Technical Whitepaper

Version 2022

Open Industry 4.0

Contents

1.0 BACKGROUND

The Open Industry 4.0 Alliance is aiming to enable the digital transformation required to advance the principles of Industry 4.0 – for manufacturing (process and discrete industry automation), for on-site logistics processes (warehouse automation) and also for continuous and standardized data exchange amongst all contributors along the value chain. Large, medium, and small companies are finding that intelligent asset (equipment/devices/machines/sensors) integration and optimization of business processes is being stifled by the complexity of engaging with multiple asset manufacturers, a plethora of IIoT/Industry 4.0 software providers (IoT platforms and solutions) and requirements for multiple OT/IT service providers. In addition, customers (operators) face inherent challenges involving brownfield assets, networks, connectivity, and firewall access concerns within their manufacturing and warehouse facilities. These issues are complicated further by the diversity of asset providers defining their own IIoT solutions and ongoing discussions over data ownership.

All of these factors have a detrimental effect on adopting Industry 4.0, slowing the realization of projected benefits and blocking the return on investment.

This is the main motivation for the Open Industry 4.0 Alliance: It is aimed at bringing together leading companies in the engineering, industrial automation, software, hardware, and service industries to collaborate and support operators of intelligent assets to drive quicker adoption of Industry 4.0 processes by providing interoperable end-to-end solutions of alliance members.

For more details on the Open Industry 4.0 Alliance, refer to the Alliance website at https://www.openindustry4.com/

2.0 SOLUTION BUILDING BLOCKS AND REFERENCE ARCHITECTURE FRAMEWORK

The Open Industry 4.0 Alliance solution reference architecture for interoperability takes into consideration the following key elements:

Typical use cases by industry segment, and processes that deliver customer value

- **Mitigation of physical topology, technology, security, and landscape challenges within plants/factories and warehouses for improved time to value**
- **Providing interoperability of solutions offered by Alliance members to enable rapid adoption and accelerate return value for the operators**
- **Making system landscapes and infrastructures fit for a next generation cross company collaboration, i.e. business networks which enable innovation and value generation based on standardization and openness**

These architectural characteristics consider the detailed viewpoints that need to be addressed for an optimal framework that will enable customer (operator) benefits. These viewpoints can be classified into the following categories:

Operators' business value expectations

- Address the needs of business stakeholders, desired value, and objectives for undertaking a digital transformation journey
- Broad range of applications that break down IT system and operational technology boundaries to help process optimization and/or enable new business models

Modularity and E2E solution

- Modular coverage of a comprehensive functional, technical, security, and software architecture
- Adhere to the general concept of Digital Twins as a holistic view on all aspects that are relevant for dealing with an asset along the asset's lifecycle and across its multiple stakeholders
- Agreement on the Asset Administration Shell (AAS) designed by Industrial Digital Twin Association (IDTA) as a common denominator and standard for the implementation of Digital Twins for Industry 4.0
- Common AAS model repository, semantics, and collaboration between manufacturers and operators
- Broad Alliance ecosystem to collaborate with collective expertise and provide Industry 4.0 solutions and applications
- Meet end to end and standards-based technical needs for connectivity, data management, analytics, process integration, security, data security, and hardware infrastructure

Business Network and collaboration

Create solution approaches which focus on the idea of easy to configure and easy to adopt cross company collaboration - this will manifest for simple scenarios in a smart way to receive the latest asset-specific contents from manufacturers (OEMs) while for other scenarios a multi-directional information exchange e.g. about asset usage, status, condition etc. amongst manufacturer and operator and other stakeholders like service providers is defined.

Ease and speed of implementation

- Easy onboarding of assets
- Common data semantics for better interoperability and as an enabler for value generation based on Machine Learning and other Artificial Intelligence (AI) approaches
- Cohesive service offerings for successful deployment from multiple OT and IT service providers

All Open Industry 4.0 Alliance guidelines are subject to an approval process based on a framework of predefined design principles. This will lead to trust in the fact that an approved set of technical solutions will be able to deliver the required standardization to enable quicker adoption of the customer's Industry 4.0 goals. It is mandatory for a committed solution provider to be a member of the Open Industry 4.0 Alliance.

2.1 INTRODUCING THE OPEN INDUSTRY 4.0 ALLIANCE FRAMEWORK OF SOLUTION DESIGN PRINCIPLES:

Fig. 1: ONE and OPEN

The principle of "ONE" provides the framework for design principles of solutions that will be provided by members of this alliance and applies to the following:

- One data semantics and asset network: Common semantics models across the solution stack for data interoperability, faster development of IIoT and corresponding business applications by Alliance members, and simplified master data management.
- One asset model repository shall hold information templates about types or instances of assets as provided by manufacturers following existing and upcoming concepts of the AAS. OEMs shall provide readily available asset models to enable collaboration and plug & play onboarding.
- One defined data custodianship giving customers full flexibility in defining where their data resides,
- its ownership, and the ability to share data with governing rules that comply with data privacy requirements.
- One approach to security that fully enables customers to ensure the security of the solution, data,
- and network needed for plants, factories, and warehouses.
- One interface: The guidelines of the Alliance will provide well-defined interfaces that allow full interoperability between all Alliance solution providers.
- One asset registry: As a kind of "address book" feature which allows to identify and locate an AAS in a stakeholder network.
- One solution directory: One directory for listing all Alliance-approved solutions.
- One Alliance: A coalition of companies with equal say, not dominated by any member, enabling development of the best solutions for customers. Solutions provided by members of this alliance will be interoperable.

The Principle of "OPEN" applies for the Alliance:

The Alliance is deemed open along several critical dimensions as listed in the figure above. This enables compatibility with all brands and types of assets, manufacturers, system integrators, and operators. Most importantly, the Alliance is open to data custodianship and establishes a trust-based, interoperable solution offering owned, delivered, and supported by members of the Alliance, which represent a critical mass of the automation market for our customers (operators).

2.2 INTRODUCTION TO THE OPEN INDUSTRY 4.0 ALLIANCE REFERENCE ARCHITECTURE FRAMEWORK

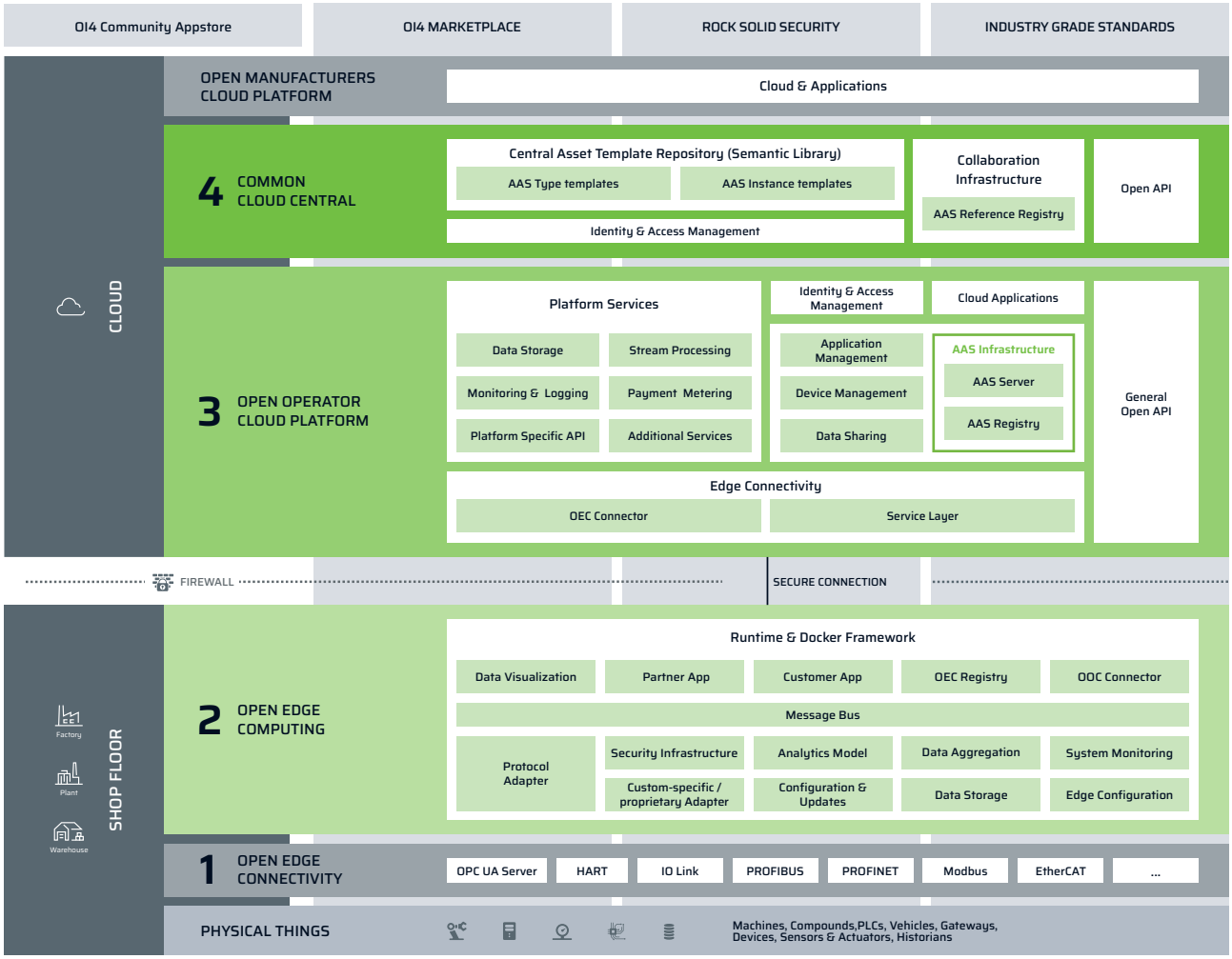


Fig. 2: Reference Architecture

The building blocks of the end-to-end technical solution are divided into four key categories:

- Open Edge Connectivity
- Open Edge Computing
- Open Operator Cloud platform
- Common Cloud Central

The building blocks of the architecture are modular and provide full flexibility to generate value for the customers of the Alliance members. Further details on each layer are given in the subsequent sections of this whitepaper.

2.3 RELATIONSHIP WITH EXISTING STANDARDS AND FRAMEWORKS IN INDUSTRY 4.0

This solution architecture framework is conceptualized keeping in mind key industry 4.0 standards and protocols. It is the explicit goal of the Open Industry 4.0 Alliance to not define new standards but, wherever possible, to leverage existing standardization efforts, augmenting these to allow full interoperability amongst the Open Industry 4.0 Alliance ecosystem. A summary of in scope standards and standardization efforts by expertise as well as related associations are listed below – this is however not limited and might be extended in the future:

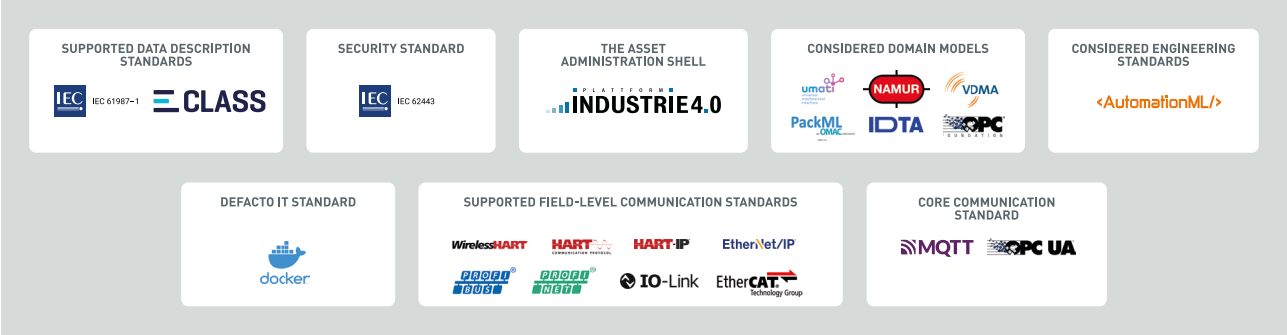


Fig. 3: Excerpt of considered Standards and Associations

The supported field level communication standards in the Open Industry 4.0 Alliance will be covered by appropriate technology adapters offered by member companies. Since the Alliance includes some of the most distinguished communication experts from different industry branches among its members, in-depth coverage of technology features will be provided.

IEC standard 62443 provides not only a responsibility assessment of security in industrial applications, but also gives a state-of-the-art list of measures to be taken for certain security levels. It is the basis of the work of the security working group inside the technical committee of the Alliance, which will detail specific requirements to be fulfilled by Alliance compliant solutions in order to provide rock solid security.

With regard to the Edge Computing Layer a combination of the best practice features of OPC UA and MQTT ensures easy interoperability of Alliance compliant solutions.

With regard to data modeling and instantiation of Digital Twins within the Open Operator Cloud and for the exchange of Digital Twin data between the layers and with business applications the main concept in the Alliance reference architecture is the Asset Administration Shell (AAS).

The AAS as defined by Plattform Industrie 4.0 and further developed by the IDTA is the only sensible choice for implementing standardized digital twins in the Alliance framework. As an I.40 standard for semantic interoperability, the AAS concept shall cover the complete lifecycle of an asset and leverages or reuses existing well-known and mature I.40 standards like AutomationML, OPC UA and ECLASS. At the same time the AAS allows new information models, providing flexibility for cases where a standard is not yet considered or available.

Attributes for industrial equipment must be standardized in data description standards in order to allow computer-driven engineering of solutions. A basic level of semantics is given by the available taxonomy dictionaries. ECLASS has a wide user range and covers many technologies, augmented by a second option in the form of the IEC Common Data Dictionary. Both standards can be used in the same manner by referencing the unambiguous identifier for attributes and integrate properly with the AAS specifications.

> … The AAS has standardized the structure and ECLASS has standardized the semantics for information elements, which should be used for the definition of digital twins. The structure of the AAS and the ECLASS dictionary complement each other in a perfect manner to achieve this objective … (Whitepaper: „Modelling the Semantics of Data of an Asset Administration Shell with Elements of ECLASS“)

The concept of submodels is a main part of the information model of the AAS. To be able to associate information from different technical domains many different properties are required to be represented in an AAS. To manage the complexity of these sets of information, submodels provide a separation of concern and they are linked to use cases to aggregate information that belongs together and can be built according to industry- and industry-branch specific requirements (Domain Models).

> Additional information is composed in The Asset Administration Shell in the OI4 solution framework.

3.0 OPEN INDUSTRY 4.0 ALLIANCE PROPOSAL FOR SOLUTION BUILDING BLOCKS DEEP DIVE AND DETAILED BUILDING BLOCK DESIGN PRINCIPLES

Motivation: The AAS Lifecycle

Taking a a look at the complete lifecycle of an asset and its AAS shows why a Digital Twin should be considered as an entity which could have different “owners” and the option to have multiple instances at different places. For example: until the physical shipment of an asset, the Manufacturer might collect information about the asset and keeps them in an AAS which is instantiated in the manufacturer‘s software landscape. But this AAS might not be deleted or “shut down” after shipment. Audit, Due Diligence, Warranty or an effort to win the manufacturer‘s environment. At the same time, the physical asset is in use at the operator‘s premises. Here, the operator could create their own AAS with other, usage specific submodels. Live data, up-to-date maintenance details or even the purchase details of the asset might be information that is structured and stored by means of the AAS submodels in the AAS instance under the operator‘s responsibility.

Fig. 4: AAS Lifecycle

As defined by the RAMI 4.0 and adopted by Plattform Industrie 4.0 for the concept of the Asset Administration Shell the lifecycle of assets is separated into type and instance phase.

During type phase the manufacturer collects and creates all asset related data, first as artifacts, then as AAS or submodels to become parts of the AAS for the individual asset. The submodels may be separated into those submodels that stay on the manufacturer‘s side and those submodels to be shared with partners and customers.

As part of the delivery of the asset to the customer, the corresponding AAS and its submodels will be shared with the customer and / or integrator via the Common Cloud Central to become part of the on-boarding process.

As soon as the concrete AAS is instantiated in the Open Operator Cloud platform and therefore in the ownership of the operator, the AAS will also support use cases to exchange asset related data between operator and manufacturer and vice versa.

3.1 OPEN EDGE CONNECTIVITY

The Open Edge Connectivity layer covers a wide range of possible data sources and possible communication technologies used. For each of the technologies that are covered by an Open Industry 4.0 Alliance solution, some form of adaptation has to exist. For many technologies, the associated adapter can be provided on the Open Edge Computing layer. However, it has to be ensured that data is accessible in a digital format and that identity information about field level assets can be acquired. For technologies where this information access poses a challenge, a technological bridge or gateway on the Open Edge Connectivity layer will be needed. In the future, Open Industry 4.0 Alliance compliant field devices will be able to directly communicate with any Alliance-compliant ecosystem. For more information on how device manufacturers will be able to achieve this, members should consult the Development Guideline document. The tasks of this layer are thus:

Enable greenfield or brownfield connectivity scenarios for:

- Device (asset) identification
- Data conversion to compatible Open Edge Computing platforms (e.g. MQTT, OPC UA, etc.)
- Local diagnostics

For connectivity of brownfield devices with analog protocols:

- Enable conversion of analog to digital protocols (e.g. using HART or IO Link)

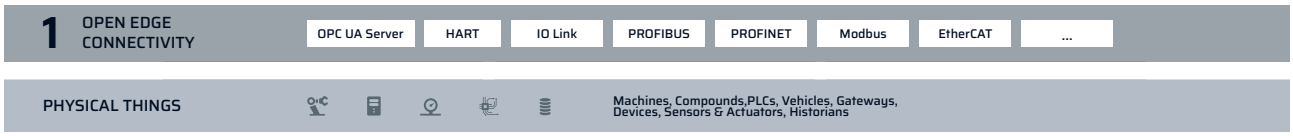


Fig. 5: The Open Edge Connectivity layer

3.2 OPEN EDGE COMPUTING

Edge computing provides local data processing and an applications platform for plant operators, supervisors, warehouse users, etc. for real-time information about operational performance statistics. Edge computing is an emerging trend that provides direct access to data for the users/operators of the machines. Depending on the use case, edge computing may not be needed, and data can be directly ingested into the cloud. This mandates, however, that there already exists access to a system-wide message bus with Alliance compliant topics and message payloads. This has to be accessible from applications connecting the Open Edge Connectivity layer. A main task covered by the Open Edge Computing layer in this reference architecture framework is the onboarding of equipment. Critical identification and asset information has to be provided from this layer onwards in order to ensure proper interoperability of onboarded devices.

An important point of note is that the provided architecture is a reference framework for ensuring full coverage of relevant architecture elements. The Alliance does not make presumptions about the physical distribution of the functions described in the reference architecture.

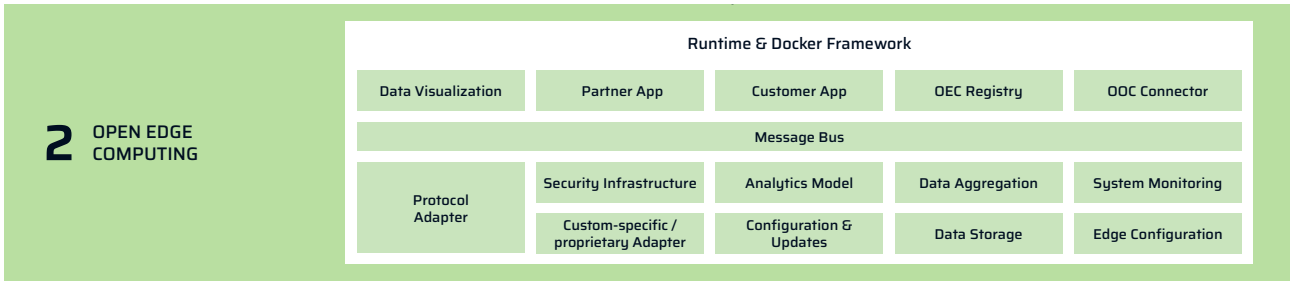


Fig. 6: The Open Edge Computing layer

The high-level understanding behind the technical modules is briefly explained below.

» **Docker Framework**
This framework provides the runtime for containerized applications to be run inside the Open Edge Computing layer. Only the most basic services for this layer do not have to be run containerized.

» **Message Bus**
The lifeline of data exchange inside the Open Edge Computing layer is the Message Bus. It is to be implemented in the form of a MQTT broker handling the Alliance-defined topic structure. All data transmissions between containers in this layer (and possibly some going beyond it) must use the Message Bus.

» **OOC Connector (Open Operator Cloud Connector)**
In the Open Industry 4.0 Alliance architecture framework, every edge computing solution is expected to have a north-bound interface to communicate with an Open Operator Cloud Platform chosen by the operator. This component exposes an Alliance-compliant communication and information model interface towards the Message Bus for tasks like asset onboarding, while offering a platform-compatible interface to the Open Operator Cloud Platform layer.

» **Protocol adapter**
In order to access the diverse and heterogeneous communication technologies on the Open Edge Connectivity layer, a range of protocol adapters will have to be provided in the form of Alliance-compliant containers. These protocol adapters have the responsibility to encapsulate OT access both for onboarding and data acquisition tasks, as well as any other access to the OT network they were written for, that is requested over the Message Bus. Members can find more details on the responsibilities of the Protocol Adapter in the Development Guideline document.

» **Customer App and Partner App**
The docker container platform enables the development and deployment of custom applications at the Open Edge Computing layer.

» **Analytics model**
Analytics models to be used for data enrichment on the Open Edge Computing layer have to be deployed in the form of Alliance-compliant containers, receiving their payload data through the Message Bus.

» **OEC Registry**
The OEC Registry has the critical task of keeping track of all onboarded assets as well as all containers deployed on the particular Open Edge Computing platform. It serves as a directory of available entities to be addressed through appropriate topic structures in the Message Bus.

» **Custom-specific / proprietary Adapters**
For devices that have to be accessed by a customer-specific method, the customers can have their own device adapters in the form of Alliance-compliant containers. Especially in legacy devices, proprietary protocols are utilized for device access and management. For these, specific adapters can be provided in the form of Alliance-compliant containers.

» **Data visualization**
The Open Edge Computing layer is an appropriate environment to realize localized visualization solutions.

» **Data storage**
For some applications, it is feasible to ensure localized data storage on the Open Edge Computing layer.

» **Edge configuration**
The configuration of both edge devices and underlying field devices is a major engineering task that has to be supported in order to reap the benefits of Industry 4.0. The Open Edge Computing layer can help with this task by providing a runtime environment for edge configuration solutions.

» **Data aggregation**
In order to manage the amount of data transferred to the cloud, data aggregation has to be performed on the edge computing level. Dedicated Alliance-compliant containers can easily realize this.

» **System monitoring**
In order to allow for efficient administration of the Open Edge Computing layer, system monitoring allows supervisory control over the parameters and resources of the edge computing solution.

» **Security infrastructure**
For more information on the security concept of Open Industry 4.0 Alliance, click here.

» **Configuration and Updates**
The base services on the Open Edge Computing layer have to be maintained in a software management sense. The configuration and updates services fulfill this role in an Open Industry 4.0 Alliance system.

Design principles

Open to multiple operator cloud providers conforming to Open Industry 4.0 Alliance design principles:

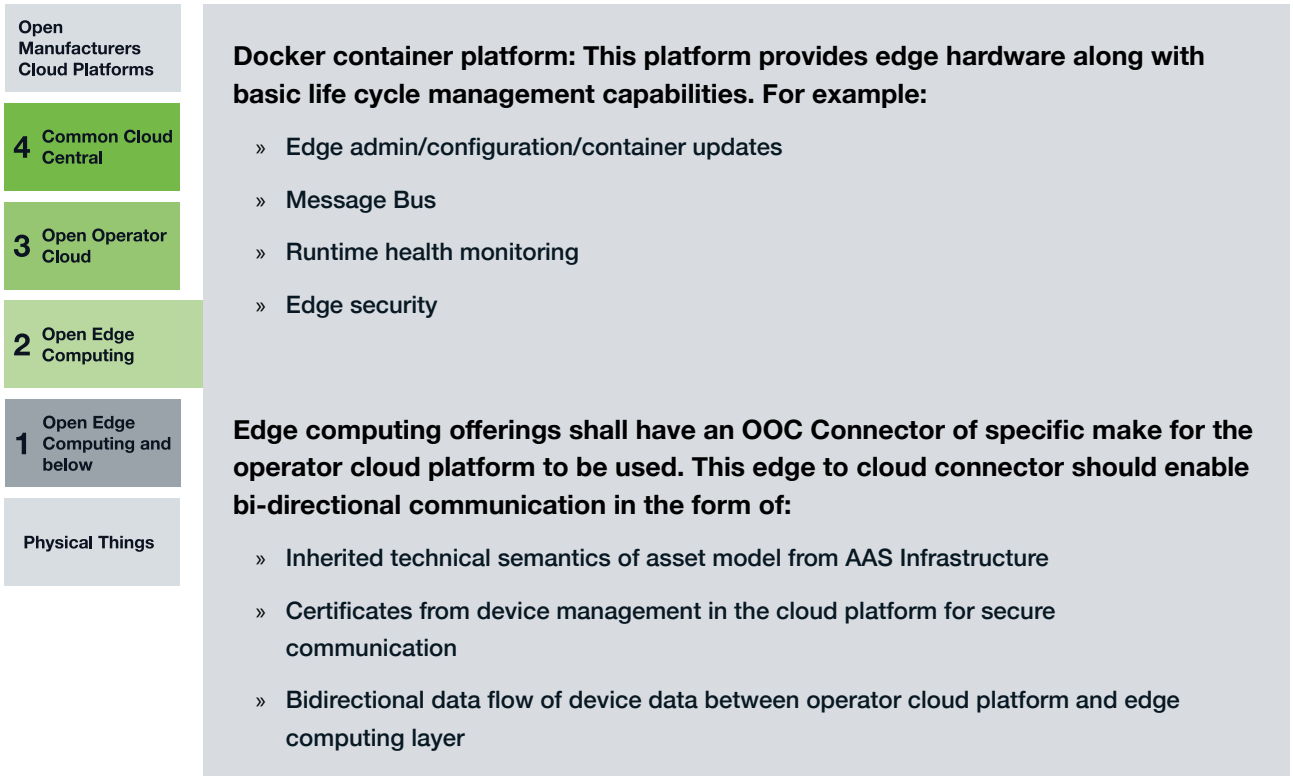


Fig. 7: Open Edge computing layer

3.3 OPEN OPERATOR CLOUD PLATFORM

The Open Industry 4.0 Alliance gives customers a choice of operator cloud platforms. The guiding design principles for Open Industry 4.0 Alliance-approved operator cloud platforms are those designed for enabling a trust-based environment, which would also provide consistent E2E interoperability and achieves the goal of faster adoption.

The Open Operator Cloud (OOC) Platform holds the dedicated instances of assets created during the onboarding process as an aggregation of data provided from the OEC layer and data retrieved from Common Cloud Central. E.g. onboarding data from the OEC layer are retrieved automatically from the layers below the OEC. If necessary, missing data may be added manually during the onboarding process by the operator. The OOC can access the CCC in order to complete missing information about a particular asset during the onboarding process or for update processes later on.

Data formats on the OEC layer are based on the information of the “Open Industry 4.0 Alliance Development Guideline” for the OEC layer. Nevertheless, latest on transition between OEC and OOC layer the common data format in an Alliance compliant infrastructure for digital twin data is based on the AAS concept. Communication on the cloud layers w.r.t. digital twin data shall always be based on the concepts of the Asset Administration Shell. It also implies the business logic necessary to follow the concept of the AAS as adopted by the solution framework of the Open Industry 4.0 Alliance.

The operator cloud shall provide access to all basic technical modules, e.g. “Device Management”, “Application Management”, “Data Sharing”, E2E security concepts, “Identity & Access Management”, etc., as depicted in the solution building blocks in Figure 8.

Depending on the business and technology strategy of a company, there are several choices for the foundation of the Open Operator Cloud Platform. The Open Operator Cloud Platform may be based on one of the following infrastructure related scenarios or any composition of them:

1. **Operator Cloud platform based on IIoT platform offerings provided by vendors or service providers for specific industrial use cases**
2. **Operator Cloud platform based on highly scalable cloud infrastructure services, could be deployed on hyperscalers**
3. **Operator-side or datacenter-located IIoT platforms as private or hybrid cloud, based on bare-metal or virtualized infrastructure**

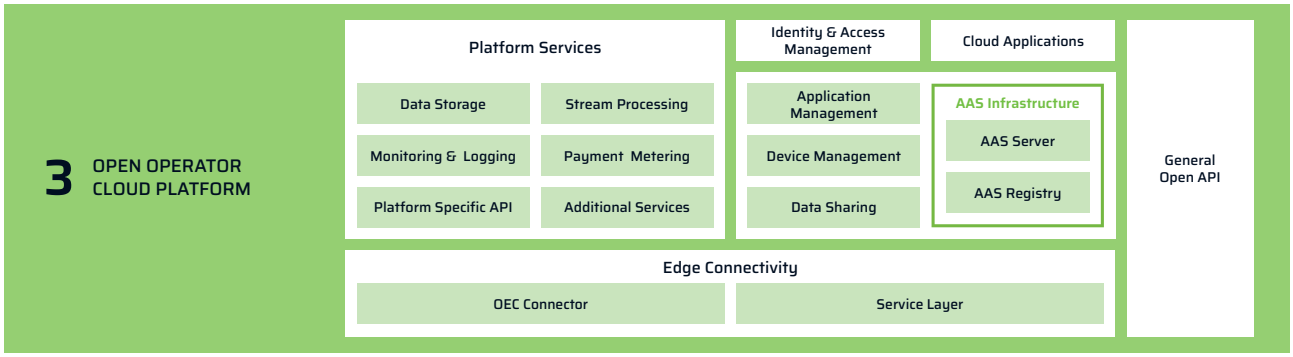


Fig. 8: Reference Architecture of the Open Operator Cloud platform

Since every customer follows its own technical strategy related to the technical choice of an operator platform only parts of the technical modules can be aligned across the members of the Open Industry 4.0 Alliance. The technical modules that are the initial focus of the work groups of the Alliance are:

1. Edge Connectivity
2. AAS Infrastructure
    a. AAS Server
    b. AAS Registry
3. General Open API

The high-level understanding behind the technical modules is briefly explained below.

» **Edge Connectivity**
Data from multiple connected edge gateways can be ingested to the operator cloud via the technical module “Edge Connectivity”. Via this module data will be forwarded to further compliant components. Additionally this module will have a back channel from cloud to edge to support cloud to edge communication for compliant services. In the context of end-to-end use cases, this module will also include the mapping of data formats and semantics of different standards between the shopfloor and the cloud.

» **AAS Infrastructure**
This module is essential for the creation and handling of digital twins. Hence it takes care of keeping track of all onboarded assets.
The AAS Infrastructure manages information based on the information model and concepts of the Asset Administration Shell. Access to assets will be based on defined API endpoints whic are part of the module “General Open API” of the OOC layer and follows the definitions of AAS related API endpoints as described in “Details of the Asset Administration Shell - Part 2, Interoperability at Runtime” [AAS_PART2]. As part of the AAS Infrastructure the AAS Server and the AAS Registry serve as technical modules.

» **AAS Server**
In sense of a reference architecture the “AAS Server” will be an essential part of the solution module “AAS Infrastructure“. Technically it may also be based on proprietary technical modules or existing services which follow the frame conditions from the AAS information model and API.

» **AAS Registry**
The technical module “AAS Registry” defines a central registry for devices and applications based on the AAS concept. Technically it may also be based on proprietary technical modules or existing services which follow the frame conditions from the AAS information model and API.

» **General Open API**
The module “General Open API” standardizes across Open Industry 4.0 Alliance members a secure access to the modules of the Open Operator Cloud, e.g. the access to the “AAS Infrastructure”, “Application Management” or “Device Management”. All APIs relevant for the Alliance are specified and documented by the Technical Workgroup on the base of e.g. OpenAPI. If APIs are defined in standards used on the OOC, they are also part of this solution module. E.g. the API defined in [AAS_PART2] are located here.

» **Device Management**
The technical module “Device Management” provides functionality for the management of connected edge devices, as well as all other manageable devices connected to the OOC, over their complete lifecycle. It includes the following functionalities:

- Preparation for cloud onboarding of devices
- Configuration during the complete lifecycle of the devices
- Maintenance like firmware updates, parametrization and diagnostics
- Decommissioning, etc.

» **Application Management**
This module provides the management of Alliance compliant applications on both the Open Edge Computing layer as well as the Open Operator Cloud.

» **Data Sharing**
“Data Sharing” focuses on functionality to share data on a horizontal level between different services and applications in the Open Operator Cloud. Additionally this module enables data sharing on a cloud to cloud base with services and applications outside the Open Operator Cloud.

» **Identity and Access Management**
The technical module “Identity and Access Management” manages identities and their individual access rights to the particular services and components operated on the Operator Cloud.

As part of the Identity & Access Management, the user & permission management will provide an Open Industry 4.0 Alliance compliant approach for managing users, roles and permissions. Thereby, it marshals access to compliant data, services and applications of the Open Operator Cloud Platform. As it stands, the “Identity & Access Management” module is a central component that will be accessed by all other components of the OOC. Together with its counterpart on the Common Cloud Central level this module shall guarantee data sovereignty, so that any participant may see and access only those information which are authorized in mutual agreement.

» **Cloud Applications**
Cloud applications use the common APIs of the underlying cloud services of the operator cloud to generate value use-case specific. Cloud Applications are managed by the solution module “Application Management”.

» **Platform Services**
The Platform services of the Open Operator Cloud subsume services of an IIoT platform as far as they are relevant for the Alliance ecosystem. They offer additional functionality like metadata and structure handling or secure transactions, as well as basic services like monitoring, logging, data storage or data lake, etc.. These services ensure smooth interaction between other platform modules and applications operated on the operator cloud.

- **Data Storage**
  Appropriate data storage shall be available to store all the kinds of data in the cloud, e.g., hot data that is used for live data analysis and cold data for historical analysis.

- **Stream Processing**
  Stream processing is used to perform on-the-fly analysis of data as soon as the data is available on the operator cloud.

- **Monitoring and Logging**
  Standardized monitoring and logging services to facilitate the operation of cloud apps and platform components.

- **Payment Metering**
  This technical module provides individual cost tracking, metering, and billing capabilities end-to-end along the underlying IIoT stack.

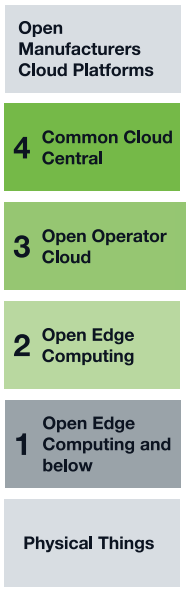
- **Platform Specific API**
  Platform specific API subsumes the APIs of the IIoT platform acting as Open Operator Cloud. In contrast to the General Open API, these interfaces and their functionalities are platform or use case related and go beyond the defined functionalities of an Alliance compliant Open Operator Cloud.

This listing shall not exclude any additional services that are required on a platform or use case basis to ensure the functionality of the IIoT platform serving as the basis for an open operator cloud.

Design Principles

In addition, for the operator's cloud platform choice to meet the vision of the Open Industry 4.0 Alliance solution reference architecture framework, the following general design principles must be adhered to.

Open to multiple operator cloud providers conforming to Open Industry 4.0 Alliance design principles:



Key design principles for an Open Industry 4.0 Alliance-approved operator cloud are:

- Adopt semantic models and integration with common cloud central or other cloud applications, as well as business applications based on concepts of the Asset Administration Shell
- Be interoperable with the Open Industry 4.0 Alliance-approved edge computing platform
- Be compliant to Alliance cybersecurity guidelines
- Include user management and permission management capabilities
- Provide test framework to allow certification for compliancy with Alliance guidelines

Alliance compliant APIs for integration of additional services such as:

- Business process integration
- ML / AI
- Data analytics
- Any other IIoT relevant service interacting with Alliance compliant devices, applications or services

Fig. 9: Operator Cloud

3.4 COMMON CLOUD CENTRAL

The Open Industry 4.0 Alliance foresees the use of a Common Cloud Central (CCC) layer as the concept for interoperability on Digital Twin models, Digital Twin Copy Templates and Digital Twin registration across companies.

The focus is seen on asset centric collaboration between OEM and operator, but also open for enabling other stakeholders (e.g. Maintenance Service Providers) to participate in such collaborations.

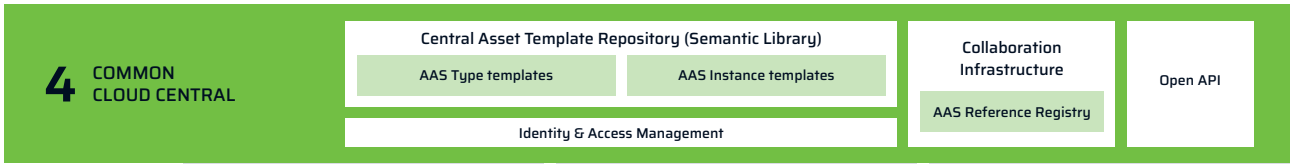


Fig. 10: Reference Architecture of the Common Cloud Central

As mentioned in previous chapters, the Alliance encourages existing and upcoming concepts of the Asset Administration Shell (AAS) as published by Plattform Industrie 4.0 and Industrial Digital Twin Association.

CCC as a logical layer holds information about templates for types or instances of Asset Administration Shells as provided by manufacturers. Hence, the approach fulfills also the idea of a Semantic Library for standardized (public) and also individual (asset specific) data models.

The distinct motivation is, to establish an infrastructure for the enablement and enrichment of the operators Digital Twin in the Alliance solution framework.

CCC is not foreseen as the layer, where an AAS of an asset itself is instantiated. Moreover, other layers (i.e. the Operator Cloud) can access the CCC in order to complete missing information about the particular asset and/or in order to identify where the particular AAS instances are hosted by means of a central registry.

Beyond that, all network participants may certainly decide on their own, if they agree on an application which covers the idea of a central digital twin repository.

In detail the following modules are part of the Alliance Common Cloud Central layer:

» **Central Asset Template Repository**
A manufacturer can upload information about types or instances of assets according to the structure and concepts of the Asset Administration Shell.
As soon as an AAS is instantiated by means of an AAS Server in the OOC layer, the AAS Server can contact the logical CCC building block Central Asset Template Repository in order to search for corresponding information. In other words, the AAS instance can be enhanced with submodels and their content as provided by the manufacturer.

There might be scenarios, where a full copy of the CCC-provided submodels results in unnecessary data replication, hence there shall be also mechanisms which allow the AAS instance to just refer to CCC-located submodels.

It is assumed, that the aforementioned sequence usually takes place in context of an asset onboarding use case, but the use case for update of asset information from CCC is feasible at any later point in time.

» **AAS Reference Registry**
The logical building block AAS Reference Registry is foreseen as a kind of address book feature which allows the identification and access of AAS in a stakeholder network. Also the manufacturer/vendor could access this registry for getting the URLs of AAS instances at his customers.

» **Identity & Access Management**
For all scenarios the Identity & Access Management building block shall guarantee, that any participant may see and access only those information which are authorized in mutual agreement.

» **Open API**
The module “Open API” standardizes across Open Industry 4.0 Alliance members a secure access to the modules of the Common Cloud Central, i.e. the access to the AAS Reference Registry and the Semantic Library. All APIs relevant for the Alliance are specified and documented by the Technical Workgroup on the base of e.g. OpenAPI. If APIs are defined in standards used on the CCC, they are also part of this solution module.

Design Principles

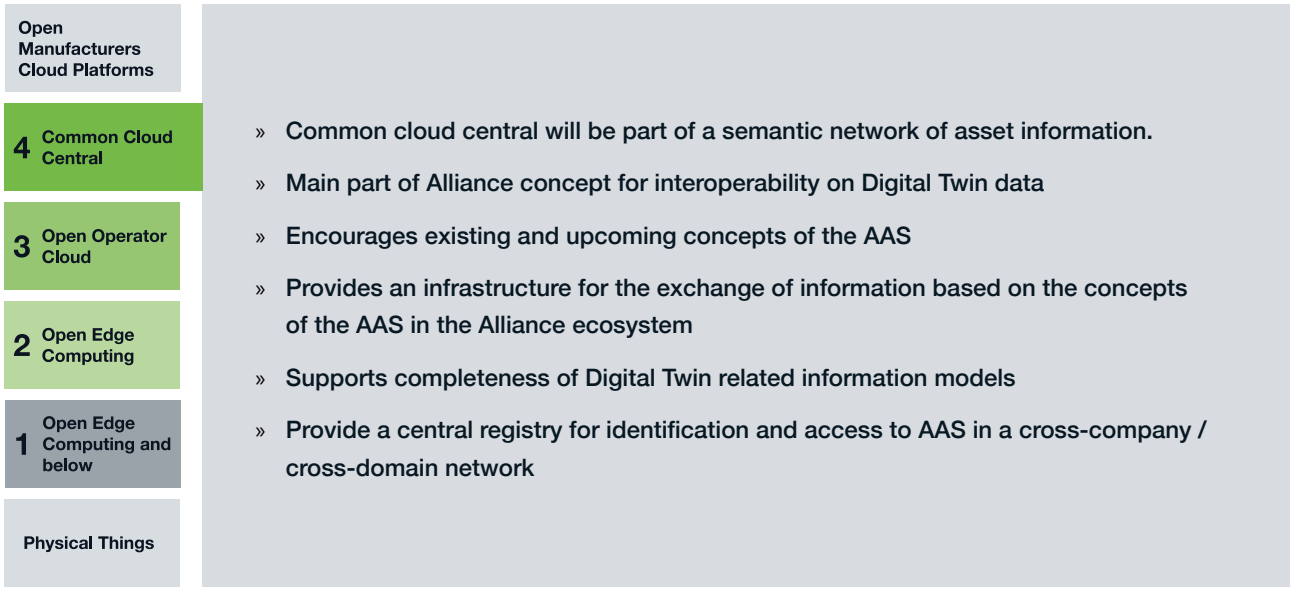


Fig. 11: Reference Architecture of the Common Cloud Central

4 SECURITY CONCEPT OF THE OPEN INDUSTRY 4.0 ALLIANCE

Cyber security is a fundamental component of the overall reference architecture of the Open Industry 4.0 Alliance. The Industrial Cyber Security Working Group (ICS-WG) supports the individual layers OEC, OOC and CCC as well as the OI4 Appstore in determining the necessary security requirements. Established IT security standards, best practices and established methods are used in this process. The working group consists of cybersecurity experts from Alliance member companies. The primary goal is to ensure that all layers of the reference architecture have a consistent and comprehensive security concept and can be integrated into existing user concepts.

Each selected technology in the Alliance ecosystem must meet security requirements for confidentiality, availability and integrity based on the need for protection.

The Industrial Cyber Security Workgroup (ICS-WG) has overall responsibility for cyber security across the ecosystem. Starting at each level, the other committees identify technical requirements and implement solutions. The ICS-WG supports the individual level workgroups with possible solutions as well as guidance on how to implement or apply the defined requirements and standards.

The ICS-WG attaches great importance to the fact that all security requirements are determined and implemented based on the need for protection and practical applicability. This approach makes it possible to present the decisions transparently to the user or operator. To this end, the ICS-WG assumes a cross-working group consulting role. The tasks include the determination of security requirements and the elaboration of technical measures.

An overview of the standards that apply to each level of the Open Industry 4.0 Alliance reference architecture can be found in the following table.

Norm, Standard / Layer	1 OEC and below	2 OEC	3 OOC	4 CCC	5 Community Appstore
IEC 62443-4-2 (device focus)	o	o			
IEC 62443-4-2 (device focus)	o	o			
OWASP		o			
SSDL - Secure Software Development		o			
DIN SPEC 27070		o			
PSIRT		o		o	o
IEC 27017			o	o	o
Cloud Ecosystem			o	o	o
CSA requirements			o	o	o

Security Concept Table of the Open Industry 4.0 Alliance

More details on the Open Industry 4.0 Alliance cybersecurity approach can be found in the whitepaper “Open Industry 4.0 Alliance Industrial Cybersecurity Design Principles” dedicated to this topic in particular.

5 SUMMARY AND CLOSING REMARKS

The world of Industry 4.0 has, in recent years, begun to take shape. Practical applications of the Reference Architecture for Industry 4.0 have been developed and have shown the viability of the approaches defined by the pioneers of the field. However, as implementations have risen in numbers, it has also become clear that the overall vision of Industry 4.0 allows for some degrees of interpretation. The efforts of the Open Industry 4.0 Alliance help our members to tackle the challenges posed by this degree of freedom. The Alliance is helping our members to integrate their solutions approaches and provide added value out of Industry 4.0 for their customers.

The intermediate results of our work outlined in this whitepaper show the direction into which our community is going to take Industry 4.0 in the light of increased demand for interoperability. As the work in the Alliance is continuously progressing, the reader should be aware that this document can only provide a snapshot. Interoperability and practical application in Industry 4.0 are challenges, still, and as long as this is the case, more work can be done to improve the effectiveness of Industry 4.0 solutions through the power of community.

The solution reference architecture for interoperability and underlying members' applications and technologies are designed to mitigate real-word challenges faced by customers in their Industry 4.0 digital transformation journey. For more information on the Open Industry 4.0 Alliance or to explore membership opportunities, please contact: **info@openindustry4.com**

Annex A
GLOSSARY AND LIST OF ABBREVIATIONS

- **Asset**
  A high-level term used for equipment, devices, sensors machines, etc. that are used in manufacturing facilities or warehouses to support production or logistics processes

- **Asset Administration Shell**
  German Translation – “Verwaltungsschale“ - The Asset Administration shell (AAS) is a basic concept for Industrie 4.0 scenarios. It defines a data structure that is an information anchor for assets in the digitised industry. The AAS is the Digital representation of an asset covering one or more different phases across the life cycle. Thus, the AAS is considered as the implementation of the Digital Twin for Industry 4.0.

- **Brownfield**
  A description for the situation as-is in a scenario where already commissioned and operational setups are supposed to be retrofitted to adhere to new heuristics and technological standards.

- **Common Cloud Central**
  Central cloud asset modeler and asset network offering from Open Industry 4.0 Alliance members (CCC)

- **Greenfield**
  A description for a clean slate situation where desired heuristics and technological standards can be applied to a new installation from before the commissioning phase

- **IIoT**
  Industrial Internet of Things

- **IT/OT**
  IT = information technology/OT = operational technology

- **Manufacturer (OEM)**
  Manufacturer of an asset (OEM = original equipment manufacturer)

- **Manufacturer’s cloud**
  The manufacturer’s (=OEM) rendered cloud platform

- **MQTT**
  Message Queuing Telemetry Transport - MQTT is a standard for devliering messages to disparate entities in an IT system through a message broker

- **Offline Engineering**
  Description for the activity to create digital twin instance models for the comissioning/onboarding process

- **Alliance, OI4**
  Open Industry 4.0 Alliance

- **OI4 Identifier**
  The minimum dataset required to uniquely create, identify and link an asset to a manufacturer through all levels of the Open Industry 4.0 Alliance architecture

- **OPC & OPC UA**
  Open Platform Communications - Unified Architecture - The OPC Foundation has defined a standard for information modeling and exchange in heterogenuous networked systems

- **Operator**
  The end user as a customer/owner of plant, factory, or warehouse

- **Open Edge Computing**
  Operator Edge Computing platform (OEC)

- **Open Operator Cloud Platform**
  Operator’s IIOT platform (OOC)

- **Physical things/control systems**
  A reference to assets (equipment, devices, sensors) in production or warehouse facilities. Control systems are operating technologies to support machine to machine automation e.g. PLCs etc.

Annex B
BIBLIOGRAPHY

» **Details of the Asset Administration Shell - Part 1**
Details of the Asset Administration Shell - Part 1, The exchange of information between partners in the value chain of Industrie 4.0, 2020 | more information

» **Details of the Asset Administration Shell - Part 2**
Details of the Asset Administration Shell - Part 2, Interoperability at Runtime - Plattform Industrie 4.0, 2020 | more information

» **DIN SPEC 27070:2020-03**
Anforderungen und Referenzarchitektur eines Security Gateways zum Austausch von Industriedaten und Diensten, 2020 | more information

» **ISO/IEC 27017:2015**
Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services, 2015 | more information

» **IEC 62443-4-1:2018**
Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements, 2018 | more information

» **IEC 62443-4-2:2019**
Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components, 2019 | more information

» **Whitepaper**
»Modelling the Semantics of Data of an Asset Administration Shell with Elements of ECLASS« - Plattform Industrie 4.0, 29.06.2021 | more information

» **AAS**
The Asset Administration Shell in the OI4 Solution Framework - Open Industry 4.0 Alliance, 2021 | more information

» **RAMI 4.0**
Reference Architectural Model Industrie 4.0 (RAMI4.0) - An Introduction - Plattform Industrie 4.0, 2018 | more information