential to increase the digitalization and to support new technologies in the area of industrial automation. The upcoming data-driven systems and innovative services are the basis to link virtual and physical processes as a fundamental concept of I4.0 [WSJ17]. This is mostly done by the adaptation of interconnecting approaches from the Information Technology (IT) domain into the environment of Operational Technologies (OT). Ubiquitous connectivity is the general enabler required by the majority of future industrial applications. In general, these trends demand for new possibilities with regard to data acquisition, processing, and utilization, resulting in a higher priority for the intrinsically linked topic of security as well.

The Asset Administration Shell (AAS) as a promising concept in this area is designed to be the future repository for all relevant information related to industrial assets. The AAS can be exchanged as a file, but can also have different communication capabilities to communicate to the represented asset itself and provide information to other services inside organizations or across company boarders [Pla20b]. In a positive scenario, the AAS can help to create future secure industrial production systems, e.g. by providing monitoring information like behaviour anomalies of the represented physical system to detect potential security-related attacks [DP20, EE18]. In a negative scenario, the universal communication capabilities and the overall available information about each asset centralized in the AASs could become a new vulnerability for industrial organizations [HR19]. In this case, a security incident including access to the AASs could have a tremendous impact. Besides manipulations and data leaks, an attacker can use the crucial information about the production system from the AAS for further attacks and exploits that could lead to further loss of intellectual property or production unavailability, like during the shutdown of the Colonial fuel pipeline in the USA in May 2021 [NTE21].
Up to now, a threat analysis for the AAS in all asset life cycle phases covering different scenarios does not exist. On the one hand, the AAS concept has a deep relevance towards the IT domain because of the used technologies. On the other hand, the AAS is specified to function inside the OT domain for industrial automation systems. This creates a tension with regard to the required type of security evaluations, the applicable threats, the general security objectives, and the available countermeasures. The current status of the security-related development of the AAS already covers various concepts and implementations. Nevertheless, an overview of the available functionalities and the subsequent mapping towards present threats and available countermeasures are missing. The results of this work are an evaluation of the security capabilities of the AAS in order to withstand the current threat landscape and the conclusion of open research challenges for future activities in this domain. The remainder of this work is organized as follows: Section 2 further introduces the current state of the art of the AAS, security capabilities of the AAS, and supporting topics. Afterwards, Section 3 presents the current threat landscape endangering AAS implementations and assess the available countermeasures. Section 4 concludes this work by displaying a summary and the outlook containing future work in this research domain.

2 Background

This section gives a short overview of the concepts of the AAS and the state of the art of AAS security from the Plattform I4.0 as well as other research domains.

2.1 The Asset Administration Shell (AAS)

During the life cycle of an asset, all information about the asset can be stored in the AAS. This can be construction data of a machine from engineering tools, values from installed sensors of a machine during operation, or a description of executed process

steps for maintenance tasks. All this data about the assets is stored in a standardized structure and enables the access of data about every asset and data exchange between AASs in a harmonized way with the AAS files or via the APIs [Pla20a]. One asset can have one or multiple AASs referring to each other, which can be stored in different locations and different kinds of storage, such as in an embedded storage on the asset itself, in edge or in cloud storages [Pla17, Pla20b].
The AAS has three different levels of data exchange capabilities and interaction patterns. The first one, called passive AAS, is a simple file containing the AAS and can be exchanged along the whole life cycle of the asset [Pla20a]. The re-active AAS has a standardized communication interface described in a technology-neutral specification and can be realized with an HTTP REST, OPC UA, or MQTT API [Pla20b]. The communication capabilities ensure a seamless communication to the OT networks of a plant containing various assets like Programmable Logic Controllers (PLCs) and Human Machine Interfaces (HMIs), as well as to the IT networks for engineering and life cycle management tools, data-driven services, or Manufacturing Execution Systems (MESs). Independent of the storage location, the AAS may need to have the same communication possibilities to the IT and OT networks, even across company boarders.
The third type of AASs, called pro-active AAS, autonomously and pro-actively interacts with other AASs in peer-to-peer communications using the I4.0 language [Pla21a]. This paper considers only the passive and the re-active AAS, due to simplicity because of the current development status of pro-active AASs.

2.2 Asset Administration Shell Security

The published security concepts for the AAS are considered and summarized in this chapter. Before the Industrial Digital Twin Association (IDTA) was founded, the Plattform I4.0 was the main driver of the AAS and published security requirements, concepts, and approaches in several specifications and discussion papers.
In general, in the current implementations of re-active AASs, a server application, such as the AASX Server, can load the AASX file and provide the information via an HTTP REST or OPC UA API [Ind21]. Hence, the AAS is not communicating by itself, but loaded into an application to enable the communication. As a result, not only the AAS itself, but also the tools and applications interacting with the AAS and providing the API need to be taken into account for the secure usage of AASs [Pla21b].
To share passive AASs with business partners, an AAS provider can share a copy of the file, in that confidential data is missing. If the data provider does not want to create several copies with individual information, or wants to keep some information inside the AAS to share this later, access control comes into play. According to IEC TS 62443-1-1:2009, access control is the “protection of system resources against unauthorized access”. The access control management for the AAS includes the management of read access, write access, and write access in a limited value range [Pla17].
In the beginning, Role Based Access Control (RBAC) was proposed for the AAS [Pla17]. However, later, Attribute Based Access Control (ABAC) was defined as the preferred

solution for the AAS in cross-company communication scenarios [Pla19a]. The permission rules for the access control are stored and exchanged within the AASs itself and can be provided by the asset manufacturer. Nevertheless, the receiver of an AAS can also set own access permission rules. Based on the subject attributes, object attributes, and environmental attributes, the access permission rules are evaluated locally to decide if the access is allowed or declined. Prerequisite for the access control are unique identities and an identity management in a secure environment to identify the subjects that want to access the AAS and the objects, such as the whole AAS or submodels, that should be accessed. Details about this secure environment for digital identities are mentioned for further development [Pla17, Pla20a].
A detailed description for an exemplary secure download service including authorization and authentication of a requester as well as the transfer of the AASX files containing custom non-public data from a supplier to the requester, such as an AAS integrator, is described by the Plattform I4.0 [Pla20c]. With a signature of the AAS provider for the AASX package, integrity and confidentiality can be ensured during file transportation [Pla20a]. The security of the AAS after download is not considered.
In the research domain, different ways to share and manage AASs via distributed systems are proposed. First, there is a concept to store the AAS in a distributed file system in combination with a git-based version control and a blockchain-based tamper-proof log [RVPK20]. In a second work, the data itself or a checksum of the data, such as a submodel, is directly shared via a distributed ledger to ensure a high integrity of the data [BBT+21]. On one hand, the distributed solutions prevent single points of failure. In addition, the access for different business partner as well as measures to ensure integrity and confidentiality by encryption are core features. On the other hand, the copies of the data in the distributed network are beyond an owner's control.
In cross-company communication scenarios, the HTTP protocol is recommended and well-established. The integrity, confidentiality, and authenticity of these connections should be ensured on the application layer to avoid an interrupt because of inspecting proxies on the transport layer (TLS proxies) used in many company networks. The availability depends on the physical and the MAC layer, realized as wireless and wired connections [Pla17, Pla20c]. A prototypical implementation of such an HTTP REST server for re-active AASs is already realized in the open-source AASX server [Ind21]. Similar to the secure download service, an authentication server provides access tokens to access objects via the HTTP REST interface of the AASs.
As an alternative to HTTP REST, the Plattform I4.0 provides functionalities for the communication with endpoints outside the organization's networks using OPC UA with direct server-client connections to the assets, or aggregation servers to bundle several OPC UA connections for the cross-company communication [Pla19b]. These methods can be applied to the OPC UA connections of re-active AASs.
Lastly, all accesses to functions and values of the AAS should be logged by the AAS to help to identify manipulations on the AAS. Other security measures, such as data usage control and data origin tracking, are mentioned for further development [Pla17, Pla20a]. Also in future, the security capabilities and especially trustworthiness level of an AAS should be rated on a not-yet-defined scale and delivered by the asset manufacturer [Pla17].

3 Threat Landscape Analysis

After introducing and explaining the fundamental background with regard to the AAS security, this section contains the analysis of the current threat landscape for industrial environments. Security-related threats build up the basis for the strictly needed risk assessment processes later on. The gained insights will be mapped to the current state of the AAS security development in order to check which threats are already considered. In addition, this section includes the comparison of AAS-related threats and the currently available countermeasures. This leads to open challenges aiming at follow-up research directions with regard to the further development of the AAS security concepts.

3.1 Threat Analysis

The current threat landscape endangering and affecting the industrial automation domain is broad and diverse with regard to attack vectors, attackers, and possible compromising approaches [PK18]. As a basis, the "Industrial Control System Security Top 10 Threats and Countermeasures 2019" published by the Federal Office for Information Security (in German BSI) [Bun19] are further investigated in Table 1. Recent incidents show the interconnection of the IT and OT domain, similar to the concept of the AAS. Therefore, the Verizon Incident Classification Patterns [Ver21] that are typical for IT systems are added. Four duplicated threats from these two sources are merged, and the remaining three added to the BSI ICS Top 10. The AAS-specific relevance (Relev.), meaning that the AAS is affected by the threat, is rated between low, medium, and high. The threats with a high relevance have a high effect on the AAS security and are analysed in detail in Section 3.2. The threats with a low relevance can be mitigated on an organization level, as shown below.

The threats *Lost and Stolen Assets* as well as *Infiltration of Malware via Removable Media and External Hardware* have no specific relevance for the AAS, as it is not a hardware component which can be stolen, or to which removable media can be connected to. Further, *Privilege Misuse*, that mainly originates from internal threat actors [Ver21], *Human Error and Sabotage*, and *Social Engineering and Phishing* have no direct relevance, as human interaction is not a key feature of the AAS and the corresponding countermeasures, such as awareness training, are on an organizational policy level. Nevertheless, the mentioned threats can have an impact on the AAS security, as these are all possible entrance points for exploits also affecting AASs.

Technical Malfunctions, Force Majeure & Miscellaneous Errors are general threats that are relevant for the particular software implementations hosting or interacting with the AAS. The *Compromising of Extranet and Cloud Components* is also a threat that is not AAS-specific. Both are out of scope of this paper and the corresponding countermeasures from the BSI [Bun19] can be applied organization-wide. In addition, GAIA-X as a future European cloud infrastructure [GX21] could contribute a secure and sovereign storage infrastructure for the AASs.

Table 1: BSI ICS Top 10 [Bun19] and Verizon Incident Classification Patterns [Ver21]

Threats and Incident Classification Patterns	**Relev.**
Basic Web Application Attacks Malware Infection via Internet and Intranet & System Intrusion	high
(D)DoS Attacks Control Components Connected to the Internet Intrusion via Remote Access Compromising of Smartphones in the Production Environment Technical Malfunctions, Force Majeure & Miscellaneous Errors Compromising of Extranet and Cloud Components	medium
Privilege Misuse Social Engineering and Phishing Human Error and Sabotage Infiltration of Malware via Removable Media and External Hardware Lost and Stolen Assets	low

For *Intrusion via Remote Access*, *Control Components Connected to the Internet*, and *Compromising of Smartphones in the Production Environment*, the AAS could even be part of a security enhancement solution, as it could replace direct connections between the asset and remote access providers, the Internet or smartphones. The AAS can be a standardized interface collecting the data from the assets and providing this to the external endpoints. In this case, the AAS interfaces could be patched more easily than the industrial assets supporting the security measures with more secure interfaces to external endpoints compared to the worse patched ICS interfaces.
In the same manner, the AAS could reduce the impact of *(D)DoS Attacks* targeting the ICS, as the direct accessibility of the ICS can be replaced by the AAS interface. However, the AAS could still be a target for (D)DoS attacks, so that the implementation of countermeasures is recommended, such as the hardening of network access points and communication channels, installation of intrusion detection systems, and redundant connection of components using different protocols [Bun19].

3.2 Detailed Threat Analysis

The remaining threats with a high relevance for the AAS are exemplified here in detail, with an outlook on exiting and missing countermeasures. Table 2 shows an excerpt of the most AAS-relevant countermeasures from the BSI [Bun19] and IEC 62443-4-2. The last column marks, if the corresponding countermeasures are already implemented for the AAS "✓", if at least concepts for the countermeasures do exist "(✓)", or if it is not yet considered "-".

Basic Web Application Attacks A typical way to compromise data from a victim are the *Basic Web Application Attacks*. This is a hacking method and acts as an entrance for further attacks, such as malware or (D)DoS. The Verizon "DBIR 2021

Table 2: Countermeasures from BSI ICS Top 10 and IEC 62443-4-2

Countermeasure	**AAS**
Standardised interfaces to reduce undiscovered ICS vulnerabilities	✓
Identification, authentication, and access control	✓
Limitation of available information	(✓)
Logging, monitoring, and attack detection	(✓)
Provisioning supplier roots of trust	(✓)
Secure communication	(✓)
Network segmentation	-
Antivirus software	-
Periodical backups (data recovery)	-

Data Breach Investigations Report" shows that servers are the most likely affected assets for security breaches in all industries and security incidents in most industries. The main sub-pattern are stolen credentials and brute force attacks [Ver21]. The re-active AAS could be a future target for this kind of attacks.
The AAS itself as a *standardized interface* is already a countermeasure to lower the risk of undiscovered vulnerabilities in APIs by replacing many asset-specific interfaces with the standardized AAS interface. A second countermeasure is the Attribute Based Access Control (ABAC) concept for the AAS including a secure *identification, authentication, and access control* process [Pla20c]. At the same time, this supports the *limitation of available information* by limiting access rights. This could be extended by the partition of an AAS in parts with different risks. As one asset can have several AASs, the information could also be distributed among these AASs. In case of an incident via a Basic Web Application Attack to an AAS connected to the Internet, not all asset data is exploited. More confidential data could be stored in an AAS with limited or no connection to the internet. The AAS concept enables such a partition of asset data, but the best practise to realize this is missing.
The same counts for the idea of *logging and monitoring* of AASs that was proposed early [Pla17]. An overall concept to realize this for the interfaces of re-active AASs is missing. For now, only an approach to log the changes of AAS files was done in [RVPK20], but does not cover the communication interface of re-active AASs. The logging could be complemented with a universal *attack detection* to identify misconducts or attacks.
A missing countermeasure to achieve *secure communication*, in addition to the secure usage of OPC UA [Pla19b] and the proposed security implementation on the application layer for HTTP [Pla20c], is the usage of Virtual Private Networks (VPNs) between AASs, and between AASs and other services.
In addition to the above-mentioned countermeasures, the Top 10 vulnerabilities in API implementations and corresponding countermeasures are listed in detail in the "OWASP API Security Top 10" [The19].

Malware Infection via Internet and Intranet & System Intrusion Especially with recent security incidents, such as the ransomware attack via the IT service provider

Kaseya [Fun21], in mind, malware including ransomware and supply-chain attacks is one of the most relevant threats. A ransomware leading to data loss of all information about the assets could have a huge impact on the owning company. Also, sabotage through manipulated data is possible. The malware can infect an AAS at any party within the supply-chain, resulting in a supply-chain attack. Therefore, the *provisioning supplier roots of trust* similar to the trustworthiness level concept in [Pla17] could increase the security of AASs. To detect malware, an *antivirus software* scanning incoming AAS files should be a minimum standard. The *logging, monitoring, and attack detection* is a second step to identify malware.
In case that the malware is already introduced via an AAS, the further spread can be limited by *network segmentation*. To do so, a suitable and secure network architecture for the AAS including firewalls, VPNs, and network monitoring should be developed to avoid a spread of malware from the Internet via the AAS to the IT and OT networks. Lastly, a *periodical backup* will be helpful to enable a quick recovery after a potential incident. A dynamic selection and rating of data importance as well as an optimization of the backup that is practicable for numerous AASs should be evaluated. For example, not every sensor value needs to be saved forever, whereas some crucial asset properties and submodels should be stored securely without time limitation. In addition, the backup interval could be different for submodels with dynamic data and static properties.

Results The AAS as a standardized interface for industrial assets and the AAS access control, including the identification and authorization, cover already two crucial countermeasures for secure ICSs. However, the detailed investigation of the two threats with the highest relevance for the AAS, as well as the investigation of the corresponding countermeasures yield to some open issues in the state of the art of AAS security.
A concept for a smart partition of asset data in several AASs with different security measures, and the implementations of an overall logging, monitoring, and attack detection system need to be developed. This should be optimized for the whole AAS cross-company life cycle and protect the AAS from unwanted access and manipulations. Further, a future I4.0 network architecture with network segmentation optimized for the AAS that enables a maximum communication capability to different IT and OT networks on one hand, and prevents the spread of malware inside the networks on the other hand, is needed. That applies as well to a backup strategy that is practicable and efficient for numerous AASs and enables a quick recovery after a possible incident.

4 Conclusions and Future Work

For a great acceptance of the AAS and the realization of the positive scenario with the AAS leading to a security enhancement, some characteristics are essential for the further AAS design. This paper shows that not all current ICS threats are relevant for the AAS. Some threats can even be mitigated by the AAS. For some other threats, solutions and countermeasures do already exist and are summarized in this paper.

Nevertheless, the threat analysis for the AAS identified some open research challenges and activities for the implementation of more countermeasures to minimize future security incidents while using the AAS.
In future work, more threats and countermeasures, such as from MITRE ATT&CK® and MITRE Shield, as well as from the IEC 62443-4-2 can be evaluated with regard to the AAS. The data from the future secure AASs can be used, for example, as the basis for an automated safety and security assessment for modular production systems [EBH+20].

Acknowledgement

This contribution was funded within the project AutoS^2 as part of the technology network it's OWL with support from the Ministry of Economic Affairs, Innovation, Digitalization and Energy of the state of North Rhine-Westphalia, Germany.

References

[BBT+21] Andre Bröring, Alexander Belyaev, Henning Trsek, Lukasz Wisniewski, and Christian Diedrich. Secure Asset Administration Shell exchange with Distributed Ledger Technology. In *Shaping a globally secure Industrie 4.0 Ecosystem*. Plattform Industrie 4.0, Berlin, 2021.

[Bun19] Bundesamt für Sicherheit in der Informationstechnik. Industrial Control System Security: Top 10 Bedrohungen und Gegenmaßnahmen: V1.3, 2019.

[DP20] Marietheres Dietz and Gunther Pernul. Unleashing the Digital Twin's Potential for ICS Security. *IEEE Security & Privacy*, 18(4):20–27, 2020.

[EBH+20] Marco Ehrlich, Stefan Benk, Dimitri Harder, Philip Kleen, Henning Trsek, Sebastian Schriegel, and Jürgen Jasperneite. Automatische Bewertung und Überwachung von Safety & Security Eigenschaften – Strukturierung und Ausblick. *Jahreskolloquium Kommunikation in der Automation (KommA)*, 2020.

[EE18] Matthias Eckhart and Andreas Ekelhart. A Specification-based State Replication Approach for Digital Twins. In *Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and Privacy*, pages 36–47, 2018.

[Fun21] Brian Fung. New ransomware attack targets key IT vendor. *https://edition.cnn.com/2021/07/02/tech/ransomware-cybersecurity-attack-kaseya/index.html*, 2021.

[GX21] GAIA-X. What is Gaia-X? *www.data-infrastructure.eu*, 2021.

[HR19] Mark Hearn and Simon Rix. Cybersecurity Considerations for Digital Twin Implementations, 2019.

[Ind21] Industrial Digital Twin Association e.V. admin-shell-io by IDTA: aasx-server. *www.github.com/admin-shell-io*, 2021.

[NTE21] Ellen Nakashima, Yeganeh Torbati, and Will Englund. Ransomware attack leads to shutdown of major U.S. pipeline system. *www.washingtonpost.com/business/2021/05/08/cyber-attack-colonial-pipeline*, 2021.

[PK18] Animesh Pattanayak and Matt Kirkland. Current Cyber Security Challenges in ICS. In *IEEE International Conference on Industrial Internet (ICII)*, 2018.

[Pla17] Plattform Industrie 4.0. Security der Verwaltungsschale: Diskussionspapier, 2017.

[Pla19a] Plattform Industrie 4.0. Access control for Industrie 4.0 components for application by manufacturers, operators and integrators: Discussion Paper, 2019.

[Pla19b] Plattform Industrie 4.0. Secure cross-company communication with OPC UA: Discussion Paper, 2019.

[Pla20a] Plattform Industrie 4.0. Details of the Asset Administration Shell: Part 1 - The exchange of information between partners in the value chain of Industrie 4.0 (Version 3.0RC01): Specification, 2020.

[Pla20b] Plattform Industrie 4.0. Details of the Asset Administration Shell: Part 2 - Interoperability at Runtime – Exchanging Information via Application Programming Interfaces (Version 1.0RC01): Specification, 2020.

[Pla20c] Plattform Industrie 4.0. Secure Download Service: Discussion Paper, 2020.

[Pla21a] Plattform Industrie 4.0. Functional View of the Asset Administration Shell in an Industrie 4.0 System Environment: Discussion Paper, 2021.

[Pla21b] Plattform Industrie 4.0. Was ist die Verwaltungsschale aus technischer Sicht?, 2021.

[RVPK20] Magnus Redeker, Sören Volgmann, Florian Pethig, and Johannes Kalhoff. Towards Data Sovereignty of Asset Administration Shells across Value Added Chains. In *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, Piscataway, NJ, 2020. IEEE.

[The19] The OWASP Foundation Inc. OWASP API Security Top 10 2019: The Ten Most Critical API Security Risks, 2019.

[Ver21] Verizon. DBIR 2021 Data Breach Investigations Report, 2021.

[WSJ17] Martin Wollschlaeger, Thilo Sauter, and Jürgen Jasperneite. The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0. In *IEEE Industrial Electronics Magazine*, 2017.