Open Industry 4.0 Alliance

Industrial cyber security design principles

Full Stack Design Reference for integral End-to-End Cyber Security

White Paper (Release Date: 16th February 2021)

OPEN INDUSTRY 4.0 ALLIANCE

Table of Contents

1. Introduction to Open Industry 4.0 Industrial Cyber Security (ICS)

1.1 Why is Open Industry 4.0 concerned with Industrial Cyber Security?

The objective of the Open Industry 4.0 Alliance is to establish an open and interoperable Industrial Internet of Things (IIoT) ecosystem involving all Open Industry 4.0 members. Therefore, cyber security is mission-critical for the success as well as the acceptance within the industry and among applying customers. To guarantee openness and interoperability, a “security by design” approach is a mandatory for robust setups, systems and applications and reduces the risk for all end user business scenarios. All Open Industry 4.0 members are committed to contributing in their best manner possible to a joint, secure IIoT ecosystem that benefits the diverse customer use cases. Therefore, industrial cyber security is an integral part within the alliance and stretches across the different layers of the reference architecture. It has the highest priority and is considered within all workgroups as well as the pilot projects of the alliance in a meaningful and pragmatic way.

1.2 Background and Objective of Open Industry 4.0 Industrial Cyber Security

The number of cyber attacks towards manufacturing companies is increasing at a very high pace. Although a lot of companies still have not been a victim of these incidents, the unavoidable consequences on the business of the affected companies show a huge impact on productivity, availability and costs. This shows that many companies are not prepared for modern cyber risks on all levels of protection. Apart from the growing number of attacks, the amount of connected devices that more and more communicate with each other is also increasing exponentially due to the efforts of digitalization in general and industry 4.0 specifically. Therefore, the possible targets increase and make cyber attacks unfortunately a growing market in terms economic “success”.

The reasons for this circumstance are manifold. Across industries, operators often have decades-old OT (Operational Technology) landscapes that lack the security mechanisms of modern systems. As more and more value adding IIoT solutions find their way into those long-established OT landscapes, the operators of those OT landscapes are creating a new attack vector for potential cyber-attacks. However, what’s the solution? Taking the risk in account? Or missing the benefits of value-adding solutions and technologies? What is the competitor doing? Am I losing my competitive advantage if I do not modernize my OT landscape? Surely, many questions come to mind when thinking about this topic. One of the answers lies in the need of a well thought cyber security concept across the underlying IT and OT landscapes. Part of this cyber security concept is a wise selection of OEMs, technology providers, asset suppliers, and service providers whenever an investment in modernization measures is foreseen by the operator. The associated purchase always needs to be aligned with the company’s cyber security strategy. A supplier that is not able to prove its product’s compliance with the operator’s cyber security needs is a security risk for the operator’s business. The Open Industry 4.0 Alliance asserts a clear and comprehensible security concept along the IIoT ecosystem that Open Industry 4.0 members are following. Every chosen technology in the

Open Industry 4.0 ecosystem must meet the state-of-the-art requirements of security for encryption, authentication, data protection, and data privacy. Through these measures the alliance is seeking to ensure the claim for cyber security in industrial IoT applications and proactively help to protect the operators' IT and OT landscapes.

1.3 How is Open Industry 4.0 dealing with Industrial Cyber Security?

Cyber security is an elementary and integral part of the basic system architecture for all products developed by the members of the Open Industry 4.0 Alliance. The integral approach towards cyber security is needed due to the layer structure of the reference architecture. All layers have to be included and security concepts need to be coordinated and aligned within the ecosystem.

Luckily, cyber security is nothing that just came into the Open Industry 4.0 mind. It is a task and objective that is already covered by various institutions, networks and associations. Therefore, all fundamentals are already covered by norms, regulations as well as best practices and whitepapers. Due to the deep integration of cyber security in the individual architecture layers, security-relevant functions are taken into account directly when developing solutions. All recommendations and guidelines are based on industry-known standards for similar applications.

The technical implementation is accompanied by an independent committee of experts. This committee, consisting of members of the alliance, determines the necessary framework conditions and is available to advise all members of the alliance. The aim of the Open Industry 4.0 Alliance is a comprehensive consideration of all relevant security aspects on all layers of the reference model based on existing norms and standards.

1.3 What are Open Industry 4.0´s deliverables in the context of Industrial Cyber Security?

Due to the current developments in attack scenarios and threats and the associated requirements for security measures, Open Industry 4.0 Alliance faces the challenge of providing secure development and operating concepts.

The solution approaches developed in Open Industry 4.0 Alliance contain basic security aspects according to the current state of the art. As a basis for reliable product development, the recommendations can be adapted to meet industry-specific requirements. Furthermore, measures are taken into account that enable the systems to be integrated into established product safety management systems.

The security functions used in the technical guidelines serve as recommendations for action for future product developments. The application of standardized requirements and the implementation of best practices on the part of the manufacturer result in a detailed platform for safe product operation.

The recommendations of the Open Industry 4.0 Alliance must be checked for the respective purpose when applied. The respective security measures are not absolutely sufficient in every area of application or may even be oversized. When applying the recommendations, it is mandatory to carry out your own risk analyzes and to define the respective safety requirements. In addition, the Open Industry 4.0 alliance cannot assume any responsibility for maintaining the respective security level over the desired product life cycle. The processes required for this must be implemented by each user himself.

2. Open Industry 4.0 Alliance Security Reference Architecture

2.1 Roles and Responsibilities in the Open Industry 4.0 Ecosystem

Securing an IIoT ecosystem requires a defense-in-depth strategy diligently followed by various members across the IIoT value chain. The defense-in-depth strategy should be developed and executed with active participation of various alliance members involved with the manufacturing, development and deployment of IIoT applications, devices and infrastructure.
Amongst the member companies within the Open Industry 4.0 Alliance the following roles can be found:

- Application Provider
- Technology Provider
- Connectivity Provider
- System Integrator
- OEM/Manufacturer
- Operator
- Service Provider

Each role has an individual perspective on the subject as well as responsibility within a secure IIoT ecosystem.
Table below summarizes on a high level the responsibilities of various alliance members in achieving a holistic defense-in-depth strategy for IIoT.

Roles involved	**Responsibilities**
Application Providers: Members providing relevant software applications within their industry/domain specific expertise	• Follow a secure software development lifecycle • Carefully consider open source software components/tools and integrate only if needed • Ensure vendor risk management when outsourcing development activities
Technology Providers: Software (IaaS, PaaS) and Hardware (Edge devices) technology providers who enable digitization and members offering solutions and services for industrial connectivity	Software (IaaS, PaaS) providers: • Physically protect infrastructure • Ensure all systems are up-to-date with patch management best practices • Monitor and protect against malicious activity • Manage and protect cloud credentials • Audit frequently

	Hardware providers: • Design the hardware to meet minimum security requirements • Ensure hardware is tamper proof • Ensure secure software updates
System Integrators: Members offering system integration services in OT (Operational Technology) and IT (Information Technology)	• Deploy hardware securely, for e.g., control access to the hardware with strong authentication and authorization • Separate assets based on criticality using appropriate network security best practices • Ensure a key management mechanism is present to keep authentication keys safe
OEMs/Manufacturers: Makers of industrial machinery, components, sensors, actuators, PLCs and robots	• Industrial automation and control system security
Operators: End customers who operate industrial assets in discrete and process industry	• Ensure proper supply chain risk management practices • Ensure suppliers provide security assurance for their solutions and comply with internal security standards
Service Providers: Members providing services throughout the life cycle of an industrial facility	• Ensure proper life cycle risk management practices • Ensure work methods and processes provide security assurance for customer solutions and comply with customer security standards

Table 1: Roles and Responsibilities in the Open Industry 4.0 Ecosystem

2.2 Full-Stack secure Solution Architecture

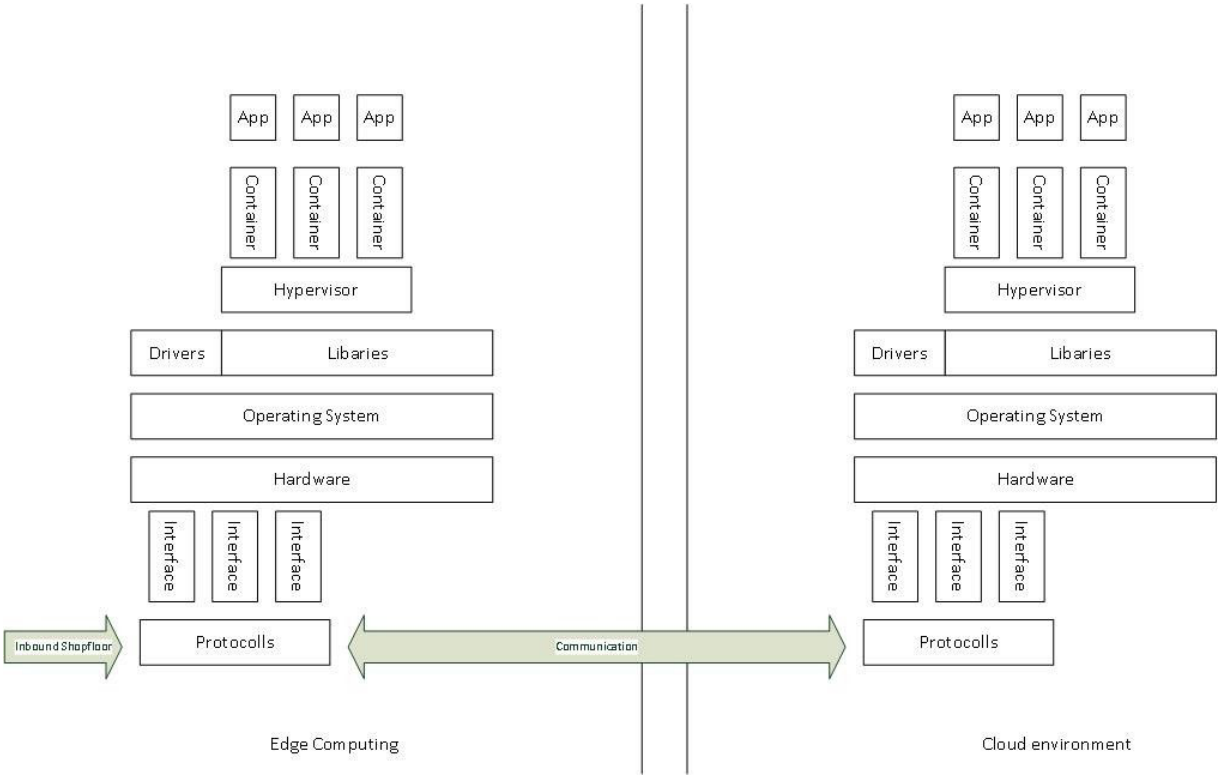
Based on the claim of the Open Industry 4.0 Alliance, security relevant functions are implemented based on the following architecture stack. The Security-in-Depth method should enable the user to consider all necessary aspects and implement appropriate measures. In addition to the functional requirements, further non-functional requirements must be considered. These include, for example, product maintenance processes and the integration of security incidents into the corporate communication policy. An inadequate security consideration over the entire life cycle of the product can lead to a complete cancellation of the desired protection goal. The security-in-depth approach minimizes the risk but does not eliminate it.

When considering security functionalities, the focus of the respective solution must be taken into account:

- A pure software application based on a container cannot contain security functionalities of the underlying layers.

- The provision of an operating system provides basic libraries and functions to the overlying layers, but application security is the responsibility of the respective vendor

In addition, other basic principles relevant to safety should be taken into account in product development. An overview of the errors to be avoided was prepared by MITRE. The Common Weakness Enumerations (https://cwe.mitre.org/) are the most common development errors that can provide a weakness in the code.



3. Cyber Security Best-Practices, Regulations and Standards referred to by the Open Industry 4.0 Alliance

3.1 Security considerations on Layer 1 and 2

Due to the architecture of the Open Industry 4.0 Alliance, different security requirements are placed on the solutions. On layers 1 and 2, basic security functionalities are required to ensure the individual protection goals.

According to IEC 62443-1-1, the following protection goals are defined in subsection 5.3

- identification and authentication IAC
- use control UC
- system integrity SI
- data confidentiality DC
- restricted data flow, RDF
- timely response TRE
- resource availability RA

These protection goals are assigned to a corresponding Security Level (SL):

- SL 1 accidental misuse
- SL 2 intentional experiments with simple means
- SL 3, like SL 2, but with knowledge and extended means
- SL 4, like SL 3, with complex means and with IACS expertise

Depending on the position in the life cycle to which the SL refers, a distinction is made between:

- SL-T (Security Level Target), this SL to be achieved is a result of the threat/risk analysis
- SL-C (Security Level Capable), SL, that a device or system can reach when properly deployed and configured
- SL-A (Security Level Achieved), the SL achieved and measurable in the overall system

The user of the end device must determine the SL-T by means of a risk assessment. A manufacturer of a terminal device can only identify the SL-C. The manufacturer of the complete system indicates the SL-A achieved in the final. A system is correctly executed if SL-A corresponds to the SL-T.

According to the desired or required security level, functions must be implemented in accordance with IEC EN 62443-4-2.

The implementation of the required technical measures must be extended or supported by processes and measures based on IEC EN 62443-4-1 if product certification by a notified body is sought.

3.2 Considerations about Cloud security requirements (Layer 3 and 4)

In contrast to on-premises or security measures on hardware platforms, other aspects are of fundamental importance in the cloud area. In the various cloud models Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), different requirements are placed on the solution provider based on distributed responsibility. The challenge of distributed responsibility is to consider all factors necessary for the secure operation of the desired model. A misinterpretation or a function that is not taken into account can, if necessary, cause great damage. Taking into account the full stack, cloud architectures are based on the same model. The provided cloud models make demands on all underlying layers.

To provide technical security functionalities, it is necessary to validate the associated service contracts with the company's own compliance requirements. This includes, for example, the contractual requirements for service providers who perform activities on behalf of the provider. This includes, for example, the operation of the data center (IaaS) or the proper destruction of data carriers.

With regard to the operation of a global cloud solution, measures in the area of data protection regulations must be fundamentally validated. The possibility of storing data outside a desired jurisdiction can lead to massive penalties from the legislator and to claims for damages from customers.

The recommendations of the Cloud Security Alliance (https://cloudsecurityalliance.org/) can be used as a basis for necessary requirements.

If your company is already making efforts to obtain 270xx certification, ISO 27017 can also be taken into account to specify the necessary measures. The 27017 is the extension of ISO 27002 to include cloud-specific factors.

3.3 Requirements for Upstreaming connectivity

A fundamental goal of the Open Industry 4.0 Alliance is interoperability between the individual layers and participants. To achieve this goal, a unified schema for data sources and sinks is indispensable and decisive for the success of the architecture. For this purpose, communication between Layer 1 and the superordinate instances is based on the specification of International Data Spaces in the form of DIN Spec 27070.

3.4 Vulnerability Management System

The use of a vulnerability management system (within a Security Management System, SMS) is elementary for the security of products. In principle, an SMS can be divided into two components:

3.4.1 Product Security and Incident Response Team (PSIRT)

Across all levels of the Open Industry 4.0 Alliance reference architecture, it is essential to maintain the solutions throughout their entire life cycle. The challenges of this instance are:

- Detection of vulnerabilities
- The analysis and evaluation
- Removal of weak points
- Publication and communication of relevant information
- Training of managers and employees

During implementation, the frameworks of the "Forum of Incident Response and Security Teams" (www.first.org) have proven their worth in IT. For vulnerability management in industrial components, the framework for Product Security and Incident Response Teams can be used as a basis for implementation. This framework defines the necessary requirements and the corresponding results of the respective field of action

3.4.2 Secure Software Development Lifecycle

Without a structured and standardized approach to the development of safe products, it cannot be tracked and guaranteed throughout the product's life cycle. In addition, weak points can be tested and eliminated in early development phases. This "Shift-Left" approach saves capacities since the elimination of weaknesses in later development phases is costly and therefore ties up capacities. The use of static application security testing solutions can automatically find weaknesses in builds and provide instructions for fixing them.

Furthermore, the consideration of security measures already in the product planning phase is necessary, since architectural requirements can be set in advance. This way, a subsequent adjustment can be avoided.

In recent years, various approaches have been established in the area of Secure Software Development Lifecycle. These include the SDL from
- Microsoft (https:/www.microsoft.com/en-us/securityengineering/sdl) and the SAMM from
- OWASP (https://owasp.org/www-project-samm/).

Relevance of Norms and Standards regarding Open Industry 4.0 Layer structure

Norm, Standard / Layer	Layer 1 - Devices	Layer 2 - Open Edge Computing	Layer 3 - Open Operator Cloud	Layer 4 - Common Cloud Central
IEC 62443-4-1 (organizational focus)	x	x		
IEC 62443-4-2 (device focus)	x	x		
OWASP		x		
SSDL - Secure Software Development		x		
DIN SPEC 27070		x		
PSIRT		x		x
IEC 27017			x	x
Cloud Ecosystem			x	x
CSA requirements			x	x

The norms and standards apply to the different layers of the Open Industry 4.0 setup. Nevertheless, a seamless interaction as well as interoperability is targeted with the combined approach along the layers. The order of importance and suitability for Open Industry 4.0 compliant products follows the following listing:

- officially available norms and standards from organizations, e.g., IEC, DIN
- Recommendations from vendors
- Well-Known Best Practices (can but must not be vendor independent)

4. Open Industry 4.0 Alliance security compliance requirements

Due to the different requirements and purposes of the products, it is not possible to define the necessary security functions. The generalization of functions can lead to an oversizing of the scope or an underestimated requirement can lead to a weak execution.

Basically, and decisive for the security requirements of products is the recognition of the necessity and the willingness to accept the effort and thus the costs for secure products. When developing safe components, the challenge lies in the above-mentioned safe development process and the maintenance of integrated solutions over the entire life cycle. The maintenance of the life cycle of a product also

includes checking the implemented functions by regular penetration tests. The requirements of the Open Industry 4.0 Alliance include the following requirements.

4.1 Security requirements for edge computing devices (Open Edge Computing Platform)

As a component manufacturer in the field of edge computing, an SL-C 2 of the 62443-4-2 should be aimed for. The focus of the Open Industry 4.0 Alliance is on provisioning containerized applications and does not place any direct demands on the security of the underlying levels beneath these applications. However, general requirements about the environments will be made. It should be in the own interest of the component manufacturer to evaluate and integrate the necessary measures for the other levels in the product design and the development process.

4.2 Requirements for Cloud-based solutions (Open Operator Cloud and Common Cloud Central)

In the area of cloud-based solutions, the requirements for secure processes must be implemented at the highest level both during development and operation of the solution. The attack vectors and the associated damage potential must be comprehensively considered by the provider of the solution and appropriate measures implemented in conjunction with the service provider. In addition to this, data protection relevant processes and measures must be developed.

At the time of writing this white paper, there are no legally defined requirements for security in industrial components. Due to this fact, the security requirements of the Open Industry 4.0 Alliance are based on self-declarations of the respective manufacturer.