OPEN INDUSTRY 4.0 ALLIANCE

OPEN INDUSTRY 4.0 ALLIANCE TECHNICAL SOLUTION DESIGN PRINCIPLES

Enhanced Industry 4.0 Interoperability for Quicker ROI

White Paper, Version 2.0

TABLE OF CONTENTS

1 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) and on-site logistics processes (warehouse automation). 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 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

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
- Common asset 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

User adoption

- Deliver an intuitive user experience to simplify processes and facilitate change management with new and improved ways of doing things
- Provide an easy way to receive the latest asset-specific contents from manufacturers (OEMs)

Ease and speed of implementation

- Easy onboarding of assets
- Common data semantics for better interoperability
- Cohesive service offerings for successful deployment from multiple OT and IT service providers

All Open Industry 4.0 Alliance solutions are subject to an approval process based on a framework of predefined design principles. These are designed to enable interoperability and give customers an option to retain their existing IT/OT investments. This also leads 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 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 applications by Alliance members, and simplified master data management.
- One asset repository: Alliance OEM members will provide readily available assets in the system 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 specification: The OI4 technical specification will provide well-defined interfaces that allow full interoperability between all OI4 solution providers
- 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

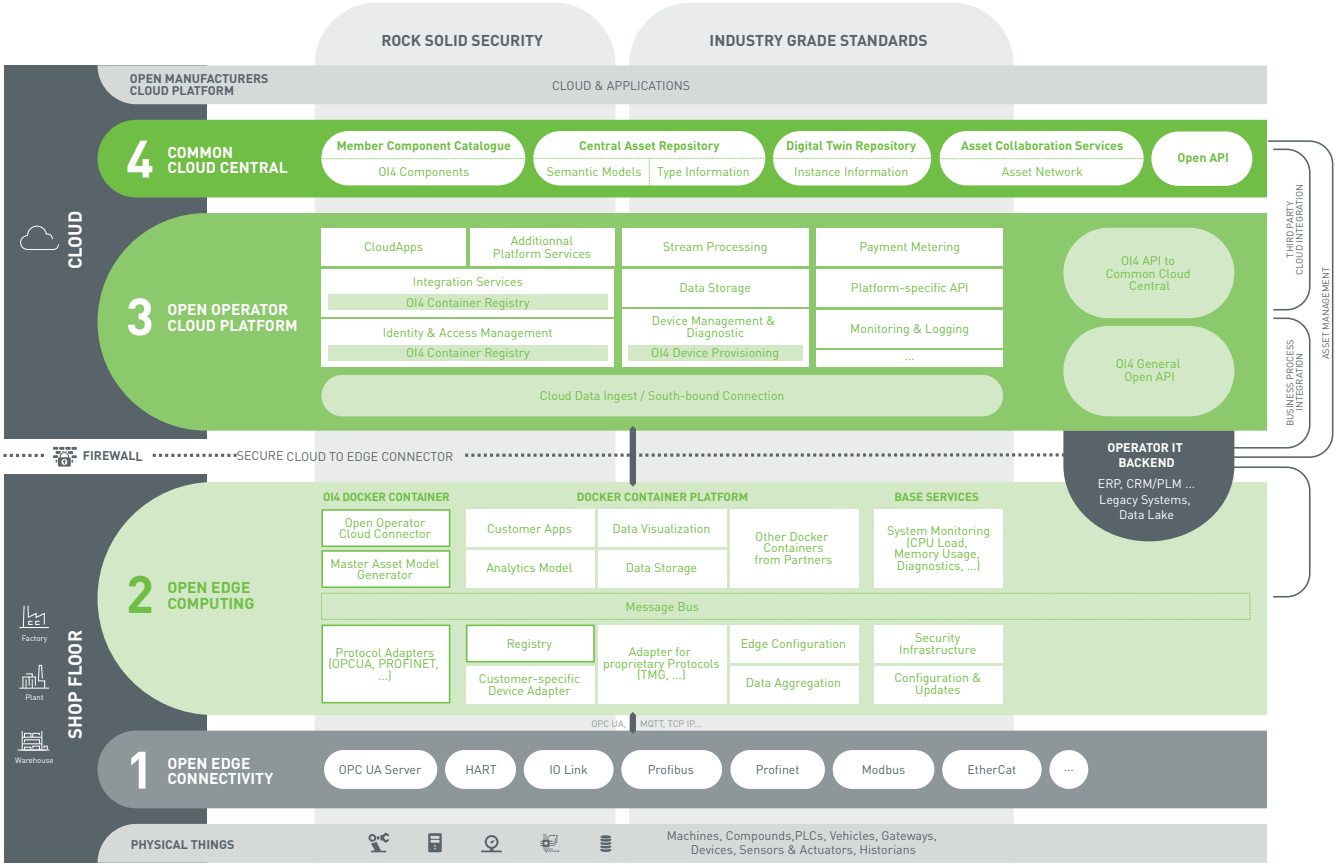


Figure 2 The Open Industry 4.0 Alliance reference architecture framework

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 for customers to define shop floor hardware infrastructure needs for edge gateways and micro data center (with or without virtualization) strategies. 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 express goal of the Open Industry 4.0 Alliance to not define new standards but, wherever possible, build on pre-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 are listed below – this is however not limited and might be extended in the future:

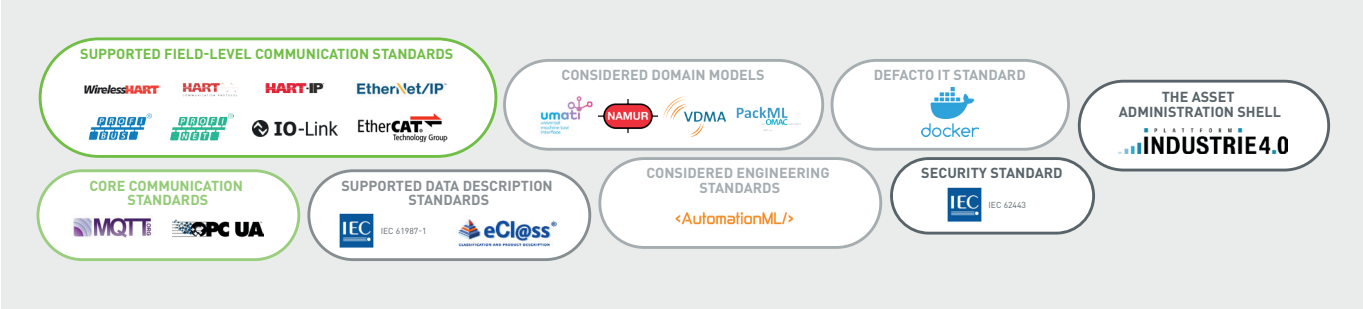


Figure 3 Considered Standards of the Open Industry 4.0 Alliance

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 OI4 technical committee, which will detail specific requirements to be fulfilled by OI4 solutions in order to provide what we consider "rock solid security."

At the core of OI4 interface specifications are the core communication standards. A combination of the best, smartest, and highest-performing features of OPC UA and MQTT ensures easy interoperability of OI4 solutions, already proven in the first OI4 hackathons. With the growing number of OPC UA companion specifications to provide semantics for automation data, this technological tandem is future-proof.

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. eCl@ss 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. Full support for referencing this kind of base level semantics will be a part of OI4.

With OI4 being focused on Industry 4.0, the asset administration shell (AAS) will have to be a major part of OI4 data exchange. Mappings of the asset administration shell to other Industry 4.0 standards are currently underway, ensuring technical compatibility on the basis of this standard. OI4 has identified the AAS as the main interface definition for data to be exchanged between the common cloud central layer and other OI4 components.

Domain models are specific to certain branches of industry. For several industry branches, vendors are currently realizing the market demand for standardized data access. Resulting domain models offer possibilities for added value in OI4 systems. One possibility is the automatic integration of machine data from a standardized domain model resulting in plug & play capabilities for analytics applications. Domain model support can become a major advantage for utilizing OI4 concepts. The list of domain models under consideration will likely be extended in the future. Domain models offer great potential for easy integration if they are modeled to be represented as OPC UA server information models. The leading concepts for OI4 compatibility of such models will be the use of the OI4 identifier and the master asset model.

In addition to the above standards, engineering is a major factor for the successful implementation of OI4. Use of modern engineering tool interfaces will be a goal for OI4 interface definitions. Therefore, state-of-the-art tool interface technologies like AutomationML will be considered as data sources for OI4 components.

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

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 OI4 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 the OI4 ecosystem. For more information on how device manufacturers will be able to achieve this, members should consult the internal 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)

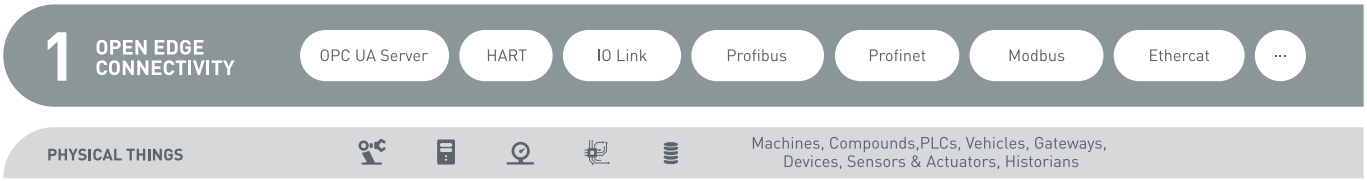


Figure 4 The open edge connectivity layer

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 applications 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 OI4 compliant message payload. This has to be accessible from 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 technical committee does not make presumptions about the physical distribution of the functions described in the reference architecture.

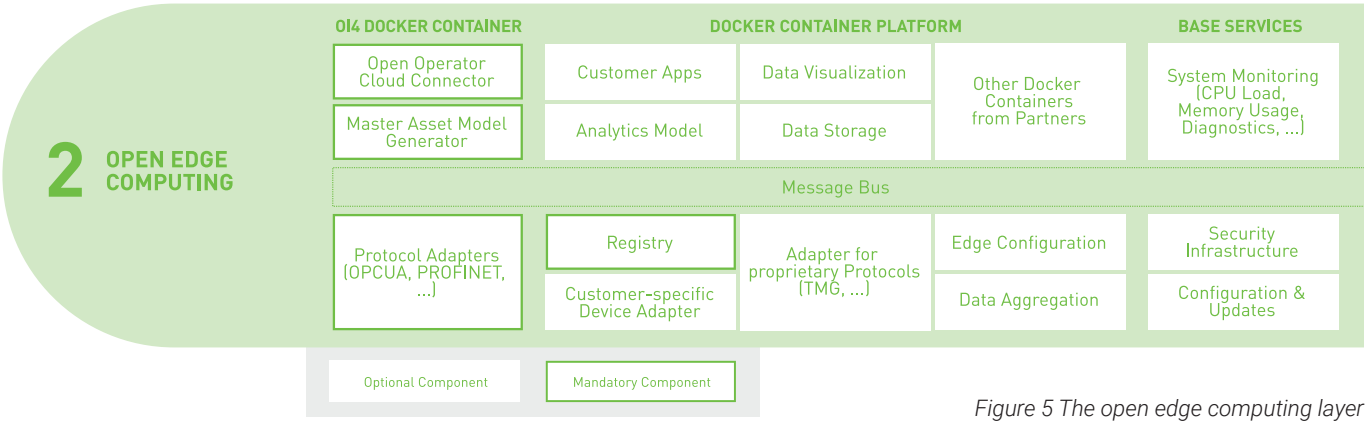


Figure 5 The open edge computing layer

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

Docker container platform

This platform provides the runtime for containerized applications to be run inside the open edge computing layer. Only the most basic services for the open edge computing 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 an MQTT broker handling the OI4-defined topic structure. All data transmissions between containers in this layer (and possibly some going beyond it) must use the message bus.

Open operator cloud connector

In the OI4 architecture framework, every edge computing solution is expected to have a north-bound interface to communicate with the open operator cloud platform chosen by the operator. This component exposes an OI4-compliant communication and information model interface towards the message bus for tasks like device onboarding, while offering a platform-compatible interface to the Open Operator Cloud Platform layer.

Master asset model generator

In order to allow identification and handling of assets in the OI4 architecture, each asset has to be assigned both an OI4 identifier and a master asset model. More details on these concepts will be made available through the OI4 technical specifications. This component is responsible for generating these critical pieces of data for each asset being onboarded.

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 OI4 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 and its collaboration with the Master Asset Model Generator during onboarding in the Development Guideline document.

Customer apps

The docker container platform allows for the development and deployment of customer-specific applications on the open edge computing layer.

Analytics models

Analytics models to be used for data enrichment on the open edge computing layer have to be deployed in the form of OI4-compliant containers, receiving their payload data through the message bus.

Registry

The 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.

Customer-specific device adapter

For devices that have to be accessed by a customer-specific method, the customers can have their own device adapters in the form of OI4-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.

Adapters for proprietary protocols

Especially in legacy devices, proprietary protocols are utilized for device access and management. For these, specific adapters can be provided in the form of OI4-compliant containers.

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 OI4-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.

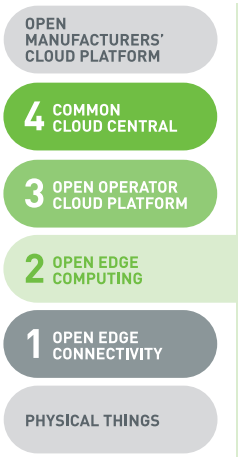
Security infrastructure

For more information on the security concept of OI4, see section 4.

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 OI4 system.

Design principles for the open edge computing layer:



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

1. Docker container platform: This platform provides edge hardware along with basic life cycle management capabilities. For example:

- Edge admin/configuration/container updates
- Message bus
- Runtime health monitoring
- Edge security and data storage

2. Edge computing offerings shall have an open operator cloud connector of specific make for the operator cloud platform to be used. This edge to cloud connector should enable bi-directional communication in the form of:

- Inherited technical semantics of asset model from operator cloud platform/asset repository
- Certificates from device management in the cloud platform for secure communication
- Bidirectional data flow of device data between operator cloud platform and edge computing layer

3.3 OPEN OPERATOR CLOUD PLATFORM

The Open Industry 4.0 Alliance gives customers a choice of operator cloud platforms (as IIoT platform).

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 operator cloud as an IIoT platform should have all basic technical modules, e.g. device management and diagnostic, application enablement tools, data storage and processing, E2E security concepts, user management etc., as depicted in the solution building blocks in Figure 6.

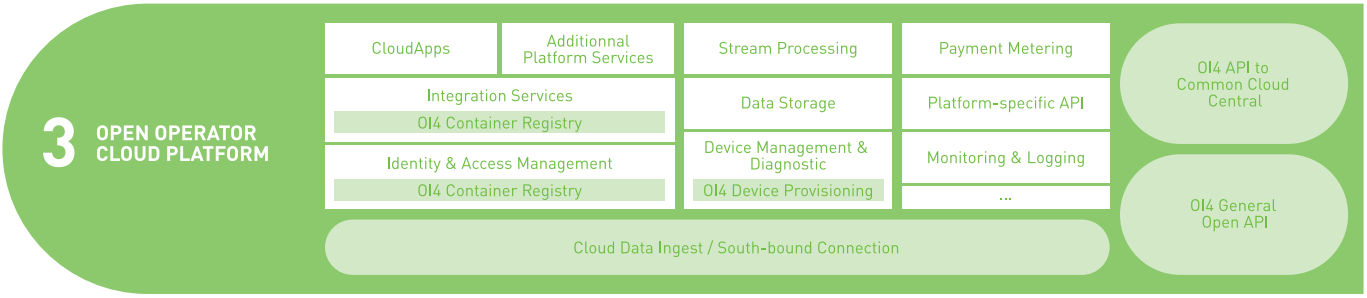


Figure 6 Open operator cloud – Modular capabilities

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 OI4 Alliance are:

1. **OI4 API to common cloud central**
2. **OI4 general open API**
3. **OI4 container registry**
4. **OI4 user and permission management**
5. **OI4-specific device provisioning**
6. **Cloud data ingest/south-bound connection**

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

OI4 API to Common Cloud Central

This API provides a standardized interaction between the Cloud Apps and Additional Platform Services of the Open Operator Cloud Platform and the Common Cloud Central of the Open Industry 4.0 Alliance.

OI4 General Open API

The module OI4 General Open API standardizes across Open Industry 4.0 Alliance members a secure access to other modules of the Open Operator Cloud, e.g. the access to the OI4 container registry or OI4 compliant device information. All APIs are specified and documented by the Technical Workgroup on the base of e.g. Swagger and use case descriptions.

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 scenarios or any composition of them:

1. Operator-side or datacenter-located IIoT platforms as private or hybrid cloud, based on bare-metal or virtualized infrastructure
2. Operator Cloud platform based on hyperscalers (e.g. Microsoft Azure, Amazon Web Services, Google Cloud Services, …) or other highly scalable cloud infrastructure services
3. Operator Cloud platform based on IIoT platform offerings provided by vendors or service providers for specific industrial use cases (e.g. GE Predix, Siemens Mindsphere, Software AG Cumulocity, …)

Cloud data ingest/south-bound connection

Data from multiple connected edge gateways can be ingested to the operator cloud via the technical module Cloud data ingest. Using this endpoint data is forwarded to further cloud components such as the module Stream processing or the module Data storage.

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.

OI4 User & Permission Management

As part of the Identity & Access Management, the OI4 User & Permission Management module 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 OI4 User & Permission Management is a central component that will be accessed by all other components of the Open Operator Cloud Platform to check for legitimization.

Integration services

Services to facilitate the integration of other services in a standardized manner, e.g. CI/CD, orchestration, and load balancing services.

OI4 Container Registry

The OI4 containers will be registered in the container registry of the operator cloud. As soon as the containers are deployed and running, they are registered in the Container Registry and can afterwards be discovered by other services automatically.

Device Management and Diagnostic

The technical module Device management and diagnostics provides for the management of connected edge devices over their complete lifecycle. The module provides provisioning, configuration, maintenance, diagnostics, and decommissioning functionalities, etc.

OI4 Device provisioning

Provisioning of the devices for cloud onboarding, e.g. initial configuration and preparation for cloud connection.

Cloud apps

Cloud apps use the common APIs of the underlying cloud services of the operator cloud to generate value use-case specific.

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.

Data storage

Appropriate data storage is 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. This data storage is accessed by the cloud apps via the services' APIs.

Additional platform services

Services of the operator cloud to offer additional functionality like metadata and structure handling or secure transactions. Services that ensure smooth interaction between other platform modules and applications operated on the operator cloud.

Monitoring and logging

Standardized monitoring and logging services to facilitate the operation of cloud apps and platform components.

Payment metering

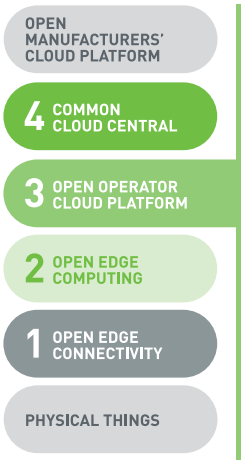
This technical module provides individual cost tracking, metering, and billing capabilities end-to-end along the underlying IIoT stack.

Platform-specific APIs

APIs which provide the basic platform-specific functionality regarding the transaction in between of each technical module of the Open Operator Cloud Platform.

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.

Design principles for interoperability as Open Industry 4.0 Alliance-approved solution – open operator cloud :



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

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

- Should adopt semantic models and integration with common cloud central
- Device management and security (certificate management)
- Data management and data streaming capabilities
- User management and permission management capabilities
- Development framework for members to develop and deploy Industry 4.0 applications
- Interoperable with the Open Industry 4.0 Alliance-approved edge computing platform
- Compliant to OI4 cybersecurity guidelines
- OI4-compliant interfaces for data sharing across cloud apps (cloud-to-cloud)

2. **Additional services (optional) such as: Business process integration, ML/AI, data analytics and asset onboarding for plug & play in conjunction with edge computing platform**

3.4 COMMON CLOUD CENTRAL

The Open Industry 4.0 Alliance mandates the use of a common cloud central layer as the main interoperability component by using a central asset information system to create a standardized semantic model. This enables the adoption of common data semantics in both the open operator cloud and open edge computing layers. It also helps to standardize and simplify application development efforts.

In addition, the common cloud central provides an asset collaboration platform for operators and OEMs (manufacturers) and a centralized catalogue for listing applications and container services offered by Open Industry 4.0 Alliance members.

These tasks are to be provided by a highly standardized and regulated repository of information that offers well-defined interfaces to ensure accessibility of all relevant models to all platforms used. For operators, it will be possible to choose between different services to gain access to the Common Cloud Central services and even combine services for specific Common Cloud Central components. To this end, data exchange interfaces between different implementations will be specified.

Figure 7 The common cloud central

The core elements of the common cloud central are structured as follows:

OI4 component catalogue

In order to allow acquisition and utilization of application functions in an OI4 context, containers have to be loaded into the Open Edge Computing and Open Operator Cloud Platform layers. In addition, operators have to have an overview of existing solutions in OI4 compliant devices and solutions. The OI4 Component Catalogue allows the search for relevant components and also provides links to the products listed.

Semantic Models Repository

As mentioned in section 2.3, the Open Industry 4.0 Alliance will support major domain information standards. The Semantic Models Repository will allow computerized access to the supported domain information standards. Thereby, even assets not fully covered by detailed type descriptions can be utilized and interpreted.

Type Information Repository

In order to allow the best effect of the Common Cloud Central platform of the Open Industry 4.0 Alliance, asset manufacturers are to supply information on the products they sell. This information is type specific and serves as a template for the Asset Administration Shells of concrete pieces of equipment. The information provided by manufacturers will be accessed through the Type Information Repository.

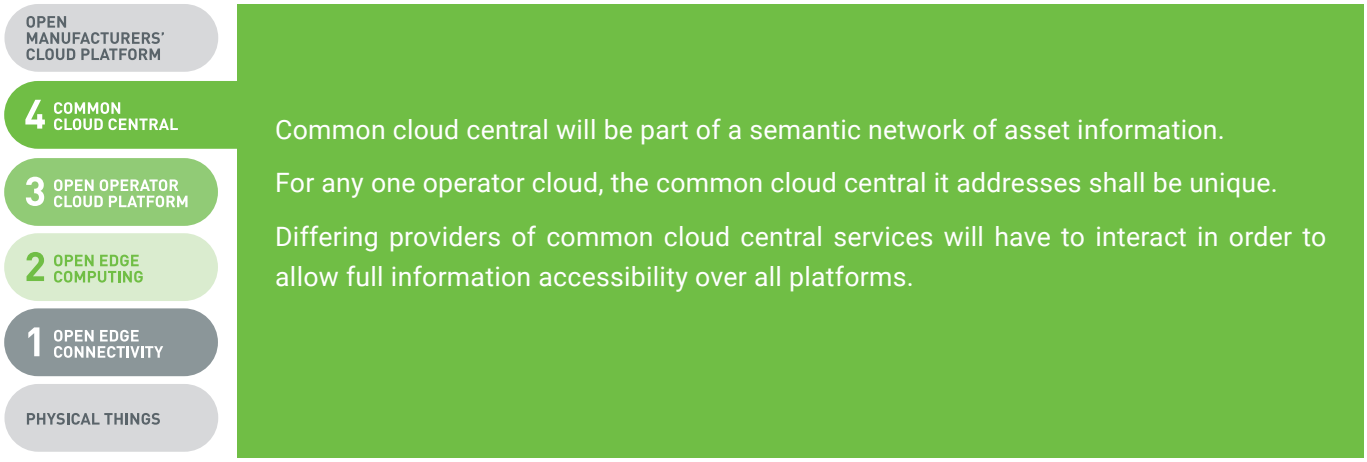
Instance Information Repository

In an Instance Information Repository, Digital Twins of assets are maintained that allow referencing asset instances and look up any historical information about the asset's lifecycle. This is a central component for the added value of OI4, as it makes asset information persistent beyond organizational boundaries. Due to this cross-boundary use case, access rights of the Instance Information Repository differ from those to the Type Information Repository. The semantics of the Instance Information Repository are modeled after those given in the Type Information Repository.

However, especially for brownfield use cases, where no information on a type might be present, the Semantic Models Repository can be utilized as a substitute for a baseline model. Hence, from the point of view of the Instance Information Repository, both the Type Information Repository and the Semantic Models Repository fulfill the same role.

Asset Network

The Asset Network structures the interactions of Asset Administration Shells that represent asset types and instances on the Common Cloud Central layer. The Asset Network in this allows the business processes of the Common Cloud Central layer and also other layers to fulfill their interaction needs with the repositories present on this layer. The data custodianship concept of the Open Industry 4.0 Alliance will be implemented through the Asset Network services. The specific services provided to interact with the asset information will be detailed in future documents.



4 SECURITY CONCEPT OF THE OPEN INDUSTRY 4.0 ALLIANCE

The OI4 Alliance established a dedicated workgroup for the subject of industrial cybersecurity. The workgroup consists of cybersecurity experts from the OI4 member companies. Within the workgroup, all OI4 members are jointly working on various aspects of industrial cybersecurity in order to develop sustainable high value security concepts for customers' use cases.

Security-by-design. The pragmatic nature of the OI4 Alliance also underlies the OI4 cybersecurity workgroup. Security concepts are elaborated and tested closely together with the technical OI4 workgroups.

The OI4 Alliance asserts a clear and comprehensible security concept. Every chosen technology in the OI4 ecosystem must meet the state-of-the-art requirements of security for encryption, authentication, data protection, and data privacy.

The subject of industrial cybersecurity is considered holistically in the OI4 Alliance. Vertical and horizontal deep dives along the IIoT ecosystem are handled dynamically upon request or based on a specific use case relevance.

More details on the OI4 cybersecurity approach can be found in the whitepaper "Open Industry 4.0 Alliance Industrial Cybersecurity Design Principles" dedicated to this topic in particular.

5 ROADMAP FOR OPEN INDUSTRY 4.0 ALLIANCE TECHNICAL SPECIFICATIONS

The technical committee of the Open Industry 4.0 Alliance has devised an ambitious plan for providing firm specifications. The goal is to provide interoperable solutions to the market as quickly as possible. To ensure market impact, important trade fairs in the automation market are cornerstones of the specification schedule. An overview of historic and planned activities is given in Figure 8.

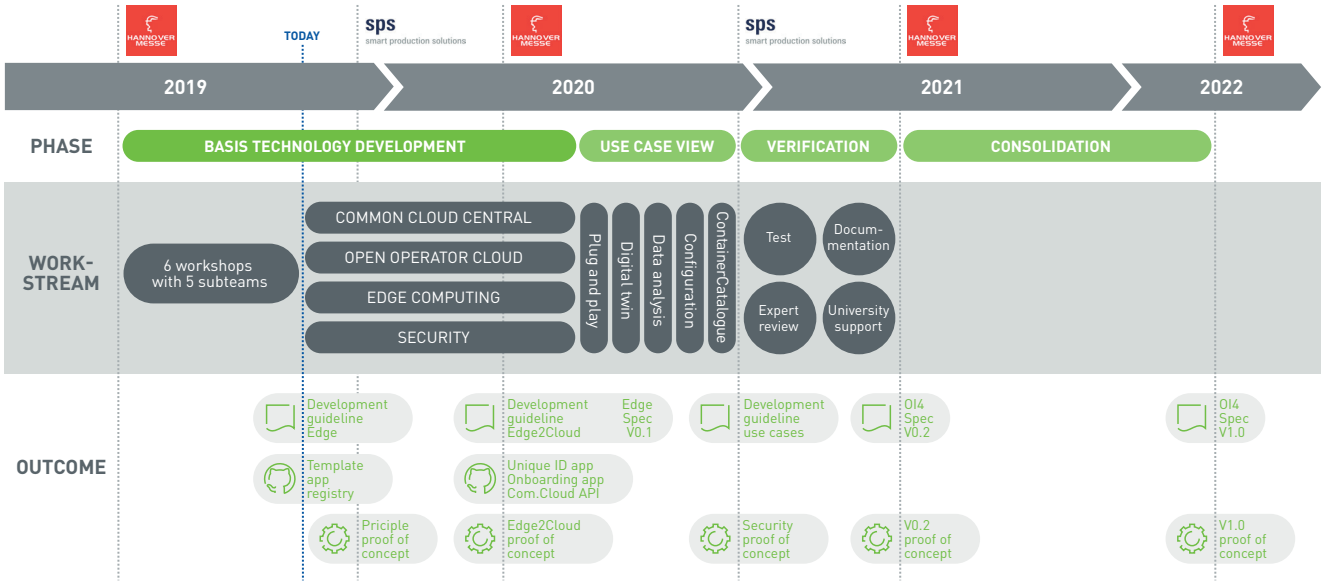


Figure 8 The Roadmap of the Technical Committee of the Open Industry 4.0 Alliance

The technical committee of OI4 has branched into four work streams covering the three main layers of the reference architecture framework (see Figure 2) as well as the security working group. In the middle of 2020, a first specification for the open edge computing layer will have been released and evaluated through proofs of concept. At this point, specific use cases will be addressed in greater detail based on the technological decisions already made. A verification phase will ensure that the first holistic specification covering all layers will be implementable for the Hanover trade show in 2021. An additional year of consolidation will lead to a longterm stable version of the specification.

The overall process will produce several documents that will be distributed in order to gain member feedback on the solutions found for the overall Open Industry 4.0 vision. In addition to specification documents, development guidelines for quick feedback loops will be provided at regular intervals. The goal of this is to ensure membership acceptance of the technical results through dissemination and joint implementation and testing.

6 SUMMARY AND CLOSING REMARKS

As manufacturing companies feel greater pressure from the market to innovate rapidly, support highly-variable product configuration demand, and compress their time to market, they must instill Industry 4.0-driven intelligence and automation into their operations. Customer feedback has confirmed the value proposition of the proposed Open Industry 4.0 Alliance approach to address their current challenges in digital transformation and IIoT adoption.

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**

7 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 – "Verwaltungschale"

Common cloud central – Central cloud asset modeler and asset network offering from Open Industry 4.0 Alliance members

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

OI4 – Open Industry 4.0 Alliance

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

Open edge computing – Operator edge computing platform

Open operator cloud platform – Operator's IIOT platform

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.

www.openindustry4.com