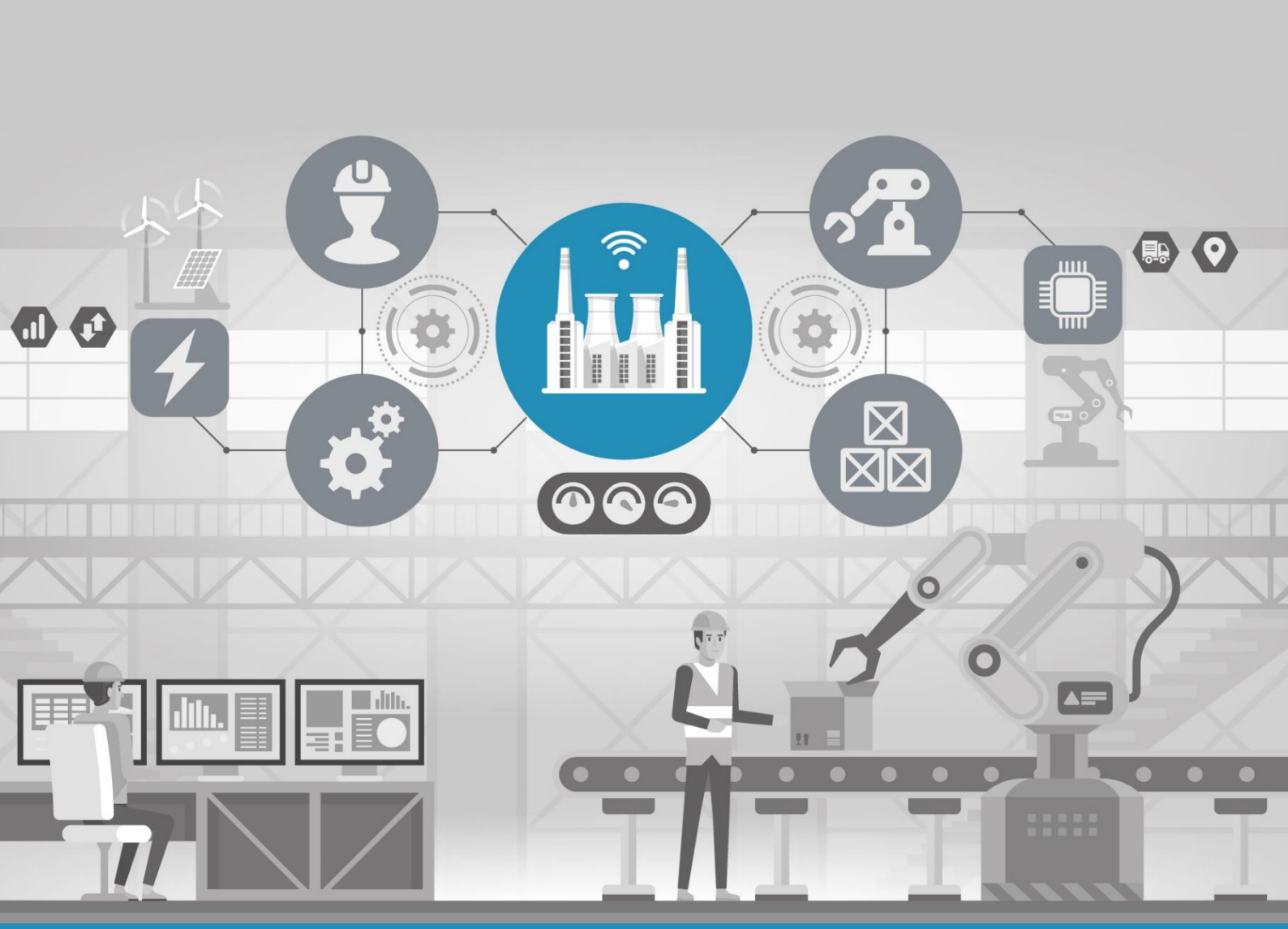


*IIP-Ecosphere Whitepaper*

# Current Industry 4.0 Platforms – An Overview

Christian Sauer, Holger Eichelberger,
Amir Shayan Ahmadian, Andreas Dewes,
Jan Jürjens

White Paper IIP-2020/001-en

IIP-Ecosphere
Next Level Ecosphere for Intelligent Industrial Production

## Disclaimer

The contents of this document has been prepared with great carefulness. Although the information has been prepared with the greatest possible care, there is no claim to factual correctness, completeness and/or timeliness of data; in particular, this publication cannot take into account the specific circumstances of individual cases.

Any use is therefore the reader's own responsibility. Any liability is excluded. 

This document reflects only the views of the authors at the time of publication. The Federal Ministry for Economic Affairs and Energy or the responsible project agency are not liable for the use of the information contained herein.

**Publication:** January, 2021 (translated version of the original IIP-2020/001 whitepaper from November/December, 2020, partially with additional explanations on the translation if needed) on https://www.iip-ecosphere.eu/

**DOI:** 10.5281/zenodo.4485756

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

# Executive Summary

This white paper provides an overview of current Industry 4.0 platforms, particularly from the perspective of the IIP-Ecosphere project, which is funded by the German Federal Ministry for Economic Affairs and Energy (BMWi) in the “KI-Innovationswettbewerb” (AI innovation competition). The focus is on topics such as interconnectivity, digital twins, openness, security and the use of AI in the context of smart manufacturing. The document describes the approach to data collection, the detailed results for individual industrial platforms, and a summarizing overview. A total of 21 industrial platforms are analyzed based on publicly available documents using 16 analysis topics. Both platforms and analysis topics originate from intensive discussions between the IIP-Ecosphere project partners.

In particular, the analyzed platforms cover the required basic functions. For example, a wide range of communication protocols is often provided and a wide variety of cloud services are integrated. Even newer trends such as artificial intelligence can now be found in the platform descriptions. However, the range of functions also varies greatly among the platforms. Newer standards such as OPC-UA, UMATI or the Industry 4.0 Asset Administration Shell are often used only cautiously, if at all, which may be due in part to the development history, but also due to strategic considerations.

Based on the cross-platform analysis of the 16 topic areas, we derive challenges for future platforms and especially for our work in IIP-Ecosphere. These include topics such as open ecosystems, extensible architectures with standardized interface descriptions, flexible and dynamic support for AI procedures, secure and unified data exchange (for data sharing, resource sharing, and data usage control) as well as end-to-end and consistent configurability that builds user trust in the respective platform. Standardization of (some of) these topics would be desirable to improve exchange and interoperability between platforms and platform ecosystems and to avoid vendor lock-ins.

# Table of Contents

# 1 Introduction

## 1.1 Motivation and Goals

The digitization of industry contributes to the performance of technical systems and their processes, but also increases their complexity. For the digitization of the industrial production, approaches are currently being developed, introduced and evolved under the keywords Internet-of-Things (IoT), Industrial Internet-of-Things (IIoT) or, especially in the German-speaking world, "Industrie 4.0" (I4.0, Industry 4.0). To support the implementation of IoT, IIoT and I4.0, various vendors provide software platforms with different features.

Currently, however, the platform landscape is rather diverse: The authors of [13] name more than 450 different IIoT platforms, and [7] mentions 1266 vendor/provider companies. Non-uniform interfaces and protocols [3], lack of standardization [2, 4, 6, 16], fear of proprietary implementations [2, 4, 6, 16], or concerns about data sovereignty and protection [3, 4, 8, 17] contribute to a further fragmentation of the platform landscape, to incompatibilities between platforms, to barriers for deployment in practice, and, thus, to overall obstacles for innovation.

The vision of the IIP-Ecosphere project, which is funded in the BMWi[1] “KI-Innovationswettbewerb” (AI innovation competition), is to achieve an innovative leap in the field of industrial production based on networked, intelligent, autonomous systems to increase the productivity, flexibility, robustness and efficiency of Industry 4.0 or IIoT. The goal is to build a novel ecosystem - the "Next Level Ecosphere for Intelligent Industrial Production" - enabling a "next level" of intelligent industrial production. A core activity in IIP-Ecosphere is the exploration and realization of a cross-enterprise virtual platform that connects both, existing devices and factory installations in a vendor-independent manner, and provides Artificial Intelligence (AI) on such installations in a secure and flexible manner. In addition to the low-threshold application of AI procedures, AI procedures (or AI techniques) should be provided as optimally as possible on (or close to) manufacturing devices and be linkable to platform services. The platform should also enable data sharing and provide required protection and security mechanisms.

Before planning and implementing such a platform, it is essential to understand the landscape of current IIoT platforms, in terms of the functionalities that are commonly used in practice, the innovative evolution of existing concepts, and the identification of gaps and problems in existing platforms. However, IIP-Ecosphere's goal is not to add just another platform to the existing landscape. IIP-Ecosphere will develop a so-called **virtual platform** [20], i.e., take up platform services of existing, already installed protocols and platforms, integrate them appropriately and offer additional, innovative services on top. In order to identify the opportunities and requirements, we have already prepared a comparison of IIoT platforms in the competition phase of the “KI-Innovationswettbewerb”. However, that comparison focused more on exploring the current landscape as well as on top-selling platform vendors. The **contribution of this white paper** is an overview of current and relevant Industry 4.0 platforms in the context of IIP-Ecosphere as well as a systematization of capabilities and features of current platforms, but also the identification of gaps in terms of not yet provided (but desirable) capabilities.

This platform overview serves as the basis for developing a vision for the IIP-Ecosphere platform and, subsequently, defining requirements as well as the design of this overarching virtual platform. This is also the motivation for detailing and expanding the original comparison of 10 platforms to additional platforms as well as expanding to additional analysis topics that have emerged from the discussions in IIP-Ecosphere. In total, this white paper examines 21 IIoT platforms with respect to 16 analysis topics. This white paper documents the capabilities of each platform and also provides a clear summary as well as a discussion of the results.

[1] https://www.bmwi.de/Redaktion/DE/Publikationen/Technologie/ki-innovationswettbewerb.html

## 1.2 Interactions with other Initiatives

Existing IIoT platforms are being developed while facing trade-offs between business interests, standardization efforts and customer requirements. Initiatives in this area include in particular:

- Industry 4.0 **standards and specifications** that aim to achieve interaction between Industry 4.0 devices and platforms. Examples of standards in this area are RAMI 4.0 [19], Asset Administration Shell [1, 24], OPC-UA[2] or oneM2M[3].
- **Open source initiatives** that implement standards and specifications, such as, the BaSyS project[4] for Asset Administration Shells or protocols or services in the Eclipse IoT ecosystem[5].
- Various **platform overviews** are available, such as short summaries [5, 10, 22], larger collections [13], market analyses [9], or scientific overviews [11, 18], the latter, however, with comparably few analysis dimensions. A directly related work is the Fraunhofer IAO market study [7] published in 2017. At first glance, this work and [7] address rather similar analysis topics. However, there are also significant differences, e.g., we capture topics like "artificial intelligence", edge computing or systematic configurability. Furthermore, in [7], the information about the platforms was collected in open, direct interaction with the vendors, while our analysis is based on vendor documents.

Although this white paper also focuses on the properties of relevant IIoT platforms, it analyzes them in particular from the perspective of the IIP-Ecosphere project. Although the analyzed platforms and analysis topics partly overlap with other works, the compilation of the platforms, the selection of the analysis dimensions and the approach justify an independent analysis.

## 1.3 Structure of the Document

This document is structured as follows: In the next chapter, we describe the approach used to obtain the results, in particular the analysis topics used in data collection and the selection of platforms. In Chapter 3, we apply the analysis topics to the individual platforms and describe the results for each platform. Chapter 4 summarizes and discusses the individual results in the form of tables, figures, and discussions. Chapter 5 highlights the validity of the approach and the presented results (threats to validity). Chapter 6 concludes this document and provides perspectives on the next work in IIP-Ecosphere. Chapter 7 lists work used and referenced in this document.

# 2 Approach, Analysis Topics and Platform Selection

The goal of this work is to provide a systematic and objective overview of the capabilities of current IIoT platforms[6] for Industry 4.0 applications. The planning and execution of such an overview includes:

1. The **definition of topics** or questions for which the individual platforms are to be examined. This involves both, the functions offered and the desirable functions that may not yet be available. As stated above, we base this definition of topics on the perspective of IIP-Ecosphere on AI-supported production in Industry 4.0.
2. The **selection of concrete platforms**. The set of platform candidates is very large. As mentioned in the introduction, there are more than 450 different IIoT platforms [13] or more than 1266 known vendors [7]. While an analysis of all these platforms would provide a comprehensive overview, it is neither feasible nor targeted within the scope of IIP-Ecosphere's

[2] https://opcfoundation.org
[3] https://www.onem2m.org/
[4] https://www.basys40.de/
[5] https://iot.eclipse.org/
[6] Because our focus is on IIoT, we use only the term IIoT in the rest of the document, implicitly meaning IoT in places where this generalization is meaningful.

capabilities and goals. Therefore, we limit ourselves to a pragmatic selection that includes, on the one hand, the vendors with the highest sales - these were already considered in the original analysis of the competition phase - and, on the other hand, platforms that are considered to be of particular interest for the project based on the experience of the project partners.

3. The **collection of raw data** for the individual platforms. For this purpose, the authors searched the respective vendor sites for information and documents, analyzed them with regard to the previously defined topics and questions, and recorded the information.
4. The **analysis of the raw data**, i.e., a summary of the data in the form of overviews and a discussion or interpretation of the aggregated data.

In the following four subsections, we detail these four steps.

## 2.1 Analysis Topics

In order to capture the existing and (from IIP-Ecosphere's point of view) desirable capabilities, we have created a list of relevant topics in discussion with interested IIP-Ecosphere partners (especially in the sub-projects[7] Think Tank “Platforms” and “AI Accelerator”). Besides general information about the platform and references to relevant standards (see also Section 1.2), basic functionalities such as security, communication protocols, openness, extensibility, use of digital twins [23], device management or cloud connectivity are relevant for this overview. From the particular perspective of IIP-Ecosphere, further topics like edge/fog computing, software deployment, (systematic) configurability, data protection, data security, AI support or ecosystem building capabilities are added.

In this section, we introduce all analysis topics. For each analysis topic, a short explanation or some sample questions have been formulated so that the goal of the respective topics is explained and, thus, the uniformity of the data collection is supported. For some topics it is useful to sub-structure the respective topic. It is quite conceivable that individual platforms may offer interesting capabilities that could be allocated to further topics that are not covered here. These capabilities are captured in the generic analysis topic "other technical capabilities" (T16). Since we do not specify a structure for this topic and it is considered as additional information, the author performing the analysis decides whether and how to capture respective information. In addition, it may not be possible to identify information for some topics in the vendor documentation being analyzed. This is indicated by "*No information available*" in the presentation of raw data per platform in Chapter 3. If this applies to all sub-topics of a certain topic, the structuring into sub-topics can be omitted and the "*No information available*" marker can be used directly at the level of the overarching analysis topic. Likewise, the structuring can be omitted if insufficient information was identified in the vendor’s documentation for the respective sub-topics.

In the following, we detail the analysis topics briefly listed above. In Chapter 3, we will present the results for each platform in the sequence given here. Chapter 4 also takes up the order to summarize and analyze the results across platforms.

**T1. Overview**

General information about the platform and the platform vendor or provider.

a) **Name of the platform**
The name of the platform

b) **Platform vendor or provider**
Name of the vendor/provider, registered address of the provider (country)

c) **Vendor summary**

[7] All parts of the project are explained on https://www.iip-ecosphere.eu/

Technical and less marketing-oriented statements of the provider about the platform, if feasible in terms of a quote.

d) **Platform components**
Components of the platform, such as middleware or dedicated components like device managers or analysis tools.

e) **Online marketplace platform**
Can the platform be used as an online marketplace?

f) **Mobility platform**
Can the platform be used for mobility solutions, such as fleet management?

g) **B2B context**
Is the platform aimed exclusively at industrial customers?

h) **B2C context**
Can end consumers also use the platform?

i) **Platform users**
Who uses the platform? Which industries use the platform?

j) **Fields of application**
In which areas/domains has the platform been applied so far?

k) **Market penetration**
To what extent and by what type of customers is the platform used? If applicable, list (in extracts) the customers if named in the materials.

**T2. License information**

Information on the licenses of the software solutions offered by the platform.
Information on licenses regarding any open source software used in the platform.

**T3. Protocols**

Which communication protocols are supported by the platform? Which IIoT/IoT-specific communication protocols are supported by the platform? Are there any special hardware or software solutions for connecting devices or protocols?

**T4. Edge support**

Edge or Fog devices bring IT capabilities closer to production technology. Recently, IT and OT technologies [14] are converting, e.g., to combine real-time capability on the OT side with further non-real-time processing on the IT side.

**a) Overview**
How are Edge (or Fog) devices used in the platform? What role do edge devices play in the context of the platform? Are there edge-specific components in the platform? What are the roles of edge-specific components in the platform?

**b) Communication**
How and on which channels do edge devices communicate with connected IIoT devices, the platform itself, or possible third-party services? Can edge devices communicate bi-directionally, i.e., both to stream data to, e.g., the platform, and to accept commands from the platform's services and applications?

**c) Memory usage**
What options for storing data from connected IIoT devices can be used by edge devices?

**d) Specific capabilities**

Does the platform offer special capabilities and/or services for edge devices? Can calculations be performed on edge devices? Can edge devices in the platform be used by customers in such a way that customers can develop special (own) solutions?

**T5. IIoT devices**

Capabilities of the platform to support "classic" IIoT devices, especially devices without edge/fog capabilities.

**a) Device connectivity**

Which capabilities does the platform offer for physically connecting IIoT devices? Which capabilities does the platform offer for integration/connection with devices in other platforms?

**b) Device management**

Which IIoT device management capabilities are offered by the platform?

**c) Deployment, provision of software**

How are software/software updates deployed to IIoT devices? How software is made available within the platform? How services are made available within the platform?

**T6. Security**

What security standards and techniques are used/supported by the platform? Are there specific security solutions within the platform? Are there specific security techniques for Edge or Fog devices? Is personal data processed?

**T7. Data protection**

Which technical or organizational measures (such as pseudonymization, or anonymization) are in place to effectively implement data protection principles (DSGVO[8]/GDPR Article 5 - transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality)?

**T8. Cloud support**

Does the platform offer the use of its own cloud or support for third-party clouds and if so, what cloud usage options are offered? Can the platform only be used via a cloud or is it usable within a (special, local) cloud or are local (on-premise) installations possible?

**T9. Scalability**

Can a customer's own IIoT/IoT applications scale within the platform? How well can an IIoT/IoT application scale within the platform? Does the platform offer technical features that particularly support scaling?

**T10. Digital twins / Asset Administration Shells**

Digital twins [23] are used in the Industry 4.0 environment to make information (and simulations) of assets such as machines but also products available in a digital way, i.e., to read out information or also to control assets. Asset Administration Shells (AAS) [1, 24] are intended as a uniform interface for digital twins in Industry 4.0.

**a) Digital twins**

Does the platform offer the modeling and use of digital twins? Does the platform provide any special features for modeling and using digital twins?

**b) AAS approach used for IoT devices**

Is there any link in the platform or in the documentation of the platform between the concept of IoT devices and the Industry 4.0 AAS concept?

[8] https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

**c) AAS approach used for edge devices**

Is there any link in the platform or in the documentation of the platform between the concept of edge devices and the Industry 4.0 AAS concept?

**T11. Data management and data analysis**

Does the platform offer capabilities for collecting, analyzing, and managing IoT data? If so, what processes and services does the platform offer? Can non-platform data streams be used by customers?

**T12. Offered AI methods**

Which AI methods (e.g., anomaly detection or rule-based triggering of events on IoT devices) does the platform offer? Can customer-owned AI techniques be applied in the platform? Can third-party AI implementations be used?

**T13. Openness and Extensibility**

Platform development cannot cover all conceivable possible uses and offer realizing software components. Frequently, interfaces or other capabilities enabling openness or extensibility are offered. While this is very often the case for protocols (T3) (and should be mentioned there), it may not be typical for data processing. In contrast to ecosystem capabilities (T15), the focus here is more on vendor extensions or customer-specific extensions.

**a) Store**

Does the platform have its own online marketplace, sales platform, for the software solutions and/or services offered by the platform?

**b) App management support for/by developers**

Are developers supported in the development and management of applications for the platform and if so, how is this support realized?

**c) Use of "external" algorithms or "external" data**

To what extent can algorithms, such as analysis procedures, that are not offered by the platform be used independently by customers or integrated into the platform? To what extent can data that does not originate from/in the platform be collected and used in the platform?

**d) AI interfaces**

Does the platform offer interfaces to the platform's own AI processes? Can customer-specific processes be used here?

**T14. Systematic Configurability**

To what extent can the platform itself or its applications and services be configured by customers to realize customer-specific requirements/scenarios? Various options for implementing systematic configurability are known. These range from "simple" (possibly not so systematic) configuration files up to configuration models (in advanced cases software product lines, e.g. [21]). We look for statements, which indicate (systematic) configurability that lies beyond programmability via APIs, release of new services or the installation/exchange of software on devices.

**T15. Ecosystem support**

Platforms can support activities to form an ecosystem. Often, extensions and services emerge around the platform, i.e., due to extension mechanisms such as in T13. Here, however, we specifically target interaction between platforms, integration of third-party solutions, or common reference architectures.

a) **"Multi-Sided" platform allowing to form ecosystems (e.g., networks with other platforms)**

Can the platform, or the IIoT/IoT systems implemented in the platform, be networked with other platforms or systems in other platforms?

b) **Open to third-party content** (e.g. software extensions, etc.)
Can third-party software solutions, services or data be used within the platform or in the IIoT/IoT systems implemented in it?

c) **Reference to the RAMI 4.0 architecture**
Is there a link to the Reference Architectural Model Industrie 4.0 (RAMI 4.0) [22] in the platform or in the documentation for the platform?

**T16. Other technical abilities**

Does the platform offer additional or special technical capabilities or features not covered by the topics mentioned so far, such as virtual reality support?

**T17. References**

Information on the sources used, as well as a list of the sources themselves.

In summary, our analytics themes thus also cover the "indispensable functions" (e.g., [12]) that an IIoT architecture should support: Industrial connectivity (T3 but also T10), ease of app creation (T13 and T14), management and orchestration (T5, T14, and T16 for dashboards), data analytics (T11, T12), and optimized (role-based) user experience (T16 for virtual reality and dashboards, respectively). However, we aim for a broader overview and, as mentioned earlier, follow IIP-Ecosphere's perspective on industrial production, which leads to a different weighting and cut of the analytics topics.

## 2.2 Plattform Selection

The goal of this work is to identify the characteristics of a representative set of IIoT/Industry 4.0 platforms for IIP-Ecosphere. A complete analysis of all providers is not feasible due to the size and dynamics of the market [7]. The platforms to be analyzed were thereby determined by two significant sources:

1. The **stakeholder analysis** from the competitive phase, which, among other aspects, also identified platform candidates for a more detailed analysis and prioritized them. The prioritization was based on revenue and profit figures as well as relevance to the Industry 4.0 approach and the planned ecosystem based on the assessment and experience of IIP-Ecosphere's core partners. Within this framework, the following platforms (sorted by name) were identified as relevant[9]:
    - Amazon - AWS IoT
    - Bosch – Bosch IoT Suite
    - Cisco - Kinetic
    - IBM - Watson IoT Suite
    - Microsoft - Azure IoT Suite
    - Oracle – Oracle Cloud IoT
    - PTC - ThingWorx
    - SAP - Leonardo
    - Siemens - MindSphere
2. The **discussions of the IIP-Ecosphere partners** being particularly interested in the platform and its architecture. These are the working group Software Systems Engineering of the University of Hildesheim, the Institute for Software Technology of the University of Koblenz-Landau, Siemens (Erlangen), the Lenze Group, Bitmotec GmbH, KIProtect GmbH, and Phoenix Contact Deutschland GmbH. Here, the following additional platforms (also sorted by name) were named as candidates[9]:
    - Adamos - Adamos
    - BMW/Microsoft - Open Manufacturing Platform
    - B&R - Automation mapp Technology
    - Deviceinsight - Centersight
    - Endress und Hauser - Netilion
    - Emerson - Plantweb
    - General Electrics - Predix
    - Google – Google Cloud IoT Core
    - Harting - Mica
    - Manubrain Konsortium - Manubrain
    - Recogizer Analytics - Recogizer Analytics IoT Platform
    - Software AG - Cumolocity
    - S&T - SusieTech
    - Weidmüller - Industrial Analytics

A total of 23 candidates were thus identified for this analysis.

## 2.3 Collection of Raw Data

In this step, we examine the platform candidates from Section 2.2 to collect answers for the topics or questions from Section 2.1. We rely on materials that the respective platform vendors make available

[9] No URLs or references per platform are given here, as these are listed in Chapter 3 in the form of T17.

on their own websites. This can be information on the websites, but also advertising documents and flyers or technical documentation. We explicitly limit ourselves to the **information provided by the respective vendors** and do not take into account existing analyses, so that we base this overview on information that is as up-to-date as possible and not influenced by opinions (other than those of the vendor).

To store the information systematically, we derived a question/answer template from the topics in Section 2.1. We instantiated and filled this template for each platform examined based on the information provided by the vendor. First, the web site of the vendor or platform is identified and the linked web pages and documents are processed in terms of a deep traversal in the preset browser language (German, where not available English). In order not to overlook any obvious information, the results of a web search with Google Search for the respective platform are checked for vendor pages and these are included if not already recorded.

While collecting the raw information for all candidate platforms, we found that there was not enough information for both Manubrain[10] and the Open Manufacturing Platform[11] for a more detailed analysis, so the following chapters focus on the remaining 21 platforms.

We assigned the identified information to the analysis topics introduced in Section 2.1 and recorded the information in the respective results document either as quotations, textual summaries, bullet points or combinations thereof. Sources used in the process are also recorded in the results document (T17) in the form of URLs. Consulting services, such as those provided by chat functions on the vendor's pages, are not to be used, as we exclusively focus on vendor documents as sources, as described above.

The raw data collection took place in two phases. In the first phase, we processed initially all topics with a focus on software and platform engineering or AI support. In the second phase, we focused in particular on security and data protection and supplemented the results documents created in the first phase. Data collection for both phases took place in the period from June 2020 to August 2020. Web pages used as well as downloaded files such as PDF documents were saved - unless this was excluded by vendor statements/measures - and made available to all authors so that, as far as possible, we had the same view on the material for the respective platform. All result documents were available to all authors at all times. The processing status per platform and phase was entered in a common status table to enable parallel processing of the information and to avoid access conflicts during the data collection. We also created an initial overview of the most important results per platform/analysis topic from section 2.1 in the status table to prepare a later classification during data analysis.

## 2.4 Analysis of the Collected Raw Data

For the analysis, we first integrated the raw data from the instantiated templates into this document and prepared the final presentation, e.g., by adjusting text sections in length or by adapting the formatting. Then, we categorized the information per platform (based on the analysis topics from Section 2.1 and the initial results table from Section 2.3).

We performed an open-minded, incremental categorization and allowed an adjustment of the categories during categorization based on the available data. Depending on the analysis topic, we split too large, non-uniform categories successively into smaller categories or merged too small categories with larger categories or even eliminated irrelevant categories if necessary. We performed the categorization in an Excel spreadsheet (with one worksheet per analysis topic) so that we were able to derive simple statistics and illustrations directly from the data.

[10] https://manubrain.de/
[11] https://www.press.bmwgroup.com/global/article/detail/T0294085EN/the-bmw-group-and-microsoft-launch-the-open-manufacturing-platform

Finally, we summarized the results of the categorization textually and illustrated the results graphically in terms of tables or figures.

# 3 Plattform details

In this chapter, we present the information that we identified in the materials of the individual vendors to answer the topics from Section 2.1. As expected, the level of detail in the materials varies, i.e., while some platforms provide very detailed information and technical documentation, other platform material sometimes contains very little information.

In the platform summaries, we use several acronyms and terms as used in the collected material. Some international/English terms, e.g., HAVC, do not have direct correspondences in German, the origin language of this white paper. Thus, it was relevant to explain them here and for links between the both versions of the white paper (English and German), we also present the full list here. Technical acronyms, especially specific communication protocols are not listed here. In the platform summaries, we may use the following terms:

- **Application Programming Interface** (**API**): technical programming interface.
- **Business Intelligence (BI):** A form of business analytics, including procedures and processes to systematically analyze your own business.
- A **blockchain** is an extensible list of records that are linked using cryptographic techniques.
- **Heating, ventilation and air conditioning (HVAC):** Domain of and technics for heating, ventilation and air conditioning.
- **Human Machine Interface** (**HMI**): Technical interface between a human and the machine, e.g., a screen.
- **Identity and Access Management (IAM):** Technical measures to manage identities and to allow for access management.
- **Internet Protocol (IP):** Fundamental communication protocol of the Internet, together with the Transmission Control Protocol (TCP) part of the so-called TCP/IP stack.
- **Key Performance Indicators (KPI):** Predefined or freely definable performance indicators.
- **Platform-as-a-service** (**PaaS**): Cloud environment that provides a platform for the development of applications on the Internet.
- **On-premise**: On-site installation of software components on customer's hardware.
- **Software Development Kit** (**SDK**): Collection of program libraries and programming tools for software development.
- **Software-as-a-service** (**SaaS**): Cloud environment that provides individual, possibly customer-specific services on a predefined platform.
- **3rd party:** Devices or (software) components that can be obtained from a third-party vendor.
- **Machine Learning (ML):** Machine learning, a form of Artificial Intelligence (AI).
- **No code:** Programming approach where developers and other professionals can create application software without programming, usually via graphical user interfaces or configurations.
- **Over-the-air (OTA) update**: Network-based (WLAN) update, especially for software and firmware of machines and edge devices. Special form **Firmware-over-the-Air (FOTA)**.
- **Plug-and-Play (P&P):** Use of technical interfaces using protocols that automatically configure the software or devices involved in a conflict-free way that enables ease of use.
- **Representational State Transfer (REST):** Programming paradigm for distributed systems, especially for web services as an abstraction of the structure and behavior of the World Wide Web.
- **Role-based access control (RBAC):** Security/access model based on roles.
- **Service Level Agreement (SLA):** Formal or informal agreements for the quality of service.
- **Transport Layer Security (TLS):** Encryption protocol for secure data transmission, successor to Secure Sockets Layer (SSL).

- **User Interface (UI):** Means to allow users to interact with software, often in forms of a **Graphical User Interface (GUI)**.
- **Virtual Machine (VM)**: Software-technical encapsulation of a system within an executable computer system. **Containers** offer another type of encapsulation with access to the underlying host operating system, e.g., even for individual services up to so-called **microservices**.
- **Virtual Private Network (VPN)**: A virtual (self-contained) communications network that can be established over existing Internet connections to provide transparent, encrypted remote access into corporate networks.
- **What you see is what you get (WYSIWYG):** Real-time representation of information in the form in which it can be extracted via another device, e.g. a printer.

A subsection now follows for each platform, structured according to the topics from Section 2.1. As stated above, the order of the sub-sections follows the aforementioned sequence of platform vendors or analysis topics. Quotations in the platform sections are taken from the respective sources. English quotations have been recorded at the same time the corresponding German quotations have been selected for the original white paper. However, for other analysis topics than for the overview (T1), we give also German quotations and provide an explaining text in English.

## 3.1 Adamos – Adamos

| T1. Overview | | |
|---|---|---|
| a) | **Name of the platform** | Adamos (ADAptive Manufacturing Open Solutions) |
| b) | **Platform vendor or provider** | Adamos GmbH, Darmstadt, Germany |
| c) | **Vendor summary** | *„In mechanical and plant engineering, digital solutions are becoming more important than ever for sustainable business success. ADAMOS offers with its network and technologies future-proof solutions for the development of digital products and IIoT applications. This makes the enormous potential of digitalization for companies tangible. “* |
| d) | **Platform components** | • Adamos Hub (Cross-vendor access to applications, from 2020)<br>• Adamos IoT Platform |
| e) | **Online marketplace platform** | Adamos Hub (from 2020) |
| f) | **Mobility platform** | *No information available* |
| g) | **B2B context** | Yes |
| h) | **B2C context** | *No information available* |
| i) | **Platform users** | Machine operator, plant operator |
| j) | **Fields of application** | Mechanical engineering, acquisition of machine data, remote maintenance, quality control, condition monitoring, fault response maintenance management, actual/target comparison |
| k) | **Market penetration** | incl. DMG Mori, Dürr, Zeiss, Karl Mayer, ASM, Engel, Mahr, oerlikon, illig, weber, mayer & cie, schlenker, wittenstein, knitlink, digital workpiece, DXQequipment, Ecopure, Smart Equipment Monitoring |

| T2. License information | | |
|---|---|---|
| | | • Entry package (50 assets, 60 million data transfers, 100G storage)<br>• Platform-as-a-Service (PaaS) services based on a pay-per-use model |

| T3. Protocols | | |
|---|---|---|
| | | Plug & play, 100 gateway solutions from different vendors with out-of-the-box support of over 300 different machine protocols, e.g., OPC-UA, Canbus, Modbus, LPWAN protocols (LoRa, SIGFOX), REST, MQTT |

| T4. Edge support | | |
|---|---|---|
| | | *No information available* |

| T5. IIoT devices | | |
|---|---|---|
| a) | **Device connectivity** | See protocols (T4), no specific information identified. |
| b) | **Device management** | • Structuring in taxonomies, manual/automatic assignment<br>• Remote shell with terminal to the devices<br>• Remote access to operating units of machines with HMI |
| c) | **Deployment, provision of software** | Platform is a SaaS. Deployment for devices is not mentioned separately, but may be possible via integrated cloud IoT services. |

| T6. Security | |
|---|---|
| | • Authentication (e.g. Basic, SAML2 token, WSS username token, WSS X.509 token, OAuth2 token), signatures and encryption.<br>• API-Gateway: DoS protection, data volume, SQL-Injection, ICAP<br>• VNC, HTTPS tunneling, Single-Sign-On<br>• User management, authentication (optional 2-factor)<br>• Role-based access model<br>• Audit log<br>• Multi-tenancy |

| T7. Data protection | |
|---|---|
| | **Smart Rules:** The platform offers predefined Smart Rule templates that can be configured via the browser, making them ideal for users without technical knowledge. Smart Rules allow alarms to be triggered when, for example, a sensor value exceeds a defined threshold or a GPS signal moves into, out of, or stays within a geographically defined area ("geofence") for a specified period of time. Furthermore, Smart Rules can be used to monitor whether an event does not occur in the expected time (non-event), etc. Once created, Smart Rules can be easily activated and deactivated by business users as needed. |
| | **Data retention rules:** The data retention rules of the ADAMOS Core module allow the retention times of data to be individually controlled and thus influence storage costs incurred, especially in the cloud environment. Rule configurations can be used to define in great detail which data is to be retained and for how long. |
| | **Data Brokerage:** ADAMOS Core has a Data Broker that enables configuration-based forwarding and subscription of data between two or more ADAMOS clients. This feature is particularly useful in distributed deployment scenarios. For example, it can be used to control the exchange of data between end customers (machine users) and machine manufacturers. Depending on the criticality of the data, the end customer can selectively decide what kind and how much of the machine data should be forwarded to the manufacturer. |
| | **Role-based access model:** Control over who may access or process personal data (Article 5). |

| T8. Cloud support | |
|---|---|
| | • Optional PaaS, based on e.g. Microsoft Azure<br>• SaaS integration (Integration Cloud Module)<br>• Optional on-premise integration<br>• Cloud Connector Framework (for 30 cloud vendors)<br>• Multi tenancy, hierarchical client organization possible |

| T9. Scalability | |
|---|---|
| | The platform supports scalability and high availability. |

| T10. Digital twins / Asset Administration Shells | | |
|---|---|---|
| a) | **Digital twins** | Device simulations for virtual machines and devices. |
| b) | **AAS approach used for IoT devices** | *No information available* |
| c) | **AAS approach used for edge devices** | *No information available* |

| T11. Data management and data analysis | |
|---|---|
| | • Real-time data analysis using streaming analytics with a focus on condition monitoring and predictive maintenance. The hypertree technology used allows high throughput with low latency.<br>• Event Processing Language (EPL), different processing models (time-based or location-based analysis windows), key figure calculation, event references, anomaly detections, model enrichment.<br>• The data model used is flexible and customizable. There is a predefined domain model that is customizable for the particular use.<br>• The data model can be represented in different ways, e.g., as XML file, XML Schema, DTD file, JSON file, Adobe Lifecycle Template, Microsoft Infopath form or SAP IDOC.<br>• The platform allows to define data retention rules. |

| T12. Offered AI methods | |
|---|---|
| | • Rule-based techniques, so-called Smart Rules, allow users to define evaluations without technical knowledge, especially to trigger alarms.<br>• The Analytics Builder is based on the EPL mentioned above.<br>• Advanced Streaming Analytics enables machine learning on data streams using the PMML[12] standards. |

| T13. Openness and Extensibility | | |
|---|---|---|
| a) | **Store** | • Adamos Store (from 2020) with apps from machine, plant, component manufacturers and third-party providers<br>• API self-service portal |
| b) | **App support for/by developers** | • Can be integrated via microservices/containers<br>• Dashboarding via visual editor, web SDK |
| c) | **Use of "external" algorithms/data** | Via the integrated languages, builders or APIs |
| d) | **AI interfaces** | see https://adamos.com/developer-center |

| T14. Systematic Configurability | |
|---|---|
| | • Definition of functions for security checking of API calls<br>• Definition of functions through graphical modeling<br>• Definition of dashboards |

| T15. Ecosystem support | | |
|---|---|---|
| a) | **"Multi-Sided" platform** | SaaS integration or on-premise integration through application adapters (for 40 different applications) |
| b) | **Open to third-party content** | Main objective of the platform: open and vendor-neutral |
| c) | **Reference to RAMI 4.0** | *No information available* |

| T16. Other technical abilities | |
|---|---|
| | • Container integration with Kubernetes and Docker[13], container isolation during execution<br>• Microservice support through registry and microservice API/SDKs for Java and C#<br>• Advanced API features such as API management (REST, SOAP, Swagger, RAML), API policies for access, forwarding and restrictions (quotas), and tools for API analytics |

[12] https://en.wikipedia.org/wiki/Predictive_Model_Markup_Language
[13] https://www.docker.com/

| T16. Other technical abilities |
| --- |
| • For on-premise installations, Docker containers uploaded to the repository can be reused.<br>• Multi-stage application lifecycle consisting of development, test, production<br>• Graphical specification or development of integrations (in addition to direct programming) |

| T17. References |
| --- |
| • Adamos Flyer from https://adamos.com<br>• Further materials from https://adamos.com |

## 3.2 Amazon - AWS IoT

| T1. Overview | | |
|---|---|---|
| a) | **Name of the platform** | AWS IoT |
| b) | **Platform vendor or provider** | Amazon Web Services, Inc., USA |
| c) | **Vendor summary** | *„AWS has broad and deep IoT services, from the edge to the cloud. AWS IoT is the only cloud vendor to bring together data management and rich analytics in easy to use services designed for noisy IoT data.*<br>*AWS IoT offers services for all layers of security, including preventive security mechanisms, like encryption and access control to device data, and a service to continuously monitor and audit configurations.*<br>*AWS brings AI and IoT together to make devices more intelligent. You can create models in the cloud and deploy them to devices where they run 2x faster compared to other offerings.*<br>*AWS IoT is built on a secure and proven cloud infrastructure, and scales to billions of devices and trillions of messages. AWS IoT integrates with other AWS services, so you can build complete solutions. “* |
| d) | **Platform components** | • AWS IoT Core<br>• AWS IoT Greengrass<br>• AWS IoT Defender<br>• AWS IoT Device Management<br>• AWS IoT Analytics<br>• AWS IoT SiteWise<br>• AWS IoT Events<br>• AWS IoT ThingsGraph<br>• FreeRTOS (Open-Source real-time operating system for micro controllers) |
| e) | **Online marketplace platform** | AWS Marketplace: Online marketplace in which third-party software solutions, algorithms and models are offered. |
| f) | **Mobility platform** | Yes |
| g) | **B2B context** | Yes, no direct focus on end customers |
| h) | **B2C context** | *No information available* |
| i) | **Platform users** | IoT platforms and industry applications for enterprises |
| j) | **Fields of application** | • Administration environment for managing and monitoring sensor data generated by technical objects from the Internet of Things<br>• Development, customization and operation of cloud-based IoT business applications<br>• Focus on the application of AI techniques in IoT systems |
| k) | **Market penetration** | • Global application by a wide range of users<br>• Widespread application by major customers |

| T2. License information | |
|---|---|
| | • Commercial software package / license for all AWS offerings<br>• FreeRTOS (Open Source Operating System for Microcontrollers): Open Source MIT License<br>• Licenses of customer's own developments/applications are not mentioned. |

| T3. Protocols | | |
|---|---|---|
| | | Realized via the dedicated AWS IoT Greengrass Connectors component: AWS IoT Greengrass Connectors can be used to identify and import applications and services at the edge. Devices can be configured and provisioned without requiring a user to understand various device protocols, manage credentials, or interact with external APIs. |

| T4. Edge support | | |
|---|---|---|
| a) | **Overview** | AWS IoT Greengrass implements working with edge devices in AWS IoT. AWS Greengrass enables Docker container-based execution of applications on edge devices. Note: AWS IoT Greengrass is almost entirely based on Python 2.7/3.7. |
| b) | **Communication** | AWS IoT Greengrass enables messaging between AWS IoT Greengrass Core and devices running the AWS IoT Greengrass SDK on a local network, facilitating communication even when not connected to AWS. With AWS IoT Greengrass, devices can process messages and send them to another device or to the cloud based on specified business rules. |
| c) | **Memory usage** | AWS Lambda functions deployed on AWS IoT Greengrass Core can access local resources of the respective device. This allows serial ports, peripherals such as additional security devices, sensors and actuators, onboard GPUs, or the local file system to be used to access and process local data.<br>Applications to run on edge devices will run in Docker containers. Docker images can be stored in Docker container registries, such as Amazon Elastic Container Registry (Amazon ECR), Docker Hub, or private Docker Trusted Registries (DTRs). In addition to running on-premises applications on Edge devices, Edge devices can also access any web services available on AWS cloud. |
| d) | **Specific capabilities** | • Also included in AWS IoT Greengrass is the AWS IoT Device Shadow feature. The device shadow acts like a cache of your device's state, representing a virtual version or "shadow" (digital twin) of each device that can be used to track the current state of each device, as well as its desired future state, and synchronize each with the cloud when connectivity is available.<br>• Use of visualized AWS IoT Things Graphs, a model-based representation of IoT devices or device federations.<br>• AWS IoT Things Graph applications can run in the AWS Cloud or on the edge, for example, on AWS IoT Greengrass-enabled devices. This allows devices to respond quickly to local events, even when there is no Internet connection. AWS IoT Greengrass is software that can securely perform local data processing, messaging, caching, synchronization, and machine learning inference operations. Deployment is simple and can be launched with a few clicks in the AWS IoT Things Graph console. AWS IoT Things Graph packages customer-owned models with the runtime, pushes them to the customer-owned IoT Greengrass device, and begins message monitoring and coordination of interactions there. |

| T5. IIoT devices | | |
|---|---|---|
| a) | **Device connectivity** | See protocols (T3): Implemented via the AWS IoT Greengrass component. |
| b) | **Device management** | • Edge computing functionalities via dedicated edge computing component AWS IoT Greengrass, which extends AWS to edge devices so they can act on the data generated there locally, while still using the cloud for management, analytics and persistent storage, even when there is no network connection (device shadow).<br>• Continuous device monitoring, support for the entire IoT lifecycle.<br>• Enrollment, organization, monitoring, and remote management of connected IoT devices using the dedicated AWS IoT Device Management component: "AWS IoT Device Management facilitates secure enrollment, organization, monitoring, and remote management of connected IoT devices."<br>• Over-the-air updates (OTA)<br>• Alexa Voice Service (AVS) integration for AWS IoT Core enables sending audio messages to and from connected devices. |
| c) | **Deployment, provision of software** | **Software Deployment:**<br>• REST<br>• Software-as-a-Service (SaaS)<br>• Wide range of Amazon Web Services that can be used platform-wide<br>• Offering apps for administrative tasks<br>• Deployment of FreeRTOS (open source real-time operating system for microcontrollers)<br>• AWS IoT Greengrass provides the ability to upgrade the AWS IoT Greengrass Core software on AWS IoT Greengrass devices. The AWS IoT Greengrass console, API, or command line interface can be used to update the running version of AWS IoT Greengrass Core to provide security updates, bug fixes, and new AWS IoT Greengrass features.<br>**Deploying (AI) components on Industry 4.0 devices:**<br>• AWS IoT puts an emphasis on deploying AI techniques within the platform.<br>• Deployment of custom decision logics and rules for event detection and event handling is possible. |

| T6. Security | | |
|---|---|---|
| | | **Security techniques within the platform:**<br>• AWS IoT Core provides automated configuration and authentication when a device first connects to AWS IoT Core, as well as full encryption at all connection points so that data is not shared between devices and AWS IoT without a verified identity.<br>• Secure data storage and software (encryption, authorization)<br>• AWS IoT Device Defender makes it easy to manage and enforce IoT configurations, such as securing device identity, authenticating and authorizing devices, and encrypting device data.<br>• Container-based execution of applications<br>• AWS IoT Device Defender scans and monitors devices and sends alerts when their behavior deviates from what has been defined as normal behavior for each device.<br>• Special protection against DDOS attacks through automatic scaling of resources |

| T6. Security | |
|---|---|
| | **User and user rights management:** Extensive options for user and user rights management |
| | **Edge device security:** Dedicated component to secure IoT devices: AWS IoT Defender |
| | **Security management on edge devices:** AWS IoT Greengrass Secrets Manager enables secure storage, access, rotation, and management of security settings - credentials, keys, endpoints, and configurations - at the edge. |

| T7. Data protection | |
|---|---|
| | **Technical-organizational measures:**<br>• Use of multi-factor authentication (MFA)<br>• Use of SSL / TLS to communicate with AWS resources<br>• Setting up API and user activity logging with AWS CloudTrail<br>• Use of AWS encryption solution along with all standard security controls in AWS services<br>• Role-based access management |
| | **Auditing and control:** Use of advanced managed security services, such as Amazon Macie, to discover and secure personal data. |

| T8. Cloud support | |
|---|---|
| | • AWS IoT is Amazon cloud-based. This enables the use of all services available in the AWS Cloud.<br>• Cloud usage can be scaled (via the Amazon Cloud).<br>• IoT devices can be persistently represented in the AWS Cloud via AWS IoT Device Shadows. |

| T9. Scalability | |
|---|---|
| | • The platform can be scaled according to the needs of the customer (data volume, number of devices, etc.).<br>• IoT devices or edge devices can be added or removed at any time, as the entire lifecycle is covered by AWS IoT.<br>• Use of cloud computing capacity only when it is actually needed, controlled via AWS Lambda component. |

| T10. Digital twins / Asset Administration Shells | | |
|---|---|---|
| a) | **Digital twins** | Digital twins are not explicitly mentioned, but AWS offers the ability of creating "AWS IoT Device Shadows": *"The AWS IoT Device Shadow service adds shadows to AWS IoT thing objects. Shadows can make a device's state available to apps and other services whether the device is connected to AWS IoT or not. AWS IoT thing objects can have multiple named shadows so that an IoT solution has more options for connecting devices to other apps and services. "* |
| b) | **AAS approach used for IoT devices** | AWS "Things" are similar in approach to the AAS concept: AWS IoT Things Graph simplifies collaboration between devices and web services by representing these "things" as models. A model is an abstraction that represents a device as a set of actions (inputs), events (outputs), and states (attributes). Models separate the device interface from its underlying implementation. For example, a switch can be represented as a set of attributes (state, dimmable), events (end of daylight saving time), and actions (turn on). |
| c) | **AAS approach used for edge devices** | See T10b. |

| T11. Data management and data analysis | |
|---|---|
| | • Extensive capabilities to collect, monitor and analyze data is in near real-time, realized in a dedicated data analytics component AWS Analytics.<br>• Defining business rules, filtering, transforming data<br>• Visualization of data and data analysis<br>• Use of data for other AWS services: AWS Lambda, Amazon Kinesis, Amazon S3, Amazon DynamoDB, Amazon CloudWatch, and Amazon Elasticsearch Service.<br>• Local collection and processing of bulk data from a site through the AWS SiteWise component. |

| T12. Offered AI methods | |
|---|---|
| | • Comprehensive data analytics capabilities through AWS Analytics.<br>• Handling of complex events through AWS Events<br>• Creation of decision logics (to detect events and respond to them appropriately) by customers.<br>• Creation of (AI) models by customers and execution of these models in Docker containers on edge devices. |

| T13. Openness and Extensibility | | |
|---|---|---|
| a) | **Store** | The platform offers the AWS Marketplace, an online marketplace where third-party software solutions, algorithms and models are offered.<br>The categories in which software solutions, algorithms and models are offered in the Sore are: Operating Systems, Security, Networking, Storage, Data Analytics, Dev Ops, IoT Solutions, Machine Learning, and Data Products. Furthermore, special IoT Solutions as well as special Machine Learning Solutions are offered in the AWS Marketplace. |
| b) | **App support for/by developers** | • Freely accessible extensive documentation and tutorials on APIs, SDKs for almost all services are offered.<br>• Provision and support of GitHub repositories for developers<br>• Provision of the open source operating system FreeRTOS for microcontrollers<br>• Provision of MQTT library for FreeRTOS<br>• Support for IoT application development via the AWS IoT Things Graph: AWS IoT Things Graph accelerates IoT application development by eliminating the need to deal with basic device details and write code that aligns devices and web services. |
| c) | **Use of "external" algorithms/data** | • Unrestricted integration of customer's own applications and AI models is given by the use of Docker Containers for own applications.<br>• Third-party content can be offered via the AWS Marketplace. |
| d) | **AI interfaces** | • Customers can run their own custom analytics in a Docker container in AWS IoT Analytics.<br>• AWS IoT Analytics automates the execution of custom analytics created in Jupyter Notebook or customer-owned tools (such as Matlab, Octave, etc.).<br>• Creation and storage of custom AI models in the AWS cloud is possible.<br>• Leverage Amazon SageMaker: Use Amazon SageMaker Neo deep learning compiler to optimize custom models in |

| T13. Openness and Extensibility | | |
|---|---|---|
| | | Tensorflow, Apache MXNet, PyTorch, ONNX, or XGBoostframeworks. |

| T14. Systematic Configurability | |
|---|---|
| | • Customers can customize the applications they deploy.<br>• Graphical integration development in the AWS Things Graph<br>• Extensive customization capabilities with the ability to define custom business rules, event handlings, schedules for data transfers, etc. |

| T15. Ecosystem support | | |
|---|---|---|
| a) | **"Multi-Sided" platform** | Ecosystem building opportunities exist, but the focus is on building ecosystems within the Amazon platform(s).<br>The AWS Partner Network (APN) is the global partner program for technology and consulting companies that use Amazon Web Services to build solutions and services for customers. The APN helps companies build, market, and sell their AWS offerings by providing valuable business, technical, and marketing support. |
| b) | **Open to third-party content** | There is a great freedom of development within the platform(s) and software provided by AWS IoT. However, there is a focus on keeping new software development and adaptation primarily within the AWS IoT platform and its components. Third-party content can be offered through the AWS Marketplace. |
| c) | **Reference to RAMI 4.0** | *No information available* |

| T16. Other technical abilities | |
|---|---|
| | • Distinct developer network: GitHubs to various APIs and SDKs for developers<br>• Kubernetes, Jupyter Notebooks, Mathlab, Octave, Docker, container isolation<br>• Microservice API/SDKs<br>• API Management (REST)<br>• FreeRTOS: open-source real-time operating system for microcontrollers<br>• MQTT Library for FreeRTOS<br>• Integration on-premise: reuse functionality packaged in Docker images and uploaded to repositories, supported by: Amazon Elastic Container Registry (Amazon ECR), Docker Hub or private Docker Trusted Registries (DTRs).<br>• Coverage of the complete IoT lifecycle<br>• Graphical integration development (also direct programming) in the AWS Things Graph<br>• AWS IoT Device Shadow service: persistent representation of IoT devices in the AWS cloud<br>• Use of voice services (Alexa) for IoT devices: Alexa Voice Service (AVS) Integration for AWS IoT |

| T17. References | |
|---|---|
| | • Extensive information available on the AWS IoT web pages and the web pages for each AWS component/service. Technical documentation available as PDFs for, among others: AWS IoT Greengrass, AWS IoT Device Shadow, AWS IoT Analytics.<br>• AWS IoT overview:<br>  ○ https://aws.amazon.com/de/iot/<br>  ○ https://aws.amazon.com/de/iot-core/<br>• AWS marketplace |

**T17. References**

https://aws.amazon.com/marketplace/

- GitHub repository for AWS IoT:
  https://github.com/awsdocs/aws-iot-docs/tree/master/developerguide
- AWS IoT in the context of IIoT:
  https://aws.amazon.com/de/iot/solutions/industrial-iot/
- AWS IoT Analytics:
  - https://aws.amazon.com/de/iot-analytics/
  - https://docs.aws.amazon.com/iotanalytics/index.html
  - https://docs.aws.amazon.com/iotanalytics/latest/userguide/iotanalytics-ug.pdf
- AWS IoT Things Graph:
  - https://aws.amazon.com/de/iot-things-graph/
  - https://aws.amazon.com/de/iot-things-graph/features/
- AWS IoT Device Shadows:
  https://docs.aws.amazon.com/iot/latest/developerguide/iot-device-shadows.html
- AWS Greengrass (for edge devices):
  - https://aws.amazon.com/de/greengrass/
  - https://docs.aws.amazon.com/greengrass/index.html#lang/en_us
  - https://docs.aws.amazon.com/greengrass/latest/developerguide/gg-dg.pdf
- AWS Lambda:
  https://aws.amazon.com/lambda/
- AWS IoT Device Management:
  - https://aws.amazon.com/de/iot-device-management/
  - https://docs.aws.amazon.com/iot-device-management/index.html
  - https://docs.aws.amazon.com/iot/latest/developerguide/iot-dg.pdf
- AWS IoT Defender:
  - https://aws.amazon.com/de/iot-device-defender/
  - https://docs.aws.amazon.com/iot/latest/developerguide/device-defender.html
  - https://docs.aws.amazon.com/iot/latest/developerguide/avs-integration-aws-iot.html
- AWS IoT Events und AWS IoT Sitewise:
  - https://aws.amazon.com/de/iot-events/
  - https://aws.amazon.com/de/iot-sitewise/
- FreeRTOS: Open-Source real-time operating system for micro controllers:
  - https://aws.amazon.com/de/freertos/
  - https://docs.aws.amazon.com/freertos/latest/userguide/freertos-getting-started.html
  - https://docs.aws.amazon.com/freertos/latest/userguide/freertos-lib-cloud-mqtt.html
- AWS partner network and AWS marketplace:
  - https://aws.amazon.com/de/partners/
  - https://aws.amazon.com/marketplace/
  - https://aws.amazon.com/marketplace/solutions/IoT
  - https://aws.amazon.com/marketplace/solutions/machine-learning

## 3.3 Bosch – Bosch IoT Suite

| T1. Overview | | |
|---|---|---|
| a) | **Name of the platform** | Bosch IoT Suite |
| b) | **Platform vendor or provider** | Bosch.IO GmbH, Berlin, Germany |
| c) | **Vendor summary** | *"The Bosch IoT Suite is a flexible IoT platform that comprises an array of cloud-enabled services and software packages and addresses the typical requirements of IoT projects. Companies can easily start with a proof of concept (PoC), enter the market quickly with a minimum viable product (MVP), and operate their digital offerings in a scalable and secure manner."* |
| d) | **Platform components** | • Bosch IoT Hub<br>• Bosch IoT Insights<br>• Bosch IoT Analytics<br>• Bosch IoT Things<br>• Bosch IoT Manager<br>• Bosch IoT Remote Manager<br>• Bosch IoT Rollouts<br>• Bosch IoT Gateway Software |
| e) | **Online marketplace platform** | Yes, applications in the retail sector are explicitly mentioned. |
| f) | **Mobility platform** | Yes, applications in the automotive sector are explicitly mentioned. |
| g) | **B2B context** | Yes, focus on industrial customers or large-scale customers such as service providers. |
| h) | **B2C context** | *No information available* |
| i) | **Platform users** | IoT platforms and industry applications for enterprises |
| j) | **Fields of application** | • Administration environment for managing and monitoring sensor data generated by technical objects from the Internet of Things.<br>• Customization and operation of cloud-based IoT business applications.<br>• Offering solutions for the following sectors (among others): retail, manufacturing, automotive, agribusiness, smart home, smart city. |
| k) | **Market penetration** | • Global application through a wide range of users<br>• Widespread application by major customers |

| T2. License information | |
|---|---|
| | Proprietary licenses of the vendor (Bosch) with complex licensing situation, due to the integration of a wide variety of open source components (e.g. Apache Tomcat, Eclipse Ditto, etc.) as well as third-party services (e.g. AWS IoT). |

| T3. Protocols | |
|---|---|
| | • MQTT, TR-069, OMA-DM, OMA LwM2M, REST/http<br>• Additional protocols are supported by the Bosch IoT Gateway component. |

| T4. Edge support | | |
|---|---|---|
| a) | **Overview** | The Bosch IoT Suite offers very good support for edge devices. In particular, the management and communication with edge devices is very flexible and efficient due to dedicated components and a specialized middleware.<br>Description of the middleware Bosch IoT Gateway Software by the supplier: *"Bosch IoT Gateway Software is a platform-independent edge computing middleware deployed on more than 40 types of gateway devices. It runs on common operating systems such as Linux, Windows, MacOS, and VxWorks. Bosch IoT Gateway Software is based on Java and OSGi building a modular framework with possibility to dynamically install and update new software.*<br>*Edge and cloud computing are complementary approaches for solving some of the most challenging use cases in IoT. The Bosch IoT Gateway Software is included in several pre-configured packages part of the Bosch IoT Suite to give you flexibility with building custom edge-to-cloud solutions.*<br>• *The Bosch IoT Suite for Asset Communication combines the device connectivity and device data processing capabilities of Bosch IoT Gateway Software with cloud services such as Bosch IoT Hub, and Bosch IoT Things, to provide a complete telemetry, command & control solution.*<br>• *The Bosch IoT Suite for Software Updates combines Bosch IoT Gateway Software with Bosch IoT Remote Manager and Bosch IoT Rollouts for scenarios involving edge management and software updates.*<br>• *Other Services such as Bosch IoT Insights and Bosch IoT Analytics provide additional data management and analytics capabilities in the cloud."*<br>Description of the Bosch IoT Remote Manager component by the vendor: *"The Bosch IoT Remote Manager provides you with a proven and feature-rich solution to address device management throughout the device life cycle. It supports multiple device management protocols out-of-the-box and various classes of gateways and devices. The Bosch IoT Remote Manager can be used as a fully managed cloud service in different cloud environments or deployed on-premise.*<br>*Bosch IoT Remote Manager can also act as an IoT application platform – by providing a rich set of services and APIs for the realization of custom IoT applications. Some of the basic services provided for this purpose include:*<br>• *Device data collection*<br>• *Real-time readings*<br>• *Historical data*<br>• *Remote device control*<br>• *Remote network access to devices"* |
| b) | **Communication** | • The Bosch IoT Remote Manager component implements connectivity and communication with edge devices as follows:<br>○ Extensible: Open to the implementation of additional management protocols, business logic extensions, and user interfaces.<br>○ Remote access from applications and application servers to gateways and devices. |

| T4. Edge support | | |
|---|---|---|
| | | ○ Easy integration: Integrates with existing management systems through a comprehensive set of APIs: Java, OSGi, Webservices (REST).<br>• Bi-directional communication with edge devices possible: *"IoT applications are able to retrieve telemetry data from devices either with or without guaranteed delivery (device-to-cloud communication) and send command & control messages to devices (cloud-to-device communication)."* |
| c) | **Memory usage** | Edge-based data collection, pre-processing and analysis on edge devices, and forwarding from edge storage for further processing by platform services. |
| d) | **Specific capabilities** | • Diverse/rich connectivity<br>• Bosch IoT Remote Manager enables very complex software management on edge devices (version monitoring, bulk updates, SOTA, etc.) |

| T5. IIoT devices | | |
|---|---|---|
| a) | **Device connectivity** | • Wide range of all common protocol options for device and enterprise applications<br>• Possibility to integrate 3rd party devices<br>• Integration of a wide range of protocols and systems via Bosch IoT Gateway |
| b) | **Device management** | • Secure on- and offboarding of devices of various types<br>• Device and gateway lifecycle management<br>• Remote configuration of devices<br>• Remote update of device software (SOTA) realized by "Bosch IoT Rollouts"<br>• Diagnostics and troubleshooting of devices<br>• Backup and restore of device configurations<br>• Full life cycle support of IoT devices |
| c) | **Deployment, provision of software** | • Deployment via REST<br>• Software-as-a-Service (SaaS)<br>• Broad offering of platform-owned (internal) software<br>• Apps for administrative tasks are offered.<br>• Overall, however, a focus on Bosch (platform)-owned software<br>• Dedicated component for bulk updates "Bosch IoT rollouts" |

| T6. Security | | |
|---|---|---|
| | | **User and user rights management:** Extensive options for user and user rights management |
| | | **Security techniques within the platform:**<br>• Secure connection of assets to hardware or software connectivity solutions<br>• Secure data storage and software (encryption, authorization)<br>• Identity management and access control |
| | | **X.509 certificate-based device authentication** |
| | | **Supports TLS1.2** |

| T7. Data protection |
|---|
| • Bosch IoT Things<br>  ○ Find your things (accuracy, transparency)<br>  ○ Control access: policies to enable the authorization<br>• Bosch IoT-Rollouts<br>  ○ Device and software repository (transparency, accountability)<br>  ○ Software update and rollout management (control over data and processes)<br>  ○ Reporting and monitoring (accountability) |

| T8. Cloud support |
|---|
| • The platform is cloud-based and uses the cloud services of the Bosch IoT Cloud or third-party cloud storage (MS Azure, Huawei and others).<br>• The Bosch IoT suite offers an object store and Mongo DB.<br>• Data export in various formats (including JSON and CSV) is possible.<br>• Interfaces for third-party applications (Matlab, Excel, Tableau, etc.) are offered. |

| T9. Scalability |
|---|
| • The platform can be scaled according to the customer's needs (data volume, number of devices, etc.).<br>• Secure on- and off-boarding of devices at runtime support scalability.<br>• Bulk updates support scalability.<br>• Full lifecycle for IoT devices supports scalability. |

| T10. Digital twins / Asset Administration Shells | | |
|---|---|---|
| a) | **Digital twins** | Use of digital twins for simulation, development and testing of modifications or new developments. |
| b) | **AAS approach used for IoT devices** | The Bosch IoT Suite Digital Twins approach as a digital representation of "Things" is similar to the concept of the AAS. |
| c) | **AAS approach used for edge devices** | See T10b |

| T11. Data management and data analysis |
|---|
| • The collection, monitoring and analysis of data is possible in near real time.<br>• Visualization of data and data analysis<br>• Query of data via NoSQL / MongoDB is possible via the Bosch IoT Insights component.<br>• Bosch IoT Analytics uses open-source Python libraries such as Pandas and Scikit-learn. |

| T12. Offered AI methods |
|---|
| • Extensive AI techniques are available as part of the "Bosch IoT Analytics" offering.<br>• Anomaly detection in data<br>• Use of "smart algorithms" to automate routine data analysis tasks<br>• Extensive capabilities in the area of device data analysis (health monitoring, statistical analysis, etc.)<br>• Extensive data analysis capabilities, both on edge devices and in the cloud<br>• Complex, rule based, event handling |

| T13. Openness and Extensibility | | |
|---|---|---|
| a) | **Store** | Bosch IoT Suite offers its services via the (Amazon) AWS Store. Bosch IoT Suite does not maintain its own store. Software solutions or applications developed within Bosch IoT Suite by third parties are not offered. |
| b) | **App support for/by developers** | • Large parts of the Bosch IoT Suite are based on open source software and therefore per se support their further development through corresponding documentation, APIs, SDKs, etc.<br>• The Bosch IoT Suite platform itself supports app management and developers by providing extensive documentation, APIs, tutorials, etc. for its proprietary components.<br>• There is active support of the developer community via GitHub. |
| c) | **Use of "external" algorithms/data** | Since large parts of the Bosch IoT Suite are based on open source software, it can be assumed that the use of external data and algorithms in customer-specific applications is possible to the greatest possible extent. |
| d) | **AI interfaces** | Apart from the platform's own AI components, no information is provided on the integration of other (customer's own) AI components. |

| T14. Systematic Configurability | | |
|---|---|---|
| | | • Customers can create their own platform configurations.<br>• Customers can also use customized "packages" oriented to customers' scope of application. |

| T15. Ecosystem support | | |
|---|---|---|
| a) | **"Multi-Sided" platform** | • The Bosch IoT Suite platform allows integration of other platforms.<br>• The Bosch IoT Suite platform partly integrates components of other platforms into its own platform, so cloud services from AWS, Azure or Huawei, for example, can be used in the Bosch IoT Suite. |
| b) | **Open to third-party content** | • Allows the development of custom application configurations<br>• Provides a set of APIs for custom application development<br>• Custom software development capabilities are not explicitly mentioned. |
| c) | **Reference to RAMI 4.0** | *No information available* |

| T16. Other technical abilities | | |
|---|---|---|
| | | • Dedicated component for bulk updates: "Bosch IoT Rollouts"<br>• Broad range of versatile functionalities in software management on edge devices, realized by "Bosch IoT Remote Manager". |

**T17. References**

- Overview of Bosch IoT Suite:
  - https://www.bosch-iot-suite.com/
  - https://developer.bosch-iot-suite.com/documentation/
  - https://developer.bosch-iot-suite.com/service/insights/
  - https://developer.bosch-iot-suite.com/service/analytics/
  - https://developer.bosch-iot-suite.com/service/remote-manager/
  - https://docs.bosch-iot-suite.com/hub/
  - https://bosch-iot-insights.com/static-contents/docu/html/Introduction.html
  - https://docs.bosch-iot-suite.com/manager/en/Bosch-IoT-Manager.html
- Bosch IoT „edge“ components:
  - https://www.bosch-iot-suite.com/edge-computing/
  - http://documentation.bosch-si.com/iot/RM/v71/en/index.htm
  - http://documentation.bosch-si.com/iot/SDK/v10/en/index.htm
- Overview on IoT device connections and software management on IoT devices:
  - https://developer.bosch-iot-suite.com/iot-devices/
  - https://blog.bosch-si.com/bosch-iot-suite/software-updates-in-the-iot-an-introduction-to-sota/
  - https://developer.bosch-iot-suite.com/iot-devices/#protocols
  - https://docs.bosch-iot-suite.com/device-management/Bosch-IoT-Suite-for-Device-Management.html
  - https://docs.bosch-iot-suite.com/asset-communication/Bosch-IoT-Suite-for-Asset-Communication.html
- Bosch IoT Analytics:
  - https://docs.bosch-iot-suite.com/analytics/discover/index.html
  - https://developer.bosch-iot-suite.com/service/analytics/
- Bosch IoT Rollouts and Remote Manager:
  - https://docs.bosch-iot-suite.com/remote-manager/en71/index.htm#getting_started.htm
  - https://docs.bosch-iot-rollouts.com/documentation/index.html
- Bosch IoT „Things“ (Digital Twins):
  https://docs.bosch-iot-suite.com/things/
- License overview:
  http://documentation.bosch-si.com/iot/SDK/v10/en/index.htm#getting_started_licenses.htm
- Github repository:
  https://github.com/bosch-io

## 3.4 B&R - Automation mapp Technology

| T1. Overview | | |
|---|---|---|
| a) | **Name of the platform** | mapp Technology |
| b) | **Platform vendor or provider** | B&R Industrial Automation GmbH (member of ABB group), Eggelsberg, Austria |
| c) | **Vendor summary** | *„mapp Technology is revolutionizing the creation of software for industrial machinery and equipment. The mapp components – mapps for short – are as easy to use as a smartphone app. Rather than writing lines and lines of code to build a user management system, alarm system or motion control sequence from the ground up, developers of machine software simply configure the ready-made mapps with a few clicks of the mouse. Complex algorithms are easy to manage. Programmers can focus entirely on the machine process. “* |
| d) | **Platform components** | • mapp services<br>• mapp control<br>• mapp view<br>• mapp safety<br>• mapp motion<br>• mapp robotics<br>• mapp cnc |
| e) | **Online marketplace platform** | *No information available* |
| f) | **Mobility platform** | Supports mobile devices |
| g) | **B2B context** | Yes |
| h) | **B2C context** | *No information available* |
| i) | **Platform users** | Industry 4.0 users, especially business users without much IT knowledge (see programming languages) |
| j) | **Fields of application** | Especially hydraulics, cranes, plastic processing, extrusion or thermoforming. |
| k) | **Market penetration** | *No information available* |

| T2. License information | |
|---|---|
| | • Basic licenses (per component)<br>• Advanced licenses (per component) |

| T3. Protocols | |
|---|---|
| | • OPC-UA, OPC-UA over TSN, POWERLINK, FIELDBUS, PVI (Process Visualization Interface)<br>• Own protocols possible based on TCP/UDP, MQTT, AMQP |

| T4. Edge support | | |
|---|---|---|
| a) | **Overview** | „Open Architecture“ through use of edge devices |
| b) | **Communication** | See protocols (T3) |
| c) | **Memory usage** | Store and pre-process data (“embedded edge”) |
| d) | **Specific capabilities** | More advanced processing („edge controller“) |

| T5. IIoT devices | | |
|---|---|---|
| a) | **Device connectivity** | • See protocols (T3)<br>• Special devices or services for connection, e.g. GateManager, machine pool management system, (cryptographic) key switch |

| T5. IIoT devices | | |
|---|---|---|
| b) | **Device management** | Remote device maintenance |
| c) | **Deployment, provision of software** | • Remote device maintenance<br>• Special "Automation Runtime software kernel" on all B&R target devices to enable hardware independence for the application components. |

| T6. Security | |
|---|---|
| | • Encrypted VPN<br>• Integrated firewall<br>• Machine level access rights (via GateManager/machine pool management system)<br>• Remote access via KeySwitch |

| T7. Data protection | |
|---|---|
| | • mapp Audit: all user actions are logged with a timestamp and a user name<br>• Alarm notifications via text message<br>• Privacy agreements are defined in the B&R privacy policy, but they are only in text form and there is no technical support (or mechanism) to support them. |

| T8. Cloud support | |
|---|---|
| | • Takes place via the (optional) "Orange Box", a special device for cloud connection of a plant using OPC-UA.<br>• ABB Cloud is mentioned. |

| T9. Scalability | |
|---|---|
| | Vendor statement on scalability: *"Complete scalability of controller, visualization system and drive: seamlessly adapt to CPUs of different performance classes, easy project porting via tooling, "grows with the application", uniform programming interface, runtime environment remains unchanged when new hardware is integrated"*. |

| T10. Digital twins / Asset Administration Shells | | |
|---|---|---|
| a) | **Digital twins** | • Device simulations: "The simulation options of mapp Control simplify development and accelerate commissioning".<br>• Integrable 3D representation of devices and machines for Simulink, Maple soft digital twin, functional mockup interface, or Industrial Physics 3D twin representations. |
| b) | **AAS approach used for IoT devices** | *No information available* |
| c) | **AAS approach used for edge devices** | *No information available* |

| T11. Data management and data analysis | |
|---|---|
| | Data management is based entirely on OPC-UA. |

| T12. Offered AI methods | |
|---|---|
| | AI seems to be envisaged for future versions: „Clever algorithms – even artificial intelligence – will be the fuel that powers ongoing performance optimizations and predictive maintenance", "which includes all the prerequisites for future cloud applications featuring artificial intelligence and machine learning." |

| T13. Openness and Extensibility | | |
|---|---|---|
| a) | **Store** | *No information available* |

| T13. Openness and Extensibility | | |
|---|---|---|
| b) | **App support for/by developers** | Automation Studio with Logical View, WYSIWYG (IEC61131-3, ANSI C) and various other languages (see T13c). |
| c) | **Use of "external" algorithms/data** | • „Open Architecture" through usage of edge devices<br>• Various languages (IEC61131-3): PLCopen, Ladder Diagram, Function Block Diagram, Instruction List, Sequential Function Chart, Automation Basic, Structured Text, Continuous Function Chart |
| d) | **AI interfaces** | *No information available* |

| T14. Systematic Configurability | |
|---|---|
| | • Modular (configurable) software components ("configure ready-made mapps")<br>• Unified configuration of devices, servos, motors<br>• Integrated CAM editor<br>• Tools for configuration testing: Test window, Oscilloscope, Monitor |

| T15. Ecosystem support | | |
|---|---|---|
| a) | **"Multi-Sided" platform** | *No information available* |
| b) | **Open to third-party content** | „Open Architecture" through use of edge devices, but no third party devices mentioned |
| c) | **Reference to RAMI 4.0** | *No information available* |

| T16. Other technical abilities | |
|---|---|
| | • mapp CodeBoxes allow programming directly on the HMI of the machine, e.g., with ladder diagrams or structured text (partially visual programming).<br>• Self-optimizing controllers: "autotuning, virtual sensing, optimization of control parameters, fine tune"<br>• HMI based on HTML5, CSS3 and JavaScript |

| T17. References | |
|---|---|
| | https://www.br-automation.com/en/products/software/mapp-technology/ |

## 3.5 Cisco – Kinetic

| T1. Overview | | |
|---|---|---|
| a) | **Name of the platform** | Cisco Kinetic |
| b) | **Platform vendor or provider** | Cisco Systems, USA |
| c) | **Vendor summary** | *„Cisco Kinetic is the cornerstone of the Cisco® IoT portfolio. With this platform, Cisco is not only fulfilling the need for IoT technology and products, but is also revolutionizing our understanding of networking. Instead of simply providing connectivity, the network will host computation, improving the value of data as it is transported. The network is now smarter. Instead of viewing 'the cloud' as a destination, modern IoT networks will pass data through clouds as well as to clouds. Instead of simply enabling connectivity, the Kinetic platform will control the distribution of data, providing far reaching distribution while maintaining and restricting access to data. In numerous ways, Cisco is advancing the state of the art in both IoT and networking. "* |
| d) | **Platform components** | • Gateway Management Module (GMM)<br>• Edge and Fog Processing Module (EFM)<br>• Data Control Module (DCM) |
| e) | **Online marketplace platform** | Yes, the platform can be used for online marketplaces. |
| f) | **Mobility platform** | Yes, the platform can be used for mobility platforms (e.g., fleet management). |
| g) | **B2B context** | Yes |
| h) | **B2C context** | No focus on end users |
| i) | **Platform users** | IoT platforms and industry applications for enterprises |
| j) | **Fields of application** | • Administration environment for managing and monitoring sensor data generated by technical objects from the Internet of Things.<br>• Development, customization and operation of cloud-based IoT business applications.<br>• Focus on the management of network structures and data streams in IoT platforms. |
| k) | **Market penetration** | • Global application by a wide range of users<br>• Widespread application by major customers |

| T2. License information | | |
|---|---|---|
| | | No open source software is used, hence only propitiatory licences from Cisco are given. |

| T3. Protocols | | |
|---|---|---|
| | | • Integration of native IoT protocols from (existing) IoT devices via the use of the Gateway Management Module (GMM) component of the platform.<br>• MQTT, AMQP 0.9, AMQP 1.0 |

| T4. Edge support | | |
|---|---|---|
| a) | **Overview** | The focus of the Cisco Kinetic platform is on data collection and analysis in edge and fog devices. This focus is implemented by means of the dedicated Edge & Fog Processing Module (EFM) component. Controlling data flows from IoT devices to different layers of an IIoT environment, from edge devices to Fog nodes, to a connected cloud and its applications, is another focus of the EFM |

| T4. Edge support | | |
|---|---|---|
| | | component of the Cisco Kinetic platform. Edge devices are used for the following tasks:<br>• Data flows: Aggregation and evaluation for trend analysis, for example for predictive maintenance already at the level of edge devices or, if necessary, for more complex operations at the level of Fog nodes.<br>• Visualization: The aggregated and, if necessary, already evaluated IoT data can be displayed in complex visualizations already at the level of edge devices.<br>• Real-time monitoring (device health) and control of IoT devices via edge devices.<br>• Deploying software updates (also bulk updates) of IoT applications via edge devices. |
| b) | **Communication** | Communication with edge devices and the IoT devices connected to them in the Cisco Kinetic platform provides the capabilities to:<br>• Integration of native IoT protocols from (existing) IoT devices via the use of the Gateway Management Module (GMM)) component of the platform.<br>• Use of data formats from a wide variety of IoT devices, as well as their harmonization/conversion into a uniform data format (no information available on this data format).<br>• Use of message brokers that enable the following communication capabilities for edge devices and IoT devices:<br>○ Publish-Subscribe model<br>○ Request-Reply Messages |
| c) | **Memory usage** | • Edge-based, storage of local data in edge and/or fog nodes<br>• Optional forwarding of edge and/or fog node data to various cloud service providers (Cisco, IBM, Microsoft) |
| d) | **Specific capabilities** | The capabilities specified under T4a can be applied to all IoT devices connected to edge devices throughout their IoT life cycle. |

| T5. IIoT devices | | |
|---|---|---|
| a) | **Device connectivity** | • Wide range of all common protocol options for device and enterprise applications<br>• Focus on the use of gateways with a dedicated gateway management component (Gateway Management Module (GMM))<br>• Possibility to integrate third party devices<br>• Integration of different protocols and systems via abstraction of protocols using Cisco routers within the GMM of the platform |
| b) | **Device management** | • Hierarchical management<br>• Extensive edge and fog computing functionalities via dedicated edge computing component (Edge and Fog Processing Module (EFM))<br>• Devices and apps can subscribe to specific data (subscriber model)<br>• Cloud-based gateway management<br>• Real-time deployment of Cisco 8x9 Industrial Integrated Services Routers (IR8x9)<br>• Continuous device monitoring and health check |

| T5. IIoT devices | | |
|---|---|---|
| c) | **Deployment, provision of software** | • Software deployment<br>  ○ REST<br>  ○ Software-as-a-Service (SaaS)<br>  ○ Apps for administrative tasks (dashboard)<br>  ○ Deployment of microservices in Cisco containers on Gateways<br>• Bulk updates are possible via the Edge / fog application lifecycle manager, which allows Edge and Fog applications to be started, stopped, uninstalled or updated at any time. |

| T6. Security | |
|---|---|
| | Security related to edge devices: As part of the EFM component, the platform applies a set of security techniques specifically targeted at edge devices (and Fog Nodes):<br>• EFM supports secure encrypted communication between brokers to prevent data from being intercepted and traffic from being intercepted.<br>• EFM user and node management: EFM organizes data hierarchically. Node management allows the administrator to assign list, read, write, and configuration permissions to nodes in this hierarchy and their child elements.<br>• The Kinetic EFM system uses a highly reliable messaging system based on IoT message brokers that establish multi-hop communication between brokers.<br>• The system sends all data over the network using TLS connections to prevent traffic monitoring. The EFM System Administrator application is protected by the HTTPS protocol. |

| T7. Data protection | |
|---|---|
| | Data Control Module (DCM) component delivers the right data to the right applications in the cloud to drive better business outcomes.<br>• DCM allows data to be unlocked from devices and moved securely to a cloud-based application (complete control over data and where it is stored, providing visibility and portability).<br>• DCM provides the ability to forward policies and rules to easily move IoT device data to cloud applications across deployments with multiple clouds and locations, while executing policies to enforce data ownership.<br>• DCM provides the ability to create policies that make data available to different applications based on device type, or set custom rules using rule sets. |

| T8. Cloud support | |
|---|---|
| | • Use of the Cisco Cloud<br>• Connection to the IBM Watson Cloud and the services available on it<br>• Connection to the Microsoft Azure Cloud and the services available on it |

| T9. Scalability | |
|---|---|
| | • Connection of new edge devices via gateways is possible<br>• The integration as well as the removal of IoT devices into/from existing systems is possible at any time, as the Kinetic platform supports the complete IoT lifecycle. |

| T10. Digital twins / Asset Administration Shells | |
|---|---|
| | *No information available* |

| T11. Data management and data analysis | |
|---|---|
| | Extensive options for collecting, monitoring and analyzing data in real time, implemented in a dedicated data management component Data Control Module (DCM):<br>• Access to all data sources (IoT devices, databases, etc.) in a unified workspace ("single, unified workspace")<br>• Customizable policy-driven data flows<br>• Aggregation of multiple data points from different sources to identify trends and patterns, trigger actions, and route a precise selection of data to any combination of applications.<br>• Historical data store (IoT Historian Database):<br>  ○ Continuous import of time series with high ingestion rate<br>  ○ Response time for query results even in the terabyte range is below seconds<br>  ○ Immediate and continuous analysis of real-time data while the data is still being loaded<br>  ○ Local real-time analysis and storage near the data source |

| T12. Offered AI methods | |
|---|---|
| | • Comprehensive data analytics capabilities, both on edge devices and in the cloud<br>• Complex, rule-based event handling |

| T13. Openness and Extensibility | | |
|---|---|---|
| a) | **Store** | *No information available* |
| b) | **App support for/by developers** | • Provision of SDKs for the development of customer-specific Apps<br>• Support for "no code" development or configuration of apps via visual programming / configuration of apps via drag-and-drop user interfaces and via configuration of data flows via graphical user interfaces |
| c) | **Use of "external" algorithms/data** | • Restricted, allows integration of data from third-party providers<br>• Integration of customer's own software is not explicitly mentioned |
| d) | **AI interfaces** | • No information on AI interfaces from Cisco<br>• Ability to use interfaces and services in IBM Watson Cloud or Microsoft Azure Cloud supported by Cisco Kinect. |

| T14. Systematic Configurability | |
|---|---|
| | • "No code" development of applications<br>• Data flow configuration |

| T15. Ecosystem support | | |
|---|---|---|
| a) | **"Multi-Sided" platform** | • Partial possibility to form ecosystems. The platform allows networking with a wide variety of cloud service providers (Microsoft Azure, IBM Watson).<br>• Direct integration of the platform into other IoT platforms is only possible to a limited extent; at least the networking of data streams is possible via the protocols, services and data abstraction used, but is not described as a core element of the platform. |
| b) | **Open to third-party content** | • Restricted, allows integration of third-party data.<br>• Integration of customer's own software is not explicitly mentioned. |

| T15. Ecosystem support | | |
|---|---|---|
| c) | **Reference to RAMI 4.0** | *No information available* |

| T16. Other technical abilities |
|---|
| • Microservices in Cisco Containers on Gateways<br>• Visual programming |

| T17. References |
|---|
| • Overview of Cisco Kinetic Platform: https://www.cisco.com/c/en/us/solutions/internet-of-things/iot-kinetic.html<br>• Overview of the Gateway Management Module (GMM): https://www.cisco.com/c/dam/en/us/solutions/collateral/internet-of-things/kinetic-datasheet-gmm.pdf<br>• Overview of the Edge and Fog Processing Module (EFM): https://www.cisco.com/c/dam/en/us/solutions/collateral/internet-of-things/kinetic-datasheet-efm.pdf<br>• Overview of the Data Control Module (DCM): https://www.cisco.com/c/dam/en/us/solutions/collateral/internet-of-things/kinetic-datasheet-dcm.pdf<br>• Overview of security in the Cisco Kinetic platform: https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/kinetic/tech_notes/kinetic-security.pdf<br>• Whitepaper on the use of Cisco Kinetic in the industrial production: https://www.cisco.com/c/dam/en/us/solutions/collateral/internet-of-things/cisco-kinetic-mfg-whitepaper.pdf |

## 3.6 Deviceinsight – Centersight

| T1. Overview | | |
|---|---|---|
| a) | **Name of the platform** | Device Insight / CENTERSIGHT NG |
| b) | **Platform vendor or provider** | Device Insight GmbH, Munich, Germany |
| c) | **Vendor summary** | *"Want to make your processes more efficient and bring smart, networked products to market? Is your goal nothing less than implementing a new business model? Based upon our flexible IoT framework and well proven applications we enable you to implement any IoT or IIoT project quickly, economically and safely.*<br>*For a sustainable business success we put you in the position to analyze your data and create value by planning needs-based maintenance and services, avoiding downtimes and boosting productivity. Our customized applications and cutting-edge software mean that our IoT solutions can optimize any operations, anywhere in the world."* |
| d) | **Platform components** | • Applications<br>• Device & Edge<br>• Platform & Cloud |
| e) | **Online marketplace platform** | *No information available* |
| f) | **Mobility platform** | • Tablets and Smartphone Apps<br>• Support for Telematics and Connected Cars |
| g) | **B2B context** | Yes |
| h) | **B2C context** | *No information available* |
| i) | **Platform users** | Developers, plant operators |
| j) | **Fields of application** | • Predictive Maintenance<br>• Condition Monitoring |
| k) | **Market penetration** | Kuka, Fendt, Kärcher, reflex thinking solutions |

| T2. License information | | |
|---|---|---|
| | | *„Pay as you grow"* |

| T3. Protocols | | |
|---|---|---|
| | | • HTTPS, MQTT, OPC UA, field bus protocols like Modbus, SNMP, CSV, FTP, etc.<br>• Protocol adapter (standardized and proprietary) |

| T4. Edge support | | |
|---|---|---|
| a) | **Overview** | "Edge Analytics" based on a modular structure to integrate customer-specific extensions. |
| b) | **Communication** | See Protocols (T3) |
| c) | **Memory usage** | *No information available* |
| d) | **Specific capabilities** | Data processing on edge devices, local pattern recognition, and machine-specific rule sets for condition monitoring. |

| T5. IIoT devices | | |
|---|---|---|
| a) | **Device connectivity** | See Protocols (T3) |
| b) | **Device management** | • Via cloud or REST API, e.g., for automatic firmware updates or remote configuration<br>• Integrated remote access (remote maintenance) |

| T5. IIoT devices | | |
|---|---|---|
| c) | **Deployment, provision of software** | Via cloud or REST API, e.g., for automatic firmware updates |

| T6. Security | |
|---|---|
| | Integrated VPN tunnel |

| T7. Data protection | |
|---|---|
| | *No information available* |

| T8. Cloud support | |
|---|---|
| | • Cloud-based (Multi-Tenancy SaaS), on-premise or hybride installation ("Cloud and hybrid Services")<br>• Azure Cloud integration |

| T9. Scalability | |
|---|---|
| | • Unlimited scalability (*"unlimited scalability and rapid linking of devices"*)<br>• For cloud-based installations: automatic resource adaptation during peak loads<br>• Millions of values and data points in near real-time |

| T10. Digital twins / Asset Administration Shells | |
|---|---|
| | *No information available* |

| T11. Data management and data analysis | |
|---|---|
| | • "Big data advanced analytics" for automated data analysis<br>• Long-term data storage for time series and monitoring data<br>• Blobstore, NoSQL or Data Warehouse are supported |

| T12. Offered AI methods | |
|---|---|
| | • Three-step approach: 1) Collect data from devices, 2) Combine data with expert knowledge and describe it in the form of rules (rule engine), 3) Use statistical tools or ML algorithms for predictions.<br>• Advanced Analytics & Predictive Maintenance<br>• Condition Monitoring<br>• Integrated ML toolbox<br>• Azure IoT Hub and Azure Machine Learning Integration |

| T13. Openness and Extensibility | | |
|---|---|---|
| a) | **Store** | *No information available* |
| b) | **App support for/by developers** | • Use of existing UI modules or dashboard elements<br>• (Cloud-)API |
| c) | **Use of "external" algorithms/data** | APIs and integrated Python environment |
| d) | **AI interfaces** | *No information available* |

| T14. Systematic Configurability | |
|---|---|
| | • Condition monitoring definable by drag & drop editor<br>• Customizable (integrated) solutions ("customize solutions to company requirements") especially through rule customization ("self-service rule engine"), e.g. for anomaly detection or condition monitoring<br>• Customizable dashboards |

| T14. Systematic Configurability | | |
|---|---|---|
| | | • Editor for KPIs |

| T15. Ecosystem support | | |
|---|---|---|
| a) | **"Multi-Sided" platform** | Interface standardization ("easily integrate with IoT ecosystems thanks to company-wide interfaces") |
| b) | **Open to third-party content** | In the form of adaptation/configurability ("customizing") and Apps |
| c) | **Reference to RAMI 4.0** | *No information available* |

| T16. Other technical abilities | | |
|---|---|---|
| | | • Augmented reality during remote maintenance by editing images/screenshots, overlays and virtual dashboard<br>• IoT Microservices<br>• KPI Editor |

| T17. References | | |
|---|---|---|
| | | • https://www.device-insight.com/en/centersight/<br>• https://www.device-insight.com/en/centersight-ng-available-on-microsoft-azure/<br>• https://www.device-insight.com/en/<br>• Whitepaper "Artificial intelligence in IoT practice – use cases and success factors" https://www.device-insight.com/en/white-paper-artificial-intelligence-in-iot-practice-use-cases-and-success-factors/ |

## 3.7 Emerson – Plantweb

| T1. Overview | | |
|---|---|---|
| a) | **Name of the platform** | Plantweb digital ecosystem, Plantweb Optics |
| b) | **Platform vendor or provider** | Emerson Automation Solutions, St. Louis, Missouri, USA |
| c) | **Vendor summary** | *"A scalable and secure portfolio of transformational technologies, software and services that provide relevant personnel with enhanced insight to enable actions that drive Top Quartile performance.*<br><br>*Data spread across the enterprise and isolated in silos makes it difficult to identify issues impacting asset availability. With Plantweb Optics, an asset performance platform for managing enterprise asset health, data is combined from multiple applications into asset-centric information to deliver persona-based alerts and KPIs.*<br><br>*Plantweb Optics has real-time automated data collection from assets within the plant funneled into diagnostics and analytics platforms to help visualize, analyze, and predict performance. With this actionable data, plant service and maintenance is seamless with CMMS integrations and workflows. This platform makes staying on top of asset health in the plant easier than ever before."* |
| d) | **Platform components** | • Pervasive Sensing<br>• Secure First Mile<br>• Plantweb Inside Software<br>• Plantweb Advisor Software (OSIsoft PI system as basis)<br>• AMS Ares platform<br>• Always Mobile<br>• Connected Services |
| e) | **Online marketplace platform** | *No information available* |
| f) | **Mobility platform** | Mobility support, e.g., AMS Trex Communicator |
| g) | **B2B context** | Yes |
| h) | **B2C context** | *No information available* |
| i) | **Platform users** | Vague statements such as "personnel," "empowering today's workforce" |
| j) | **Fields of application** | Production, fail-safe, safety and energy management |
| k) | **Market penetration** | Chevron/Oronite, Denka |

| T2. License information | |
|---|---|
| | *No information available* (probably commercial) |

| T3. Protocols | |
|---|---|
| | • Data connections are based on OPC/OPC-UA and Web Services.<br>• Modbus TCP (via mapping)<br>• Hundreds of communication protocols are available through the OSIsoft architecture. |

| T4. Edge support | |
|---|---|
| | *No information available* |

| T5. IIoT devices | | |
|---|---|---|
| a) | **Device connectivity** | See Protocols (T3) |
| b) | **Device management** | • AMS device manager, device monitoring<br>• Device configuration templates |
| c) | **Deployment, provision of software** | *No information available* |

| T6. Security | |
|---|---|
| | Separate network of the control system, completely separated from other networks in the plant<br>• Latest templates for hardening the operating system<br>• Disabling unused system services<br>• Preventing access to removable media<br>• Smart firewall/intrusion prevention device<br>• DeltaV Smart Switches<br>• Application whitelisting<br>• Endpoint security<br>• Patch management service<br>• Network Security Monitor<br>• Assessment |

| T7. Data protection | |
|---|---|
| | Shares some aspects with security, for example:<br>• Preventing access to data<br>• Firewall<br>• Whitelisting<br>• Assessment |

| T8. Cloud support | |
|---|---|
| | Emerson has committed its platform to the cloud-based Microsoft Azure IoT Suite as foundation for services, which in turn extends the Plantweb digital ecosystem to include a secure and flexible platform (private cloud) and third-party cloud services. |

| T9. Scalability | |
|---|---|
| | • Plantweb Insight can be used for applications of any scale.<br>• The platform and the applications running on it are based on the OSIsoft PI system, a highly scalable open data infrastructure („highly scalable open data infrastructure“). |

| T10. Digital twins / Asset Administration Shells | |
|---|---|
| | *No information available* |

| T11. Data management and data analysis | |
|---|---|
| | • PervasiveSensing strategies<br>• Real-time analytics |

| T12. Offered AI methods | |
|---|---|
| | Vendor statement: “*Robust portfolio of scalable analytics tools*” |

| T13. Openness and Extensibility | | |
|---|---|---|
| a) | **Store** | *No information available* |

| T13. Openness and Extensibility | | |
|---|---|---|
| b) | **App support for/by developers** | *No information available* |
| c) | **Use of "external" algorithms/data** | Vendor statement: *„easily integrate pre-build analytics into your system"* |
| d) | **AI interfaces** | *No information available* |

| T14. Systematic Configurability | | |
|---|---|---|
| | | Vendor statement: *„easily integrate pre-build analytics into your system"* |

| T15. Ecosystem support | | |
|---|---|---|
| a) | **"Multi-Sided" platform** | Integrates Microsoft Azure IoT Suite |
| b) | **Open to third-party content** | Third-party cloud services (via Microsoft Azure IoT Suite) |
| c) | **Reference to RAMI 4.0** | *No information available* |

| T16. Other technical abilities | | |
|---|---|---|
| | | • Integrated virtual reality/remote support<br>• Plantweb appears to be a (demonstration) VM with integrated pre-built applications such as Steam Tap, Pressure Relief, Pump Application, Wiress Pressure Gauge, Location Application, etc. |

| T17. References | | |
|---|---|---|
| | | https://www.emerson.com/en-us/expertise/automation/industrial-internet-things/plantweb-digital-ecosystem |

## 3.8 Endress + Hauser – Netilion

| T1. Overview | | |
|---|---|---|
| a) | **Name of the platform** | Netilion |
| b) | **Platform vendor or provider** | Endress + Hauser, Reinach, Switzerland |
| c) | **Vendor summary** | *"You can use our products immediately, at any time and from anywhere. And you will have fun using them.*<br>*We create digital services using the most modern and secure Internet technologies. We combine them with the technologies of industrial production facilities. All our services are easy and straightforward to put into operation - complicated implementation projects are a thing of the past. "* |
| d) | **Platform components** | • Netilion Smart Systems<br>• Netilion Analytics<br>• Netilion Health<br>• Netilion Library<br>• Netilion Connect<br>• Netilion Inventory |
| e) | **Online marketplace platform** | *No information available* |
| f) | **Mobility platform** | Access to information via smartphone, but no specific services are mentioned. |
| g) | **B2B context** | Yes |
| h) | **B2C context** | *No information available* |
| i) | **Platform users** | In particular, machine operators/plant operators in application scenarios. |
| j) | **Fields of application** | Level monitoring (Netilion Value), surface water quality, aquaculture water quality |
| k) | **Market penetration** | Salzgitter AG, Municipality of Baltschieder, Department for Forrests beider Basel |

| T2. License information | | |
|---|---|---|
| | | Commercial, in tariffs FREE, BASIC, PLUS or PREMIUM |

| T3. Protocols | | |
|---|---|---|
| | | Profibus DP, Profibus DA, Hart, Modbus, Ethernet, Bluetooth, REST/JSON |

| T4. Edge support | | |
|---|---|---|
| | | Captures assets/machines and provides them as a list. No further information about edge devices was available. |

| T5. IIoT devices | | |
|---|---|---|
| a) | **Device connectivity** | See protocols (T3) |
| b) | **Device management** | • Device monitoring<br>• Smart device configuration via a special tablet (Field Expert Tablet) or special tablet software |
| c) | **Deployment, provision of software** | *No information available* |

| T6. Security | | |
|---|---|---|
| | | Vendor statement: using the most modern and secure Internet technologies (*„unter Verwendung der modernsten und sichersten Internet-Technologien"*) |

| T7. Data protection | |
|---|---|
| | Hosted by Amazon, uses Amazon Web Services (AWS). Amazon was accredited for ISO 27001, SOC 1 and SOC 2/SSAE 16/ISAE 3402, PCI Level 1, FISMA Moderate and Sarbanes Oxley (SOX).<br>*„Die physische Infrastruktur von Endress + Hauser wird in den sicheren Rechenzentren von Amazon gehostet und verwaltet und nutzt die Amazon Web Service (AWS) -Technologie. Amazon verwaltet das Risiko kontinuierlich und unterzieht sich wiederkehrenden Bewertungen, um die Einhaltung der Industriestandards sicherzustellen. Der Betrieb des Rechenzentrums von Amazon wurde akkreditiert unter:*<br>• *ISO 27001*<br>• *SOC 1 und SOC 2/SSAE 16/ISAE 3402*<br>• *PCI Level 1*<br>• *FISMA Moderate*<br>• *Sarbanes-Oxley (SOX)“* |

| T8. Cloud support | |
|---|---|
| | • Netilion is cloud-based (named especially for building blocks Inventory, Connect)<br>• Edge devices must have access to specified servers/services (“Edge-devices must have port 443 access to netilion.endress.com and api.netilion.endress.com”) |

| T9. Scalability | |
|---|---|
| | *No information available* |

| T10. Digital twins / Asset Administration Shells | | |
|---|---|---|
| a) | **Digital twins** | • The main steps for creating a digital twin are to take a photo of the asset, to enter some data and to store the information. (*„Foto vom Asset machen, ein paar Eckdaten hinterlegen, speichern … fertig! Schon ist ein digitaler Zwilling Ihres Assets angelegt. “)*<br>• The integration of the digital twins takes place in particular via connected edge devices. |
| b) | **AAS used for IoT devices** | *No information available* |
| c) | **AAS used for edge devices** | *No information available* |

| T11. Data management and data analysis | |
|---|---|
| | • File Sharing and Data Management Services via Netilion Library<br>• Assignment of data to digital twins |

| T12. Offered AI methods | |
|---|---|
| | *No information available* |

| T13. Openness and Extensibility | | |
|---|---|---|
| a) | **Store** | *No information available* |
| b) | **App support for/by developers** | *No information available* |
| c) | **Use of “external” algorithms/data** | *No information available* (potentially via REST/JSON-API) |
| d) | **AI interfaces** | *No information available* |

| T14. Systematic Configurability | | |
|---|---|---|
| | | Settings for (edge-)devices |

| T15. Ecosystem support | | |
|---|---|---|
| a) | **“Multi-Sided“ platform** | *No information available* |
| b) | **Open to third-party content** | In form of “Netilion Connect solution providers” |
| c) | **Reference to RAMI 4.0** | *No information available* |

| T16. Other technical abilities | | |
|---|---|---|
| | | *No information available* |

| T17. References | | |
|---|---|---|
| | | • https://netilion.endress.com/de<br>• https://netilion.endress.com/blog/<br>• https://netilion.endress.com/blog/cybersecurity-in-industry/ |

## 3.9 General Electrics – Predix

| T1. Overview | | |
|---|---|---|
| a) | **Name of the platform** | General Electrics – Predix |
| b) | **Platform vendor or provider** | General Electrics, USA |
| c) | **Vendor summary** | *„Created by GE to help transform its business, Predix—the operating system for the Industrial Internet—is the only solution built by industry for industry. From the edge to the cloud, Predix turns data and intelligence into actionable insights, and employs the latest innovation, including digital twins, to optimize assets and operations. All this is supported by a robust ecosystem that accelerates app development.*<br><br>*As a scalable, asset-centric data foundation, a comprehensive and secure application platform can run, scale, and extend digital industrial solutions.*<br><br>*Leading IIoT capabilities:*<br>*The platform delivers shared capabilities that industrial applications require: asset connectivity, edge technologies, analytics and machine learning, big data processing, and asset-centric digital twins.*<br><br>*Build once, deploy anywhere:*<br>*Designed as a distributed application platform, Predix Platform is optimized for high volume, low latency, and integration-intensive data management and analytics-driven outcomes."* |
| d) | **Platform components** | • Predix Essentials<br>• Predix Cloud<br>• Predix Private Cloud<br>• Predix Edge |
| e) | **Online marketplace platform** | Limited capabilities to support online marketplaces, various functionalities, services and software components can be used in logistics and retail but the focus is on IIoT. |
| f) | **Mobility platform** | In the context of IIoT, for example, fleet management is supported. |
| g) | **B2B context** | Yes |
| h) | **B2C context** | No, no focus on end customers |
| i) | **Platform users** | Industrial enterprise customers who either want to migrate to IIoT or expand or optimize existing IIoT systems. |
| j) | **Fields of application** | • Administration environment for managing and monitoring sensor data generated by technical objects from the Internet of Things.<br>• Development, customization and operation of cloud-based IoT business applications.<br>• One focus is on Digital Twin-based development and optimization of devices and products.<br>• Another focus is on edge computing, realized by the dedicated component "Predix Edge". |
| k) | **Market penetration** | • Global application by a wide range of users<br>• Widespread application by major customers |

| T2. License information | |
|---|---|
| | • Proprietary licenses of the provider (General Electrics) |

| T2. License information | |
|---|---|
| | • Use of open source software in customer's own applications is possible |

| T3. Protocols | |
|---|---|
| | • Support (via adapter) for: OPC UA, Modbus, OSI PI, MQTT, EGD<br>• REST<br>• Support for additional protocols through the "Predix Edge" component which connects to the platform's own "GE IGS Server" which can provide several hundred different protocols. |

| T4. Edge support | | |
|---|---|---|
| a) | **Overview** | GE Predix and the dedicated Predix Edge component specify the following uses for Edge devices: *"Connect, monitor and manage assets. Predix Edge provides the connectivity options and management features to:*<br>• *Easily connect to assets and data sources*<br>  ○ *Monitor Edge instance status and health*<br>  ○ *Scale to thousands of Edge instances and connected devicesPut analytics to work*<br>• *Use Complex Event Processing engines or container analytics to:*<br>  ○ *Apply rich analytics to data streams in near-realtime*<br>  ○ *Locally detect anomalies in device or process operations*<br>  ○ *Add intelligence to local equipment controls*<br>• *Take advantage of Edge applications. With Predix Edge you can use Edge applications to:*<br>  ○ *Handle near-realtime monitoring and response needs*<br>  ○ *Complement and extend existing solutions*<br>  ○ *Comply with security and regulatory requirements*<br>• *Simplify solution management. Predix Edge Manager simplifies and automates tasks to:*<br>  ○ *Provision Edge instances and connected devices*<br>  ○ *Provision and manage local apps and analytics*<br>  ○ *Monitor and control secure operations"*<br>Edge-specific deployment: *"Predix Edge can be deployed as an integrated hardware/software gateway, a VMware ESXi virtual machine or an embedded software image."* |
| b) | **Communication** | • The component "Predix Connectivity" realizes the connection and communication with edge devices.<br>• Use of various communication channels: *"Predix Connectivity offers secure and reliable communication between Predix Edge and Predix Cloud over fixed line, cellular, and satellite networks."*<br>• One focus is on the use of VPN.<br>• Bi-directional communication with edge devices possible. |
| c) | **Memory usage** | Edge-based data collection, pre-processing evaluation on edge devices, and forwarding from edge storage for further processing by platform services, realized by the dedicated Predix Edge platform and its components. |
| d) | **Specific capabilities** | • In general, due to the rather free possibilities of deploying custom applications on edge devices in the Predix Edge platform, the widest possible range of capabilities can be realized on edge devices. |

| T4. Edge support | | |
|---|---|---|
| | | • Access through edge devices to extensive Historian functionalities |

| T5. IIoT devices | | |
|---|---|---|
| a) | **Device connectivity** | • Wide range of all common protocol options for device and enterprise applications<br>• Use of VPN<br>• Possibility to integrate 3rd party devices<br>• Device connection possible via a wide variety of paths, cable, cellular, satellite, etc.<br>• Collection of data from devices and beyond includes:<br>  ○ Asset data: Time series, alarms, event data, HMI/SCADA<br>  ○ Plant data from MES, SCADA: operational data, alarms, KPI data<br>  ○ Enterprise data from EAM/CMMS |
| b) | **Device management** | • Edge computing: container-based execution of data analytics and AI techniques on edge devices<br>• Continuous device monitoring<br>• Enrollment, organization, monitoring, and remote management of connected IoT devices<br>• Over-the-air updates<br>• Remote maintenance (remote updates) of device software |
| c) | **Deployment, provision of software** | • REST<br>• Software-as-a-Service (SaaS)<br>• Wide range of services that can be used across the platform<br>• Apps for administrative tasks<br>• Apps for analysis tasks<br>• Provision of analysis and AI procedures in a marketplace for algorithms or complete applications. |

| T6. Security | | |
|---|---|---|
| | | **Edge-specific security:** Predix Edge creates a secure end-to-end operating environment via key features and design principles, including:<br>• Management console security and role-based access.<br>• Certificate-based device connectivity<br>• Hardened embedded operating system<br>• Data encryption<br>Predix Cloud Connect creates a site-to-site virtual private network (VPN) connection between the local network and the Predix Cloud. Predix Cloud Connect uses the Internet Protocol Security (IPSec) secure network protocol suite to create a hybrid cloud environment that provides private and secure access to applications and data on the on-premises infrastructure and data and services on the Predix Cloud. With Predix Cloud Connect, VPN connections can be configured with the following settings:<br>• Redundancy<br>• Forwarding proxy function<br>• Bandwidth<br>• IPSec mode<br>• AES encryption strength<br>• Cryptographic hash function<br>With Predix Cloud Connect, the VPN connection can be monitored and fully managed through an interactive dashboard. |

| T7. Data protection | | |
|---|---|---|
| | | PREDIX data protection plan - Predix platform service and security policy:<br>• PREDIX acts as a data processor of all personal data.<br>• PREDIX will comply with all laws and regulations that apply to it as a service provider<br>• Clear indication of where customer data is stored<br>• PREDIX uses controls like access control, access authorization and authentication<br>• Password setting<br>• Authorization checks<br>• Vulnerability management and malware protection<br>• Data classification and processing<br>• Data retention: PREDIX provides customers with the necessary features to exercise their rights regarding the data they hold, including the right to access, update, move, etc.<br>Customer data is retained for as long as necessary to provide the required service to the customer based on contractual agreements. |

| T8. Cloud support | | |
|---|---|---|
| | | Cloud-based platform using:<br>• Predix cloud: general cloud offering for storage and processing (analysis, further processing in customers' applications) of big data in IIoT context.<br>• Predix Private cloud: Same functionality as Predix cloud but with a direct connection to the customer's data store applying security requirements, data compliance requirements, and data ownership rights defined by the customer. |

| T9. Scalability | | |
|---|---|---|
| | | • The platform can be scaled according to the customer's needs (data volume, number of devices, etc.).<br>• Secure on-boarding and off-boarding at runtime support scalability. |

| T10. Digital twins / Asset Administration Shells | | |
|---|---|---|
| a) | **Digital twins** | Digital Twins are used to map devices (assets) and device networks in order to<br>• Facilitate monitoring of devices and device networks.<br>• Make predictions about devices and device networks based on simulations in the Digital Twin.<br>• The results of the Digital Twins simulations are used to realize maintenance, device condition analysis, predictive maintenance and productivity optimization. |
| b) | **AAS used for IoT devices** | The use of Digital Twins, also as a composite of Digital Twins, is similar to the concept of the AAS. |
| c) | **AAS used for edge devices** | See T10b |

| T11. Data management and data analysis | | |
|---|---|---|
| | | • Extensive capabilities for collecting, monitoring and analyzing data is near real-time<br>• Pattern recognition<br>• Visualization of data and data analysis<br>• Use of data for prediction of device behavior and optimization<br>• Special data analysis capabilities in edge devices<br>• Extensive library of data analysis techniques<br>• APIs provided for integration of data streams into customer's own software |

| T12. Offered AI methods | |
|---|---|
| | • Extensive data analysis capabilities<br>• Anomaly detection using machine learning<br>• Prediction-based maintenance recommendations<br>• Import capability of AI procedures on the part of the customer<br>• Container-based and VM-based execution of analytics and AI procedures on edge devices |

| T13. Openness and Extensibility | | |
|---|---|---|
| a) | **Store** | • Predix has a store (or catalog) with the main categories of a) Services and Software and b) Private cloud services. The store is part of the Predix Developer Platform.<br>• There is another store for Predix Analytics that offers AI solutions. |
| b) | **App support for/by developers** | • The Predix platform supports app management and developers by providing extensive documentation, APIs, tutorials, etc.<br>• Active developer community support (forums, repositories)<br>• With regard to the support provided by the platform, Predix does not "only" address developers, but also specifically Data Scientists and Controls Engineers. The statements of the Predix web pages on this are as follows:<br>○ *"Developers: We've built a comprehensive platform and development environment for you with all the right services, tools, techniques, and supporting community to create innovative industrial IoT apps."*<br>○ *"Data Scientists: Predix is readymade for you to manage and implement the latest, most meaningful statistical analysis, data mining, and retrieval processes for Big Data that help identify key insights and trends."*<br>○ *"Controls Engineers: Predix tools and techniques help you develop edge software solutions that seamlessly connect intelligent machines securely to the cloud for apt remote monitoring, diagnostics, and control."* |
| c) | **Use of "external" algorithms/data** | • Use of open source AI algorithms by customers is actively supported<br>• Docker container-based applications and analytics evaluations can be developed using various languages: C, C++, Python, Node.js or Java. |
| d) | **AI interfaces** | The integration of customer AI applications is widely supported. The statement of the Predix web pages on this is as follows: *"A set of over 100 algorithms and models is available in Predix Platform Analytics Marketplace. A finished analytic written in C++, Java, or Python can be orchestrated to run based on a time schedule or event occurrence. Alternatively, complex analytics developed outside Predix Platform using the preferred tools of a data scientist, can just as easily be incorporated into your application. Base algorithms can be sourced from open source libraries and configured in your Predix Platform powered applications."* |

| T14. Systematic Configurability | |
|---|---|
| | • Customers can customize the provided applications very widely<br>• APIs are provided to integrate data streams with customers' own software |

| T14. Systematic Configurability | |
|---|---|
| | • Customers can bring their own analytics and AI applications into the platform |

| T15. Ecosystem support | | |
|---|---|---|
| a) | **"Multi-Sided" platform** | Ecosystem formation is possible because it is possible to connect other platforms and applications to Predix. |
| b) | **Open to third-party content** | Free integration of third-party software on the customer side |
| c) | **Reference to RAMI 4.0** | *No information available* |

| T16. Other technical abilities | |
|---|---|
| | • The platform offers extensive Historian functionalities<br>• The platform has its own Edge OS (based on a Yocto Linux distribution)<br>• Docker container-based applications and analytics approaches |

| T17. References | |
|---|---|
| | Extensive information available on GE Predix and Predix Edge web pages and websites. Data sheets available as PDFs.<br>• General GE Predix overview:<br>  ○ https://www.ge.com/digital/sites/default/files/download_assets/Predix-Essentials-from-GE-Digital-datasheet.pdf<br>  ○ https://www.ge.com/digital/sites/default/files/download_assets/predix_onesheet_may2015_0.pdf<br>  ○ https://www.ge.com/digital/iiot-platform/predix-essentials<br>  ○ https://www.ge.com/digital/sites/default/files/download_assets/Become-digital-industrial-company-GE-Digital-overview.pdf<br>• Predix Edge platform:<br>  ○ https://www.ge.com/digital/iiot-platform/predix-edge<br>  ○ https://www.ge.com/digital/sites/default/files/download_assets/predix-edge-from-ge-digital-datasheet.pdf<br>  ○ https://www.ge.com/digital/documentation/edge-software<br>• Analytics in Predix (general and for edge devices):<br>  ○ https://www.ge.com/digital/iiot-platform/machine-learning-analytics<br>  ○ https://www.ge.com/digital/sites/default/files/download_assets/Data-Science-Services-from-GE-Digital.pdf<br>• Use of Digital Twins in Predix und Predix Edge:<br>  ○ https://www.ge.com/digital/applications/digital-twin<br>  ○ https://www.ge.com/digital/blog/digital-twins-bridge-between-industrial-assets-and-digital-world<br>• Predix security:<br>https://www.ge.com/digital/iiot-platform/cyber-security-trust-center<br>• GE Historian services:<br>https://www.ge.com/digital/applications/proficy-historian<br>• Data protection plan:<br>https://www.ge.com/digital/sites/default/files/download_assets/GE-Corp-Data-Protection-Plan-Predix.pdf<br>• Predix store and services:<br>  ○ https://www.predix.io/catalog/services/<br>  ○ https://www.predix.io/catalog/ppc-services<br>  ○ https://www.ge.com/digital/iiot-platform |

## 3.10 Google – Google Cloud IoT Core

| T1. Overview | | |
|---|---|---|
| a) | **Name of the platform** | Google Cloud IoT Core |
| b) | **Platform vendor or provider** | Google, Mountain View, CA, USA |
| c) | **Vendor summary** | *"A fully managed service to easily and securely connect, manage, and ingest data from globally dispersed devices. "* |
| d) | **Platform components** | • IoT Core<br>  ○ Cloud Functions<br>  ○ Pub/Sub<br>  ○ Dataflow<br>  ○ Cloud Bigtable<br>  ○ Big Query<br>  ○ AI Platform<br>  ○ Datalab<br>  ○ Insights<br>  ○ Data Studio<br>• Gateway<br>  ○ Tensor Flow<br>  ○ Connection Agent |
| e) | **Online marketplace platform** | Google Cloud Marketplace or Google AI Hub |
| f) | **Mobility platform** | Can be used with for mobility solutions and operated with mobile devices. |
| g) | **B2B context** | Yes |
| h) | **B2C context** | Seems geared towards B2B, although $300 starting credit allows end users to try it out as well. |
| i) | **Platform users** | • The setup seems rather technology intensive (create device registry, create device key pair add device to registry, do Git code clone, ...), i.e. the technical side is rather intended for programmers or users with IT background.<br>• Other Industry 4.0 users can use the platform via the web user interface. |
| j) | **Fields of application** | • Predictive maintenance<br>• Real-time asset tracking<br>• Logistics and supply chain management<br>• Smart cities and buildings |
| k) | **Market penetration** | Reference projects e.g. with The Home Depot, PayPal, Target, HSBC, McKesson, 20th Century Fox, American Cancer Society, American Eagle Outfitters, Bloomberg, Broad Institute, Colgate-Palmolive, eBay, Farmacias del Ahorro, FWD, Go-JEK, etc. |

| T2. License information | |
|---|---|
| | • "Pay as you go" service<br>• Cloud IoT Core costs are charged per MB of data exchanged by IoT devices with the service once the free quota of 250 MB has been exceeded.<br>• Partially Open Source, e.g., Mender[14] |

| T3. Protocols | |
|---|---|
| | • MQTT and –HTTP protocols (ZigBee, Bluetooth) |

[14] https://mender.io/

| T3. Protocols | | |
|---|---|---|
| | | • Bi-directional communication is possible (intelligent and responsive IoT data pipeline).<br>• Protocol converter provides connection endpoints for protocols for all device connections, native support for secure connection over industry standard protocols such as MQTT and HTTP. Protocol converter publishes all device telemetry data to the cloud (publish/subscribe) so it can be processed by downstream analytics systems. |

| T4. Edge support | | |
|---|---|---|
| a) | **Overview** | Edge-Analytics on gateways |
| b) | **Communication** | Communication via the mentioned protocols (see T3), especially MQTT and REST. |
| c) | **Memory usage** | *No information available* (pure pre-aggregation is conceivable due to the approach) |
| d) | **Specific capabilities** | Gateways can run Application Logic, Tensor Flow (ML Model) and Connection Agents. |

| T5. IIoT devices | | |
|---|---|---|
| a) | **Device connectivity** | • Distributes device data for later aggregation.<br>• Commands or configuration instructions can be sent to devices connected to Cloud IoT Core. Commands are quick, frequent, one-time instructions sent to devices.<br>• Configurations are persistent instructions sent to all devices subscribed to the service when using MQTT.<br>• This also applies to devices added later.<br>• Offline operation, support for resource constrained devices: a gateway can be used to provide offline operation functionality to resource constrained devices. The gateway can perform tasks on behalf of the device, for example, communicate with Cloud IoT Core, connect to the Internet, and authenticate credentials. |
| b) | **Device management** | • Asset tracking in real-time.<br>• Device Manager can configure and manage individual devices (coarse-granular).<br>• Can be controlled via console or through programs.<br>• Manages the (logical) connections of each device.<br>• Can be used to remotely control the device from the cloud.<br>• REST APIs can be used to automate device registration, provisioning, and operation at scale. The APIs can also be used to retrieve and update device properties or status, even when the devices are not connected. |
| c) | **Deployment, provision of software** | • Device updates can be distributed with Cloud IoT Core.<br>• ML model or other files/objects can be distributed.<br>• Mender OTA software update management with resilience and rollback |

| T6. Security | | |
|---|---|---|
| | | **Strict industry standard security protocols** to protect business data |
| | | **Device authentication** (based on the identity of the device) |
| | | **End-to-end security:** By authenticating with asymmetric keys via TLS 1.2, end-to-end security is realized. Certificates signed by a certificate authority can be used to verify |

| T6. Security | |
|---|---|
| | device ownership. Devices that support Cloud IoT Core security requirements can provide full security. |
| | **Role-level access control:** IAM roles can be applied to device registries to control user access to devices and data. |

| T7. Data protection | |
|---|---|
| | • Control over what happens to the data<br>• No use of customer data for advertising purposes<br>• The location of the data storage is disclosed.<br>• Assurance that government agencies will never be granted "backdoor" access to the data or to the servers where the data is stored. |

| T8. Cloud support | |
|---|---|
| | • Based on Google Cloud, e.g., to manage/remotely control devices.<br>• The service is "serverless" and requires no prior software installation. |

| T9. Scalability | |
|---|---|
| | • Protocol endpoints that ensure smooth data ingestion under all conditions thanks to automatic load balancing and horizontal scaling.<br>• Cloud IoT Core runs on Google's serverless infrastructure, which responds immediately to changes through automatic scaling.<br>• Thanks to Google Cloud Platform's horizontal scaling, instant scaling is possible without limitations. |

| T10. Digital twins / Asset Administration Shells | | |
|---|---|---|
| a) | **Digital twins** | If applicable, device simulator, for which, however, only little information is available. |
| b) | **AAS used for IoT devices** | *No information available* (might be represented as REST API in the form of own interfaces) |
| c) | **AAS used for edge devices** | *No information available* (might be represented as REST API in the form of own interfaces) |

| T11. Data management and data analysis | |
|---|---|
| | • Cloud with subscription function (publish/subscribe), retains data for seven days.<br>• Big Data analytics and ML services from Google. These include Cloud Dataflow, BigQuery, Cloud Bigtable, Google Data Studio or BI tools from partners.<br>• Notifications can also be set up based on measurement thresholds, e.g. for devices not to exceed a preset billable data limit. |

| T12. Offered AI methods | |
|---|---|
| | • ML services from Google or BI tools from partners.<br>• AI building blocks allow developers to extend applications with machine vision, speech input/output, conversational, and structured data capabilities.<br>• Training data available: AutoML provides developers and data analysts with rapid training of their own models. Google Cloud AI products are trained with some of the world's largest datasets, continuously improved, making the benefits of machine learning easily accessible.<br>• Visual Recognition, Video Processing, Dialogflow, Cloud Text-to-Speech, Cloud Speech-to-Text, Speech Translation, Natural Language Processing, AutoML Tables, AutoML Vision, AutoML Video Intelligence, AutoML Natural Language, AutoML Translation, AutoML Tables, Recommendations AI, Cloud Inference API. |

| T12. Offered AI methods | |
|---|---|
| | • Kubeflow for portable ML pipelines<br>• TensorFlow, Tensor Processing Units (TPUs) and Tensor Flow Extended (TFX)<br>• Prepare/Preprocess: Dataprep, Dataflow, Dataproc, Big Query<br>• Data labeling service, Deep Learning VM Image, AI Platform Notebooks<br>• AI Platform prediction (Tensorflow, scikit-learn in the cloud).<br>• Explainable AI |

| T13. Openness and Extensibility | | |
|---|---|---|
| a) | **Store** | Google Cloud Marketplace or Google AI Hub (P&P components, P&P workflows, release functions) |
| b) | **App support for/by developers** | Cloud SDK based on Node.js, lots of documentation and examples, otherwise management by the stores |
| c) | **Use of "external" algorithms/data** | • Reuse of AI building blocks.<br>• Proprietary algorithms are likely, especially since Tensor Flow Enterprise is described as a code-based data science development environment and since Cloud IoT is described as very technical (program-heavy). |
| d) | **AI interfaces** | • AI-Building-Blocks<br>• Kubeflow |

| T14. Systematic Configurability | |
|---|---|
| | *No information available* |

| T15. Ecosystem support | | |
|---|---|---|
| a) | **"Multi-Sided" platform** | Not explicitly described, MQTT/REST interfaces are available |
| b) | **Open to third-party content** | Google partners or third-party/user solutions in stores |
| c) | **Reference to RAMI 4.0** | *No information available* |

| T16. Other technical abilities | |
|---|---|
| | • Real-time metrics with Stackdriver Monitoring<br>• Use Stackdriver Monitoring to create dashboards that show data such as the total number of active devices in a registry.<br>• All device logs in one place: view connection and error logs in Stackdriver Logging along with audit logs.<br>• Internal: REST APIs and MQTT<br>• Location detection via Google Maps |

| T17. References | |
|---|---|
| | • https://cloud.google.com/iot-core<br>• https://cloud.google.com/solutions/ai/<br>• https://cloud.google.com/products/ai/building-blocks<br>• https://cloud.google.com/ai-hub<br>• https://cloud.google.com/explainable-ai<br>• https://cloud.google.com/solutions/iot<br>• https://cloud.google.com/functions<br>• https://cloud.google.com/blog/products/iot-devices/quick-and-easy-way-set-end-end-iot-solution-google-cloud-platform<br>• https://cloud.google.com/iot/docs/concepts/overview |

## 3.11 Harting – MICA

| T1. Overview | | |
|---|---|---|
| a) | **Name of the platform** | MICA (Modular Industrial Computer Architecture) |
| b) | **Platform vendor or provider** | HARTING Technology Group, HARTING Deutschland GmbH, Minden, Germany |
| c) | **Vendor summary** | *"Quick and easy handling, robustness, flexibility, a long life cycle and fast application development - MICA is the best basis for your Industry 4.0 projects from machine monitoring to logistics and OEE."*[15] |
| d) | **Platform components** | MICA devices (seemingly exclusively), various containers or microservices. |
| e) | **Online marketplace platform** | *No information available* |
| f) | **Mobility platform** | Intelligent location-based services |
| g) | **B2B context** | Yes (Industry 4.0, production) |
| h) | **B2C context** | *No information available* |
| i) | **Platform users** | Machine operators, plant operators, administrators (low level) |
| j) | **Fields of application** | • Rail transport systems, intralogistics<br>• Permanent condition monitoring<br>• Inventory tracking, material tracking<br>• Energy management<br>• Product life cycle improvement<br>• Retrofitting |
| k) | **Market penetration** | Infotecs, M2MGo, Harting, Exelor, IIPco, Mesco, AIS Automation, akquinet |

| T2. License information | |
|---|---|
| | Commercial software package / license |

| T3. Protocols | |
|---|---|
| | • incl. Modbus, Modbus/TCP, EUROMAP 15, EUROMAP 63, MQTT, JSON, Rest, OPC-UA, IO-Link<br>• Extensible via „solution partners" in the „MICA.network" |

| T4. Edge support | |
|---|---|
| | Vendor statement: *"MICA combines industry-compatible hardware and open source-based software to perform decentralised tasks in the field. The MICA platform is based on a secure Linux system and the applications run in independent software containers. MICA hardware is robust, suitable for industrial use and installed in a compact IP67 aluminium housing. Depending on the application, different hardware modules and software apps can be combined from a modular system and expanded with their own hardware and software elements."*<br>Essentially, MICA devices are supported, i.e., Linux-based devices that can run LXC[16] containers and provide corresponding connectors (e.g., cloud-connector, TIKA-stack container). |

[15] Probably Overall Equiment Efficiency, but not further explained in the material. There is a hint on https://www.mica.network/mit-oee-kennzahlen-besser-investieren/

[16] https://linuxcontainers.org/

| T5. IIoT devices | | |
|---|---|---|
| a) | **Device connectivity** | See protocols (see also T3), in particular all devices are MICA devices |
| b) | **Device management** | Performed by the Device Management Container. Services provided: Discover, status monitoring, network configuration, OTA update, device configuration profiles. |
| c) | **Deployment, provision of software** | • Via Container upload to the devices<br>• Supported by the Device Management Container |

| T6. Security | |
|---|---|
| | • Authentication, encryption (OPENSSL), certificates, TLS-MQTT<br>• Secure encrypted data transmission<br>• The MICA platform is based on a secure Linux system.<br>• The protection includes five core elements<br>  ○ The protection of the MICA through a secure operating system<br>  ○ The protection of applications in the MICA<br>  ○ The use of secure protocols<br>  ○ An end-to-end encrypted data transmission<br>  ○ Securing of applications |

| T7. Data protection | |
|---|---|
| | See Security (T6). |

| T8. Cloud support | |
|---|---|
| | • MICA connects machines with cloud services *(„MICA verbindet Maschinen mit Cloud-Diensten“)*<br>• The documentation includes examples of applications whose data is sent to MS Azure. |

| T9. Scalability | |
|---|---|
| | Adopted by the Device Management Container, but limited to 50 devices. |

| T10. Digital twins / Asset Administration Shells | | |
|---|---|---|
| a) | **Digital twins** | *No information available* |
| b) | **AAS used for IoT devices** | *No information available* (potentially via interfaces, e.g. RPC and metrics via JSON) |
| c) | **AAS used for edge devices** | *No information available* (potentially via interfaces, e.g. RPC and metrics via JSON) |

| T11. Data management and data analysis | |
|---|---|
| | TIGK-stack container (time-series database, telemetry routing engine, stream analytics engine, dashboard) |

| T12. Offered AI methods | |
|---|---|
| | TIGK-stack container |

| T13. Openness and Extensibility | | |
|---|---|---|
| a) | **Store** | • Pre-configured „MICA solution packages“<br>• Prepared container |
| b) | **App support for/by developers** | Prepared container (see T13a) with programming languages and JSON RPC |

| T13. Openness and Extensibility | | |
|---|---|---|
| c) | **Use of "external" algorithms/data** | Through programming or use of own containers |
| d) | **AI interfaces** | *No information available* |

| T14. Systematic Configurability | |
|---|---|
| | "Mica Solution Packages", i.e., pre-configured solutions for specific application areas |

| T15. Ecosystem support | | |
|---|---|---|
| a) | **"Multi-Sided" platform** | In the context of available containers only with cloud services, but since no details are given, the platform could be connectable with any systems. |
| b) | **Open to third-party content** | • Focus on „solution partners" in the „MICA.network".<br>• There is also (possible in addition) the open developer community MICA-network. |
| c) | **Reference to RAMI 4.0** | *No information available* |

| T16. Other technical abilities |
|---|
| • RFID support<br>• Based on Linux and LXC container<br>• Microservices in the form of Python and Java containers<br>• Containers based on Node Red, busybox, Debian stretch<br>• Mobile/Location-based services for devices via GNSS, JSON RPC, Bluetooth<br>• Dashboard (depending on container) |

| T17. References |
|---|
| • PDF-Documents from https://www.harting.com<br>• https://www.harting.com/DE/en-gb/mica<br>• https://www.mica.network/<br>• https://www.harting.com/DE/de/downloadcenter?name=&download_type=All&market=All&product_category=733<br>• http://mica-container.com/ |

## 3.12 IBM - Watson IoT Suite

| T1. Overview | | |
|---|---|---|
| a) | **Name of the platform** | Watson IoT Platform |
| b) | **Platform vendor or provider** | IBM, USA |
| c) | **Vendor summary** | *„IBM Watson IoT Platform is a managed, cloud-hosted service designed to make it simple to derive value from your IoT devices. Watson IoT Platform and its additional add on services - Blockchain service and analytic service - enable organizations to capture and explore data for devices, equipment, and machines, and discover insights that can drive better decision-making.*<br><br>*Capture data in real time:*<br>*Process IoT data instantly to help identify valuable insights related to device behavior and operations in the field. Spot trends before they impact the bottom line.*<br><br>*Optimize operations and resources:*<br>*Reduce operational expense by understanding your IoT devices to operate them more effectively and efficiently. Visualize your IoT data to better plan your operations and increase productivity.*<br><br>*Increase revenue:*<br>*Use improved business insight and bidirectional communication with the end user to introduce innovative new products and services.*<br><br>*Analytics:*<br>*Enrich, augment and interact with your IoT data from the IoT Platform with analytics using simplified data ingestion and curation.*<br><br>*Blockchain Service:*<br>*Increase trust and transparency by enabling IoT assets to validate provenance and events in a trusted, immutable ledger with the blockchain service add-on. “* |
| d) | **Platform components** | • IBM Watson IoT Platform Connect<br>• IBM Watson IoT Platform Information Management<br>• IBM Watson IoT Platform Analytics<br>• IBM Watson IoT Platform Risk Management |
| e) | **Online marketplace platform** | Support of online marketplaces is mentioned for the platform in the future in the context of "enterprise" use. |
| f) | **Mobility platform** | Yes, support for mobility platforms is mentioned |
| g) | **B2B context** | Yes, focus on industrial customers or large-scale customers such as service providers. |
| h) | **B2C context** | End users (consumers) explicitly mentioned with specification of the possibility to process end user devices (data) with the Watson IoT platform. |
| i) | **Platform users** | • Enterprise IoT platforms and industry applications<br>• Enterprise users (non-industrial)<br>• End users (such as in the smart home sector) |
| j) | **Fields of application** | • Administration environment for managing and monitoring sensor data generated by technical objects from the Internet of Things<br>• Device management in IoT environments<br>• Customization and operation of cloud-based IoT business applications |

| T1. Overview | | |
|---|---|---|
| k) | **Market penetration** | • Global application by a wide range of users<br>• Widespread application by major customers |

| T2. License information | | |
|---|---|---|
| | | IBM Watson hardly uses any open source software and no information is given about licenses, except for proprietary licenses from IBM. |

| T3. Protocols | | |
|---|---|---|
| | | MQTT and other (native) protocols possible at IoT device level, connection via gateways. |

| T4. Edge support | | |
|---|---|---|
| a) | **Overview** | Within the IBM Watson IoT platform, edge devices are not named separately/explicitly. However, it can be assumed that edge devices used by customers can access the services of the platform or connected services from IBM in a similar way to generic "IoT devices". These services include within the framework of the Watson IoT platform:<br>• IBM Predictive Maintenance on Cloud<br>• IBM Predictive Quality on Cloud<br>• IBM Predictive Warranty on Cloud<br>• IBM Maximo Production Optimization<br>Assuming that edge devices of customers can access the services of the platform in a manner analogous to the "IoT Devices" mentioned in the platform, edge devices would be able to process the following tasks:<br>• Monitoring asset telemetry across edge devices using IBM Stream Analytics<br>• Behavioral monitoring and analysis of assets<br>• Predictive diagnostics for assets<br>• Contextualization of IoT device data |
| b) | **Communication** | No bidirectional communication mentioned, "only" forwarding of data to the IBM Cloud and its services, which then forward their results to further applications, such as visualization apps and/or business logic apps.<br>Gateways can be used to connect e.g. native protocols of "IoT Devices" with the platform |
| c) | **Memory usage** | Explicit use of storage capacities on edge devices is not mentioned in the platform description. Such "local" storage may be possible within the framework of the gateways provided in the platform. |
| d) | **Specific capabilities** | • Since edge devices are not explicitly used as part of the Watson IoT platform, it can only be stated here that the data from any IoT device connected to the platform, i.e. also edge devices, can be analyzed via IBM's cloud/analytics components and the information derived from this is passed on to the visualization and business logic applications connected to the platform.<br>• The scope of functions thus corresponds to the scope and range of services (for example in the area of analysis) offered by IBM. |

| T5. IIoT devices | | |
|---|---|---|
| a) | **Device connectivity** | • Wide range of common protocol options for device and enterprise applications |

| T5. IIoT devices | | |
|---|---|---|
| | | • Ability to integrate 3rd party devices |
| b) | **Device management** | • Edge computing does not appear to be a part of the platform, only "IoT Devices" are mentioned.<br>• IBM offers a separate solution for managing edge devices: IBM Edge Computing Manager for Devices.<br>• Remote update of device software is not explicitly mentioned. |
| c) | **Deployment, provision of software** | • REST<br>• Software-as-a-Service (SaaS)<br>• Wide range of proprietary (internal) software for the platform<br>• Offer of apps for administrative tasks (dashboards)<br>• Development options for custom software are not explicitly mentioned, but customers can define their own interfaces and functions via MQTT or using the IBM Watson IoT Platform HTTP Messaging API. |

| T6. Security | |
|---|---|
| | The high security level of the IBM Cloud behind the Watson IoT platform is used as a unique selling point or a very strong selling point. The Watson IoT platform itself covers the following security aspects: |
| | **User and user rights management:** Extensive options for managing users and user rights. |
| | **Security techniques within the platform:**<br>• Secure connection of assets to hardware or software connectivity solutions.<br>• Secure data storage and software (encryption, authorization)<br>• Identity management and access control<br>• Secure integration of hardware via unique hardware identifiers |

| T7. Data protection | |
|---|---|
| | • The Watson IoT platform is internally based on the highest security standards and has been audited by third parties to ensure compliance specifically with ISO 27001 (certified, audited).<br>• The Watson IoT platform provides role configuration and management so that controls can be defined by users, applications and gateways.<br>• In the context of IBM's advanced security capabilities that extend Watson IBM with Threat Intelligence for IoT, clients can now visualize critical risks in the IoT landscape and create policy-driven mitigations to automate operational responses to IoT devices at scale. |

| T8. Cloud support | |
|---|---|
| | • Cloud based, uses Data Lake in the IBM Cloud<br>• Cloudant NoSQL DB<br>• IBM Event Streams for IBM Cloud<br>• Db2 Warehouse on Cloud<br>• Databases for PostgreSQL |

| T9. Scalability | |
|---|---|
| | Scaling (number of devices, etc.) and data usage can be customized, dynamically. |

| T10. Digital twins / Asset Administration Shells | | |
|---|---|---|
| a) | **Digital twins** | • Digital Twins are not part of the IBM Watson IoT platform or are not mentioned as such. |

| T10. Digital twins / Asset Administration Shells | | |
|---|---|---|
| | | • However, the IBM Watson IoT platform offers the possibility to simulate IoT devices or device networks. This simulation can be performed for existing IoT devices or for testing or integrating new IoT devices. This corresponds to the core functionalities of a digital twin, but IBM explicitly does not refer to it as such. |
| b) | **AAS used for IoT devices** | *No information available* |
| c) | **AAS used for edge devices** | *No information available* |

| T11. Data management and data analysis | |
|---|---|
| | • Data management happens in IBM Data Lake<br>• Collection, monitoring and analysis of data is possible almost in real time<br>• Visualization of data and data analysis<br>• Extensive querying of data<br>• Text analysis<br>• Natural Language Processing<br>• Video and image data analysis |

| T12. Offered AI methods | |
|---|---|
| | • Machine learning (supervised, unsupervised) for anomaly detection.<br>• Analysis of asset telemetry using the Stream Analytics component, which offers a wide range of analysis options.<br>• Text analysis |

| T13. Openness and Extensibility | | |
|---|---|---|
| a) | **Store** | IBM itself has a store for the multitude of its offerings. The IBM Watson IoT platform itself does not offer such a store. Rather, additional services from IBM that can be integrated via the platform are offered in IBM's own Product Store. The store does not contain any third-party application or service offerings. |
| b) | **App support for/by developers** | • There is a GitHub for IBM Edge Development, but this is currently archived and therefore no longer active.<br>• For development/use of IBM's own applications, IBM provides a number of APIs and extensive documentation and sample materials.<br>• Third-party application development outside of IBM is not actively supported. |
| c) | **Use of "external" algorithms/data** | • External data can be used (analysis in the IBM Cloud).<br>• The use of external algorithms is not provided. |
| d) | **AI interfaces** | • Apart from the platform's own AI components, no information is provided on the integration of other (customer-owned) AI components.<br>• The integration of customers' own AI components appears to be severely restricted by the limitation of the customers' ability to use their own software in the platform. |

| T14. Systematic Configurability | |
|---|---|
| | Customers can create their own platform configurations with restrictions. |

| T15. Ecosystem support | | |
|---|---|---|
| a) | **"Multi-Sided" platform** | The formation of ecosystems appears to be difficult because the platform explicitly does not support the integration of other platforms. In IBM's own area of services and offerings, "local" ecosystems appear possible. |
| b) | **Open to third-party content** | • Allows configuration of GUIs and analysis and event functions, but does not provide general APIs or SDKs.<br>• Provides an HTTP messaging API to allow customers to create configuration of custom functions. |
| c) | **Reference to RAMI 4.0** | *No information available* |

| T16. Other technical abilities | |
|---|---|
| | Blockchain: The IBM Watson IoT platform uses/used the IBM Blockchain platform to enable IoT devices to securely transact with each other.<br>However, the blockchain functionality is currently no longer actively supported by IBM. |

| T17. References | |
|---|---|
| | • Overview on the IBM Watson IoT platform: https://www.ibm.com/de-de/internet-of-things/solutions/iot-platform/watson-iot-platform<br>• Architecture of the IBM Watson IoT platform: https://www.ibm.com/support/knowledgecenter/SSQP8H/iot/overview/architecture.html<br>• IBM Watson IoT Platform IoT Data Lifecycle: https://www.ibm.com/support/knowledgecenter/SSQP8H/iot/overview/iot_data_lifecycle.html<br>• Overview on IBM Watson IoT Platform Analytics: https://www.ibm.com/support/knowledgecenter/SSQP8H/iot/analytics/as_overview.html<br>• IBM Watson IoT Platform Analytics Anomaly detection: https://www.ibm.com/support/knowledgecenter/SSQP8H/iot/analytics/as_detect_predict.html<br>• IBM Edge Computing Manager for Devices: https://www.ibm.com/support/knowledgecenter/en/SSFKVV_4.0/getting_started/edge_computing.html<br>• IBM Maximo: https://www.ibm.com/us-en/marketplace/production-optimization<br>• Overview on IBM Maximo Asset Monitor: https://www.ibm.com/support/knowledgecenter/SSQR84_monitor/iot/overview/overview_mon.html<br>• IoT Device Simulation in IBM Watson IoT Platform: https://www.ibm.com/support/knowledgecenter/SSQP8H/iot/platform/reference/dashboard/device_sim.html<br>• IBM Cloud Computing Security: https://www.ibm.com/cloud-computing/de/de/security.html<br>• IBM Edge Analytics GitHub: https://github.com/ibm-watson-iot/edge-analytics-samples/projects<br>• Presentation on a cooperation of Cisco and IBM regarding the integration of edge devices with IBM cloud services: https://www.cisco.com/c/dam/m/ro_ro/events/2016/ciscoconnect/img/presentations/IBM.pdf |

| T17. References | |
|---|---|
| | • Blockchains in the IBM Watson IoT Platform: https://www.ibm.com/support/knowledgecenter/SSQP8H/iot/blockchain/index.html<br>• Github repository for examples: https://github.com/ibm-watson-iot/edge-analytics-samples |

## 3.13 Microsoft - Azure IoT Suite

| T1. Overview | | |
|---|---|---|
| a) | **Name of the platform** | Microsoft Azure IoT Suite |
| b) | **Platform vendor or provider** | Microsoft, USA |
| c) | **Vendor summary** | *"Azure plays a very important role in our customer's IoT solutions by providing:*<br>• *Globally available, infinitely scalable and cost effective services for IoT devices and secure connectivity using industry standard protocols and security approaches.*<br>• *A central place to collect telemetry from, send commands to, and manage geographically distributed devices.*<br>• *Advanced analytics that help customers unlock key insights from their IoT data, and even monitor for important conditions over telemetry streams from millions of concurrent devices in real time.*<br>• *A rich set of services required to realize the value in IoT, and open source client libraries that make it simple to interact with the Azure IoT Suite.*<br>*The foundation for Azure IoT Suite pre-configured solutions, which are engineered to help customers quickly provision and realize business value from IoT. The Azure IoT Suite takes care of deploying and orchestrating the various services to give you a complete end to end solution.*<br>*We also provide the Azure IoT Device SDK, an open source set of client libraries that run on a variety of operating systems and devices. These libraries are a convenience, but are not required to interact with the Azure IoT Suite, and you can modify them to meet your needs."* |
| d) | **Platform components** | • Azure IoT IoT Hub<br>• Azure IoT Stream Analytics<br>• Azure IoT Storage<br>• Azure IoT Edge |
| e) | **Online marketplace platform** | The platform supports online marketplace platforms. |
| f) | **Mobility platform** | The platform supports mobility platforms. |
| g) | **B2B context** | Yes, focus on industrial customers or key accounts such as service providers. |
| h) | **B2C context** | *No information available* |
| i) | **Platform users** | • IoT platforms and industry applications for enterprises<br>• Development capabilities of customer's own software are explicitly mentioned, source code for Azure IoT apps is provided for further development by customers.<br>• Offers solutions for general "IoT platforms". |
| j) | **Fields of application** | • Administration environment for managing and monitoring sensor data generated by technical objects from the Internet of Things.<br>• Customization and operation of cloud-based IoT business applications. |
| k) | **Market penetration** | • Global application through a wide range of users<br>• Widespread application by major customers |

| T2. License information | |
|---|---|
| | Open source software in Azure IoT Suite uses MIT license. |

| T3. Protocols | |
|---|---|
| | • TLS, MQTT, AMQP<br>• IP addressing (Use of IP prefixes for connection control of individual devices)<br>• Connect native, on-premises, protocols from assets to the Azure IoT Suite using Microsoft Azure IoT Protocol Gateways. |

| T4. Edge support | | |
|---|---|---|
| a) | **Overview** | Edge computing is available as an essential part of the Azure IoT Suite in the form of the dedicated Azure IoT Edge component: *"Azure IoT Edge is a fully managed service built on Azure IoT Hub. Deploy your cloud workloads—artificial intelligence, Azure and third-party services, or your own business logic—to run on Internet of Things (IoT) edge devices via standard containers. By moving certain workloads to the edge of the network, your devices spend less time communicating with the cloud, react more quickly to local changes, and operate reliably even in extended offline periods."*<br>Other components that are provided specifically for the realization of edge capabilities are:<br>• Azure Vision Machine Learning: This component provides ML techniques for building models from image data that can then be used on edge devices.<br>• Azure Stack Edge: This component is a hardware solution that combines AI techniques and communication capabilities in an IoT system.<br>• "Project Brainwave": This component is a software solution that provides Deep Learning for Edge devices. |
| b) | **Communication** | • Edge devices in Azure IoT Suite communicate bi-directionally using the above protocols.<br>• Native protocols of assets and edge devices can be connected via Azure IoT Protocol Gateways. |
| c) | **Memory usage** | • Both local storage on edge devices and use of cloud storage (Azure Cloud) is supported.<br>• Pre-processing of data on edge devices that can then be used/stored in Azure Cloud is possible. |
| d) | **Specific capabilities** | • Deployment of custom AI models and AI algorithms via Azure IoT Edge component.<br>• Focus on AI methods that use image processing, implemented using Azure Vision Machine Learning: *"Deploy models built and trained in the cloud and run them on-premises. For example, if you deploy a predictive model to a factory camera to test for quality control and an issue is detected, IoT Edge triggers an alert and processes the data locally or sends it to the cloud for further analysis."*<br>• Focus on edge computing to achieve near real-time responses from edge devices.<br>• Using the Azure Stack Edge component, the following capabilities are optimized for edge devices:<br>  ○ Inference with Azure Machine Learning – *"With Azure Stack Edge, you can run ML models to get quick results that can be* |

| T4. Edge support | | |
|---|---|---|
| | | *acted on before the data is sent to the cloud. The full data set can optionally be transferred to continue to retrain and improve your ML models."*<br>○ Preprocess data – *"Transform data before sending it to Azure to create a more actionable dataset. Preprocessing can be used to:*<br>▪ *Aggregate data.*<br>▪ *Modify data, for example to remove personal data.*<br>▪ *Subset data to optimize storage and bandwidth, or for further analysis.*<br>▪ *Analyze and react to IoT Events."* |

| T5. IIoT devices | | |
|---|---|---|
| a) | **Device connectivity** | • Wide range of all common protocol options for device and enterprise applications<br>• Ability to integrate 3rd party devices<br>• Integration of different protocols and systems |
| b) | **Device management** | • Edge computing as an (extensive) component of Azure IoT Edge<br>• Secure onboarding and offboarding (insertion, removal) of devices of various types<br>• Remote configuration of devices<br>• Remote update of device software<br>• Telemetry management of devices |
| c) | **Deployment, provision of software** | • REST<br>• Software-as-a Service (SaaS)<br>• Wide range of proprietary (internal) software for the platform<br>• Offer of apps for administrative tasks<br>• Provision of source code for further development of apps by customers, source code is available via own GitHub repository<br>• Deployment to edge devices is done by using containers |

| T6. Security | | |
|---|---|---|
| | | **User and user rights management:** Extensive options for user and user rights management |
| | | **Security techniques within the platform:**<br>• Secure connection of assets to hardware or software connectivity solutions.<br>• Secure data storage and software (encryption, authorization)<br>• Identity management and access control<br>• Device authentication using X.509 CA certificates<br>• X.509 security standard in the IoT Hub<br>• X.509 CA certified security concepts |
| | | **Azure IoT Edge Security techniques:**<br>• Certificate-based authentication<br>• Edge devices must have unique certificate identities<br>• Application of the principle of least privilege<br>• Permissions to sign certificates and RBAC.<br>• Software attestation:<br>○ Static attestation<br>○ Runtime attestation<br>○ Software attestation<br>• Hardware root of trust: |

| T6. Security | |
|---|---|
| | ○ Trusted Platform Module (ISO/IEC 11889)<br>○ Trusted Computing Group's Device Identifier Composition Engine (DICE)<br>○ Secure enclave technologies: TrustZones, Software Guard Extensions (SGX) |

| T7. Data protection | |
|---|---|
| | **Technical-organizational measures:**<br>• Secure device authentication: "A unique identity key or security token, or an on-device X.509 certificate. Appropriate method to use security tokens based on the chosen protocol (MQTT, AMQP, or HTTPS)."<br>• Secure device communication: "IoT Hub secures the connection to the devices using Transport Layer Security (TLS) standard, supporting version 1.2 and 1.0. TLS 1.2 ensures maximum security."<br>• Secure service communication: "Azure storage or Event Hubs using only the TLS protocol."<br>• Access controls<br>• Cryptography<br>• TrustZones<br>Overview of compliance standards on the website (see sources) |

| T8. Cloud support | |
|---|---|
| | • Cloud-based, leverages Azure IoT Storage cloud services<br>• Provides object store<br>• Local storage for IaaS workloads<br>• Storage for synchronous message queuing<br>• Storage for structured NoSQL data<br>• Azure Cloud storage usage for Big Data analytics on the aggregated device data |

| T9. Scalability | |
|---|---|
| | • Scaling (number of devices, etc.) and data usage can be customized dynamically.<br>• Volume of cloud storage used can be dynamically adjusted by customers. |

| T10. Digital twins / Asset Administration Shells | | |
|---|---|---|
| a) | **Digital twins** | Azure Digital Twins are offered as a way to simulate, optimize, monitor, etc. assets. The use of Digital Twins is not limited to physical devices, but also includes modeling of people, places, business entities, i.e. entities (as defined in the AAS concept) in general.<br>Azure Digital Twins can be used for all common applications of Digital Twins, e.g. simulation, optimization, development, monitoring, authentication, visualization, etc. The creation and use of Digital Twins are part of the Microsoft Azure offering and as such are also part of the Azure IoT Suite offering.<br>Azure Digital Twins offer a special way of modeling and visualizing data/information: *"Modelling of the relationships between people, places, and devices using the spatial intelligence graph—a virtual representation of a physical environment."*<br>The modeling and use of Digital Twins is supported by Azure through the provision of its own modeling language DTDL (Digital Twin Definition Language) as well as its own SDK. |
| b) | **AAS used for IoT devices** | The modeling of a Digital Twin in Azure is (partially) similar to the concept of the AAS. Excerpt from the model description of an Azure Digital Twin - "Azure Digital Twin Model Definition: |

| T10. Digital twins / Asset Administration Shells | | |
|---|---|---|
| | | • *"Within a model definition, the top-level code item is an interface. This encapsulates the entire model, and the rest of the model is defined within the interface.*<br>• *A DTDL (Digital Twin Definition Language) model interface may contain zero, one, or many of each of the following fields*<br>  ○ *Property - Properties are data fields that represent the state of an entity (like the properties in many object-oriented programming languages).*<br>  ○ *Telemetry - Telemetry fields represent measurements or events, and are often used to describe device sensor readings.*<br>  ○ *Component - Components allow to build a model interface as an assembly of other interfaces. An example of a component is a frontCamera interface (and another component interface backCamera) that are used in defining a model for a phone. You must first define an interface for frontCamera as though it were its own model, and then you can reference it when defining Phone.*<br>*Relationship - Relationships represent how a digital twin can be involved with other digital twins. Relationships can represent different semantic meanings, such as contains ('floor contains room'), cools ('HVAC cools room'), isBilledTo ('compressor is billed to user'), etc. Relationships allow the solution to provide a graph of interrelated entities."* |
| c) | **AAS used for edge devices** | See T10b. |

| T11. Data management and data analysis | | |
|---|---|---|
| | | • Data management takes place in Azure IoT Storage and Azure IoT Stream Analytics<br>• Collecting, monitoring and analyzing data is possible in near real-time<br>• Visualization of data and data analysis<br>• Query of data (among others) via SQL<br>• Possibility of using temporal analysis (temporal logic) to control or optimize, for example, process flows (scheduling)<br>• Visualization of data/information from Digital Twins, or alliances of Digital Twins in a "Spatial intelligence graph". |

| T12. Offered AI methods | | |
|---|---|---|
| | | • Part of the "Azure IoT Stream Analytics" offering<br>• Machine learning for anomaly detection<br>• Sentiment analysis with Azure Machine Learning Studio<br>• Task scaling with Machine Learning Studio features<br>• Dedicated component "Project Brainwave":"*Project Brainwave is a deep learning platform for real-time AI inference in the cloud and on the edge. A soft Neural Processing Unit (NPU), based on a high-performance field-programmable gate array (FPGA), accelerates deep neural network (DNN) inferencing, with applications in computer vision and natural language processing. Project Brainwave is transforming computing by augmenting CPUs with an interconnected and configurable compute layer composed of programmable silicon.*" Using the capabilities of the "Brainwave" component to:<br>  ○ Optimizing the programming of FPGA's (Field programmable gate-arrays) |

| T12. Offered AI methods | |
|---|---|
| | ○ Use in the Azure Stack Edge: *"Stack Edge is an AI-enabled edge computing device with network data transfer capabilities. Azure Stack Edge is a Hardware-as-a-service solution. Microsoft ships you a cloud-managed device with a built-in Field Programmable Gate Array (FPGA) that enables accelerated AI-inferencing and has all the capabilities of a network storage gateway.* " |

| T13. Openness and Extensibility | | |
|---|---|---|
| a) | **Store** | Azure IoT Suite provides apps and services in the following (IoT relevant) categories within the Azure Marketplace:<br>• Data Analytics and Visualization<br>• IoT Core Services<br>• IoT Edge Modules<br>• IoT Solutions |
| b) | **App support for/by developers** | Azure IoT Suite supports app development and management by:<br>• Providing a variety of APIs and SDKs<br>• Providing extensive training materials and tutorials (templates, sample apps, etc.)<br>• The provision of a GitHub repository for developers |
| c) | **Use of "external" algorithms/data** | • Support development of custom edge applications by customers and third parties.<br>• Create and deploy customer-owned AI models and algorithms, deploying to edge devices using containers.<br>• Creation of customer-owned business logics for use in Azure IoT Suite.<br>• Integration of third-party data possible |
| d) | **AI interfaces** | The Project Brainwave component provides AI interfaces. |

| T14. Systematic Configurability | |
|---|---|
| | Customers can create their own platform configurations. |

| T15. Ecosystem support | | |
|---|---|---|
| a) | **"Multi-Sided" platform** | Yes, allows the integration of other platforms or does not explicitly exclude them. |
| b) | **Open to third-party content** | • Allows the development of custom application configurations based on the provided source codes of Azure IoT Apps.<br>• Provides SDKs for the development of customer's own applications |
| c) | **Reference to RAMI 4.0** | *No information available* |

| T16. Other technical abilities | |
|---|---|
| | Based on container technology |

| T17. References | |
|---|---|
| | • Overview of Azure IoT Hub: https://docs.microsoft.com/en-us/azure/iot-hub/<br>• Azure Stream Analytics: https://docs.microsoft.com/en-us/azure/stream-analytics/<br>• Memory usage in Azure IoT Suite: https://docs.microsoft.com/en-us/azure/storage/<br>• Azure Git IoT Device SDK: |

**T17. References**

https://github.com/Azure/azure-iot-sdks

- Azure Vision AI Dev Kit: https://azure.github.io/Vision-AI-DevKit-Pages
- Azure Digital Twins: https://azure.microsoft.com/en-us/services/digital-twins
- Azure Digital Twins documentation: https://docs.microsoft.com/en-us/azure/digital-twins
- Azure Digital Twins APIs and SDKs: https://docs.microsoft.com/en-us/azure/digital-twins/how-to-use-apis-sdks
- Azure Digital Twin Model: https://docs.microsoft.com/en-us/azure/digital-twins/concepts-models
- Azure IoT Edge component: https://azure.microsoft.com/en-us/services/iot-edge
- Visual ML (for Azure IoT): https://azure.github.io/Vision-AI-DevKit-Pages
- Azure Marketplace: https://azuremarketplace.microsoft.com/en-us/marketplace/apps/category/internet-of-things?page=1&subcategories=iot-edge-modules
- Security in Azure IoT Edge: https://docs.microsoft.com/en-us/azure/iot-edge/security
- Projekt Brainwave (usage in Azure IoT Suite): https://www.microsoft.com/en-us/research/project/project-brainwave
- Azure IoT Stack Edge component: https://docs.microsoft.com/en-us/azure/databox-online/azure-stack-edge-overview
- ML für FPGAs (in Azure): https://docs.microsoft.com/en-us/azure/machine-learning/how-to-deploy-fpga-web-service
- Github: https://github.com/Azure/azure-iot-sdks
- Compliance: https://docs.microsoft.com/de-de/azure/compliance/

## 3.14 Oracle – Oracle Cloud IoT

| T1. Overview | | |
|---|---|---|
| a) | **Name of the platform** | Oracle Internet of Things Cloud Service |
| b) | **Platform vendor or provider** | Oracle, USA |
| c) | **Vendor summary** | *„Oracle Internet of Things (IoT) Cloud Service is a managed Platform as a Service (PaaS) cloud-based offering. Oracle Internet of Things Cloud Service provides you real-time analysis tools that let you correlate, aggregate, and filter incoming data streams. It also provides you built in integrations that allow the automatic synchronization of data streams with Oracle Business Intelligence Cloud Service. Ready-to-use IoT SaaS solutions for remote asset maintenance, Industry 4.0, smart manufacturing, connected logistics, worker safety monitoring, and connected customer experience help organizations achieve their vision of digital transformation across the complete enterprise.*<br><br>*Built-in integrations and extensibility features enable you to extend your business applications—such as ERP, SCM, customer experience, and HCM—with rich, real-time insights from streaming IoT data to improve efficiency and derive more value from your existing business applications.*<br><br>*Oracle IoT solutions are supported by a large ecosystem of device OEMs, device integrators, network service providers, and system integrators. “* |
| d) | **Platform components** | • Oracle Internet of Things Production Monitoring Cloud Service<br>• Oracle Internet of Things Asset Monitoring Cloud Service<br>• Oracle Internet of Things Fleet Monitoring Cloud Service<br>• Oracle Internet of Things Connected Worker Cloud Service |
| e) | **Online marketplace platform** | Yes, the Asset Monitoring, Fleet Monitoring and Connected Worker components are strongly targeted at the logistics and retail sectors. |
| f) | **Mobility platform** | Conditional, the Fleet Monitoring component can be applied here |
| g) | **B2B context** | Yes, the platform is focused on B2B. |
| h) | **B2C context** | No direct focus on end users (consumers) |
| i) | **Platform users** | • IoT platforms and industry applications for enterprises<br>• Focus on industrial customers |
| j) | **Fields of application** | • Administration environment for managing and monitoring sensor data generated by technical objects from the Internet of Things<br>• Fleet management<br>• Strong focus on efficiency optimization |
| k) | **Market penetration** | • Global application through a wide range of users<br>• Widespread application by major customers<br>• Large network of "ecosystem partners" (device OEMs, device integrators, network service providers, and system integrators). |

| T2. License information | | |
|---|---|---|
| | | • Proprietary licenses from Oracle<br>• Proprietary licenses of SPARC<br>• No mention of open source licenses |

| T3. Protocols | | |
|---|---|---|
| | | • HTTPs and MQTT<br>• Legacy and other protocols via Oracle IoT Gateway: *"A device that sends data over a non-HTTPS or TCP/IP protocol or interface, such as Bluetooth, Zigbee, I2C, or GPIO, can only communicate with Oracle IoT Cloud Service via a gateway device that is already connected to Oracle IoT Cloud Service. The gateway device must have the Oracle IoT Cloud Service Gateway already configured in it."* |

| T4. Edge support | | |
|---|---|---|
| a) | **Overview** | Edge devices are currently not treated separately in the Oracle IoT production environment, but are seen as all other IoT devices and can access all services available in the Oracle IoT platform just like them.<br>However, there are some functionalities that relate directly to edge devices:<br>• Edge devices can be configured and controlled via "Device Policies": *"Oracle has simplified edge computing implementation on Oracle Internet of Things Cloud Service by letting you create and modify policies externally from the device application. You do not need to write or compile any code. Instead, you create policies on the Management Console that define the data to collect, the data computation(s) to perform, and the frequency of data transmission. The policy instructs the edge device to compile the data and send it to the central server at a defined interval."*<br>• The implementation of Digital Twins in Oracle IoT considers requirements and advantages of edge computing: *„The semantic model lets you specify the normal operating range of an attribute. This results in a simpler implementation of edge computing. The business rules that you declaratively define on top of the complex event processing (CEP) engine in Oracle IoT Cloud Service can be automatically invoked at the edge of the IoT network."* |
| b) | **Communication** | • Bidirectional communication between Oracle Cloud or its services and edge devices is possible (data streaming, command issuing).<br>• Gateways can be used to connect e.g. native protocols of IoT devices with the platform. |
| c) | **Memory usage** | • Edge devices can use local storage and optionally connect to Oracle cloud storage services.<br>• Preprocessing of data on edge devices possible |
| d) | **Specific capabilities** | Use of semantic models on edge devices: *"Compared to the typical approach of using efficient protocols such as MQTT, a semantic model significantly reduces the cost of network bandwidth by automating statistical modeling at the edge."* |

| T5. IIoT devices | | |
|---|---|---|
| a) | **Device connectivity** | • Wide range of all common protocol options for device and enterprise applications<br>• Ability to integrate 3rd party devices |
| b) | **Device management** | • Edge computing is not explicitly mentioned<br>• Continuous device monitoring in real time |

| T5. IIoT devices | | |
|---|---|---|
| | | • Registration, organization, monitoring and remote management of connected IoT devices<br>• Central deployment of software updates<br>• KPI definition for devices and their monitoring<br>• Performance analysis based on KPIs<br>• Remote execution of actions on devices |
| c) | **Deployment, provision of software** | • REST<br>• Software-as-a-Service (SaaS)<br>• Wide range of Oracle web services that can be used platform-wide<br>• Offers apps for administrative tasks (dashboards, visualizations)<br>• Deployment of customer-specific AI components, conditionally possible due to the extensive configuration of Oracle Services in this area.<br>• "On the fly" deployment of completely custom AI components is conditionally possible via the use of REST APIs to connect these components to Oracle services. |

| T6. Security | | |
|---|---|---|
| | | **User and user rights management:**<br>• Extensive options for the management of users and user rights<br>• Role-based access is forced |
| | | **Security techniques within the platform:**<br>• Secure data storage and software (encryption, authorization).<br>• Role-based access restrictions<br>• Proof of data" checks<br>• Transport level security<br>• Unique device IDs |

| T7. Data protection | | |
|---|---|---|
| | | See Security (T6). |

| T8. Cloud support | | |
|---|---|---|
| | | Oracle Cloud<br>• Oracle Inventory Cloud<br>• Oracle Service Cloud<br>• Oracle Product Management Cloud<br>• Oracle CX Cloud |

| T9. Scalability | | |
|---|---|---|
| | | The platform can be scaled according to the customer's needs (data volume, number of devices, etc.) |

| T10. Digital twins / Asset Administration Shells | | |
|---|---|---|
| a) | **Digital twins** | Oracle IoT Digital Twins and Oracle IoT Digital Twins Simulation enable comprehensive use of Digital Twins in the Oracle IoT Platform: *"The Oracle IoT digital twin implementation has three pillars, each of which has its own use cases and advantages:*<br>• *Virtual Twin: In a virtual twin, Oracle's device virtualization feature creates a virtual representation of a physical device or an asset in the cloud. A virtual twin uses a JSON-based model that* |

| T10. Digital twins / Asset Administration Shells | | |
|---|---|---|
| | | *contains observed and desired attribute values and also uses a semantic model.*<br>• *Predictive Twin: In a predictive twin, the digital twin implementation builds an analytical or statistical model for prediction by using a machine-learning technique. It need not involve the original designers of the machine. It is different from the physics-based models that are static, complex, do not adapt to a constantly changing environment, and can be created only by the original designers of the machine.*<br>• *Twin Projections: In twin projections, the predictions and the insights integrate with back-end business applications, making IoT an integral part of business processes. For insight projections, Oracle IoT Cloud Service integrates with various products:*<br>  ○ *Native pre-built integrations with Oracle ERP and Oracle CX applications*<br>  ○ *Integration with 150 applications by using Oracle Integration Cloud Service (ICS)*<br>  ○ *Integration using REST API libraries*<br>*Oracle IoT Digital Twin Simulator: The IoT digital twin simulator lets you create simulated devices for your environment without the need to connect and set up hardware. You can generate configurable live data, alerts, and events for these simulated devices. Using the IoT digital twin simulator, you can create simulation models and then use them to create simulated device instances. The IoT digital twin simulator also provides ready-to-use simulation models that you can use to create simulated devices."* |
| b) | **AAS used for IoT devices** | Approach of modeling Digital Twins in Oracle IoT is similar to the concept of AAS. |
| c) | **AAS used for edge devices** | See T10b. |

| T11. Data management and data analysis | |
|---|---|
| | • Extensive capabilities for collecting, monitoring and analyzing data is in real time, realized in dedicated data analysis component for production, assets (machines), fleets, employees.<br>• Visualization of data and data analysis<br>• Extensive functions for customization of data streams<br>• Extensive options for customer definition of parameters (e.g. KPIs) that are used in data analysis<br>• "No code" environment for creating data analysis instructions |

| T12. Offered AI methods | |
|---|---|
| | • Comprehensive data analysis capabilities<br>• Complex event processing (CEP) engine in Oracle IoT Cloud Service<br>• Domain-specific AI methods and models for: Failure prediction, event detection, anomaly detection, device behavior prediction based on machine learning |

| T13. Openness and Extensibility | | |
|---|---|---|
| a) | **Store** | No store for apps or services. No offering of third-party apps or services. Oracle only offers its own services. |

| T13. Openness and Extensibility | | |
|---|---|---|
| b) | **App support for/by developers** | • Extensive documentation and tutorials<br>• Provision of APIs: "REST APIs are available for the application, device model, device resource, and messages components of the Oracle Internet of Things Cloud Service. Requests to these REST APIs are protected through OAuth 2.0 protocol." |
| c) | **Use of "external" algorithms/data** | • External data can be used (analysis in Oracle Cloud).<br>• Oracle IoT Cloud Service uses native Spark Java APIs for analytics purposes. Developers can use the Batch and Streaming Spark APIs to create their own analytics logic. |
| d) | **AI interfaces** | • The complex event processing (CEP) engine in the Oracle IoT Cloud provides interfaces.<br>• Oracle IoT Cloud Service uses native Spark Java APIs for analytics purposes. Developers can use the Batch and Streaming Spark APIs to create their own analytics logic. |

| T14. Systematic Configurability | | |
|---|---|---|
| | | • Customers can customize the applications provided.<br>• Customers can very easily create extensive "instructions" for the provided services (analysis, event handling). |

| T15. Ecosystem support | | |
|---|---|---|
| a) | **"Multi-Sided" platform** | • Conditional, networking with other IIoT platforms does not seem to be directly foreseen.<br>• There is the possibility of forming "Oracle internal" ecosystems through the "Oracle Ecosystem": *"Oracle IoT solutions are supported by a large ecosystem of device OEMs, device integrators, network service providers, and system integrators. Our device ecosystem includes large companies that produce hundreds of device types that are used across many different industries, as well as specialized device manufacturers. We partner with network service providers operating in cellular, LoRa, and narrowband IoT."* |
| b) | **Open to third-party content** | Oracle Internet of Things Cloud has a very large network of hardware and software vendors that are directly involved in the "Oracle IoT Cloud", however, there seems to be a demarcation that only these partners (their hardware, software) can be "seamlessly" integrated into the platform, so integration of "real" third-party content is rather not foreseen. |
| c) | **Reference to RAMI 4.0** | KPI support |

| T16. Other technical abilities | | |
|---|---|---|
| | | Oracle IoT digital twin Simulator |

| T17. References | | |
|---|---|---|
| | | • Oracle IoT platform overview:<br>  ○ https://www.oracle.com/internet-of-things<br>  ○ https://docs.oracle.com/en/cloud/paas/iot-cloud/index.html<br>  ○ https://www.oracle.com/internet-of-things/saas-applications.html<br>  ○ https://www.oracle.com/internet-of-things/iot-asset-monitoring-cloud.html<br>  ○ https://www.oracle.com/internet-of-things/iot-fleet-monitoring-cloud.html |

| T17. References |
| --- |
| ○ https://www.oracle.com/internet-of-things/iot-service-monitoring-for-connected-assets-cloud.html<br>○ https://www.oracle.com/internet-of-things/iot-production-monitoring-cloud.html<br>○ https://www.oracle.com/internet-of-things/iot-connected-worker-cloud.html<br>• Oracle partner network: https://www.oracle.com/internet-of-things/tech-partners<br>• API documentations:<br>○ https://docs.oracle.com/en/cloud/paas/iot-cloud/iotrq/index.html<br>○ https://docs.oracle.com/en/cloud/paas/iot-cloud/client-software-api-references.html<br>• Oracle Paper “Developing Applications with Oracle Internet of Things Cloud Service” https://docs.oracle.com/en/cloud/paas/iot-cloud/iotgs/developing-applications-oracle-internet-things-cloud-service.pdf |

## 3.15 PTC - ThingWorx

| T1. Overview | | |
|---|---|---|
| a) | **Name of the platform** | ThingWorx |
| b) | **Platform vendor or provider** | Parametric Technology GmbH, Germany |
| c) | **Vendor summary** | *„Damit das Industrial Internet of Things (IIoT) auch hält, was es verspricht, benötigen Sie eine Spezialplattform für die Industrie. Dank des umfangreichen Fachwissens aus fast 20 Jahren Innovationsarbeit im Bereich IoT ist PTC ThingWorx eine IIoT-Plattform mit der Funktionalität und Flexibilität, die für rasche Rentabilität notwendig sind. Zugleich bietet die Lösung die nötige Sicherheit und Skalierbarkeit, um IIoT-Lösungen auf das gesamte Unternehmen auszudehnen.*<br><br>*ThingWorx ist insofern einzigartig unter den IIoT-Plattformen, als es die umfassendsten kritischen IIoT-Funktionen abdeckt, und zwar sowohl nativ als auch über zuverlässige Integrationen für Partner wie Microsoft und Rockwell. Entdecken Sie die unverzichtbaren IIoT-Funktionen für Ihre digitale Transformation.*<br><br>*ThingWorx Manufacturing Apps und ThingWorx Service Apps beschleunigen nicht nur Pilotprojekte und Implementierungen, sondern ermöglichen auch einen skalierten betriebswirtschaftlichen Nutzen.“* (no corresponding English text found) |
| d) | **Platform components** | • Application Enablement Platform (AEP), “a design and runtime engine for IoT applications”<br>• ThingWorx Manufacturing<br>  ○ Asset Advisor (device management and monitoring)<br>  ○ Software Content Management<br>• ThingWorx Service Apps<br>  ○ Controls Advisor (data collection and analysis)<br>  ○ Operator Advisor (operator support through digital instructions, on-premise) |
| e) | **Online marketplace platform** | *No information available* |
| f) | **Mobility platform** | *No information available* |
| g) | **B2B context** | Yes, focus is on B2B |
| h) | **B2C context** | No |
| i) | **Platform users** | IIoT enterprise customers to create and extend software/services within their IIoT environments. |
| j) | **Fields of application** | • Development, customization and operation of software for edge and cloud-based IIoT enterprise applications.<br>• In addition to the development of new software for IIoT, also the integration of existing IIoT assets and software assets in further developments by ThingWorx Software. |
| k) | **Market penetration** | • Global application by a wide range of IIoT users<br>• Widespread application by major customers |

| T2. License information | |
|---|---|
| | • Use of open source software in parts (for example Apache Tomcat) with the corresponding open source licenses<br>• Proprietary licenses of the vendor |

| T3. Protocols | |
|---|---|
| | • HTTPs<br>• Older (legacy) and other protocols are integrated via interfaces provided by the ThingWorx software. |

| T4. Edge support | | |
|---|---|---|
| a) | **Overview** | ThingWorx Edge Extensions and Edge Microserver (EMS) components are used to integrate and program edge devices into the ThingWorx Platform:<br>*"ThingWorx Edge Extensions provide building blocks for the C SDK that allow you to create reusable components for application development. These components are intended to simplify the complex tasks required to interface with the hardware used for data acquisition and control in IoT environments. These blocks of modular functionality can be assembled in different combinations, based on the needs of your IoT environment, into a single Thing that represents your device in ThingWorx.*<br>*Edge SDK: The ThingWorx Edge C SDK is a lightweight, but fully functional implementation of the ThingWorx AlwaysOn protocol. It is designed to minimize memory footprint while making it easy to integrate applications into the ThingWorx distributed computing environment of the Internet of Things (IoT). The goal of the C SDK is to make creating applications that use it simple, but to also give developers enough flexibility to create very sophisticated applications. For example, the SDK contains a simple "tasker" framework that you can use to call functions repeatedly at a set interval. You can use the tasker framework to drive not only the connectivity layer of your application, but also the functionality of your application. However, it is not required to use the tasker at all.*<br>*Edge SDK functions:*<br>• *Establish and manage a secure AlwaysOn connection with an instance of ThingWorx Platform. This includes SSL/TLS negotiation, duty-cycle modulation, and connection maintenance such as re-establishing a connection after network connectivity is lost and restored.*<br>• *Enable easy programmatic interaction with the properties, services, and events that are exposed by entities on ThingWorx Platform.*<br>*Implement a callback infrastructure that makes it easy to expose a set of properties and services to ThingWorx Platform. These properties and services can be surfaced from multiple entities.*<br>*When a request is made from ThingWorx Platform for a registered property or service, a callback is made to a function that you supply during the registration process."* |
| b) | **Communication** | • ThingsWorx offers its own "wrappers" for industrial connectivity from older (legacy) IoT devices. |

| T4. Edge support | | |
|---|---|---|
| | | • Establish and manage a secure AlwaysOn connection with an instance of ThingWorx Platform. This includes SSL/TLS negotiation, duty-cycle modulation, and connection maintenance such as re-establishing a connection after network connectivity is lost and restored.<br>• Bi-directional communication with edge devices is possible (Data sending, Command (Event triggered) receiving). |
| c) | **Memory usage** | Edge and Fog-based storage is realized via ThingWorx Edge Extensions. |
| d) | **Specific capabilities** | ThingWorx Edge Extensions and the corresponding SDK can be used to implement required capabilities on Edge devices. |

| T5. IIoT devices | | |
|---|---|---|
| a) | **Device connectivity** | • Wide range of common protocol options for device and enterprise applications<br>• Focus on the ability to integrate 3rd party devices<br>• Focus on the integration of the largest possible number of connectors<br>  ○ Machine-to-Machine<br>  ○ "Device to Cloud" adaptors<br>  ○ ThingsWorx own "wrappers" for industrial connectivity<br>  ○ Integration Framework Connectors: Connecting devices to enterprise frameworks such as PLM, ERP, CRM, SCM<br>• Device Discovery: automatic discovery of new devices |
| b) | **Device management** | • Edge computing and Fog computing implemented via ThingWorx Edge Extensions<br>• Continuous device monitoring<br>• (Automatic) registration, organization, monitoring and remote management of connected IoT devices<br>• Support for the entire lifecycle of IoT devices |
| c) | **Deployment, provision of software** | • REST<br>• Software-as-a-Service (SaaS)<br>• Software delivery and development for IIoT are the core business areas of ThingWorx.<br>• Wide range of services that can be used by IIoT platforms.<br>• Very wide range of apps for administrative tasks<br>• Since it is possible for customers to create their own software, any form of heterogeneous/dynamic deployment of AI components or their integration into software created with ThingWorx is possible. |

| T6. Security | | |
|---|---|---|
| | | **Edge Security / Edge Connection Security:** Supports OpenSSL v.1.1.1 and also the standard Apache Tomcat cipher suites up to and including Tomcat 8.0.33. |
| | | **Server authentication:** A client (device) can confirm the identity of a server before sending data. Standard public key cryptographic techniques are used to verify that a ThingWorx platform's certificate and identity are valid and issued by a known certificate authority (CA) listed in the device's trusted certificate authority list. |
| | | **Encrypted connection:** Requires that all information sent between a client and a server is encrypted by the sending software and decrypted by the receiving software, ensuring a high level of confidentiality. In addition to data confidentiality, SSL / TLS ensures the |

| T6. Security | |
|---|---|
| | integrity of the transmitted data. That is, it provides a mechanism for determining whether the data has been modified during transmission (message authentication). |
| | **Client authentication:** Allows a server to confirm the identity of a client (device). Using the same techniques as server authentication, the server software verifies that the certificate and the device's identity are valid and issued by a known certificate authority that is included in the server's list of trusted certificate authorities. Client authentication is optional. |

| T7. Data protection | |
|---|---|
| | Shares some aspects with security. In addition, the platform offers: |
| | Improved security using Device Authority's KeyScaler.<br>• KeyScaler ThingWorx authentication extension: device identity verification for ThingWorx significantly increases trust and improves the "appKey" solution. It also provides automation to manage this at IoT scale.<br>• KeyScaler ThingWorx crypto extension: supports encryption and decryption of data directly within the ThingWorx platform for data in transit and at rest.<br>• KeyScaler ThingWorx Always-On Agent: A crypto agent for the ThingWorx Always-On protocol provides transparent, policy-based encryption for device applications connected to ThingWorx. |
| | Extensions for a secure solution:<br>• A secure and scalable method for device enrollment, authentication and ongoing validation via the current "appKey" model.<br>• Trust and authorization for connected devices and their associated data streams.<br>• Privacy for confidential information. |

| T8. Cloud support | |
|---|---|
| | • Cloud-based with integration of Microsoft Azure<br>• Local/hybrid storage |

| T9. Scalability | |
|---|---|
| | The software solutions offered are designed for scalability, for example by supporting the entire lifecycle of IoT devices as well as using the Model View Controller (MVC) approach. |

| T10. Digital twins / Asset Administration Shells | | |
|---|---|---|
| a) | **Digital twins** | The platform enables the creation and use of digital twins, for example to simulate devices and device networks. |
| b) | **AAS used for IoT devices** | • The core approach of ThingWorx to model entities as "Things" and to build software on top of the modeled "Things", following the Model-View-Controller MVC) approach, is similar to the AAS concept.<br>• The ThinkWorx platform describes the approach of modeling "Things" as follows: *"Things are representations of physical devices, assets, products, systems, people, or processes that have properties and business logic. All Things are based on Thing Templates (inheritance) and can implement one or more Thing Shapes (composition). It is a best practice to create a Thing Template to describe a Thing, and then create an instance of that Thing Template as a Thing. This practice leverages inheritance in your model and lowers the amount of time you spend maintaining and updating your model."*<br>• Things can form hierarchies analogous to the AAS. |

| T10. Digital twins / Asset Administration Shells | |
|---|---|
| | • Things and their events are comparable to active AAS: *„A Thing can have its own properties, services, events, and subscriptions and it can inherit other properties, services, events, and subscriptions from its Thing Template and Thing Shapes. How you model the interconnected Things, Thing Templates, and Thing Shapes is key to making your solution easy to develop and maintain in the future as the physical assets change. End users will interface with Things for information in applications and for reading/writing data.*<br>*Once you have defined the types of Things your model will contain (using Thing Shapes and Thing Templates), you can start to create specific Thing instances. In a truck example, you might define a truck Thing instance for every truck in your fleet. Each instance would track the information about itself and share that information for use in your applications, reports, and mashups. For a manufacturer, you might create a Thing instance for every machine, work center, or manufacturing unit, depending on your use cases. The granularity of asset management, product tracking, and data collection will influence how you model your equipment. ThingWorx is a rapid, model-based application development platform. By employing modeling instead of coding, the content developer is able to focus on agility and application composition rather than debugging, maintaining, and updating code. The model artifacts become a set of reusable building blocks to assemble new applications.*<br>*After you have your model in place, you can assemble the data, services, and capabilities of the model into a Web application via the drag-and-drop Mashup Builder.*<br>*Imagine a set of machines in a production line. An individual machine is a Thing. The production line may also be a Thing that consists of individual machines. Although it is not a requirement to include the production line as a Thing in your model, it may be useful if there is important production line level data within your application requirements. In this scenario, you would model production line data as properties within the production line Thing, allowing you to effortlessly include those objects in dashboards and mashups. Additionally, you could represent a plant as a Thing to use as a roll up for production data across an entire plant."*<br>*"Events are interesting or critical property states that the Thing publishes to subscribers. Events are initiators to kick off some functionality in a subscription, which is basically a triggered service. Within a service definition, if you double click the event, the script necessary to fire the event will be stubbed out in the service for you. Triggers are well-defined changes of state (for example, Motor is overheating) of an asset or system (a Thing). Triggers often require an action to respond to the change (for example, Display warning light to show that the tractor is overheating). Complex predictions from analytical algorithms can fire events and allow the application developer to react to those events with business logic. Business logic and actions in a ThingWorx application are driven by events."* |

| T10. Digital twins / Asset Administration Shells | | |
|---|---|---|
| c) | **AAS used for edge devices** | See T10b. |

| T11. Data management and data analysis | | |
|---|---|---|
| | | • Extensive capabilities for collecting, monitoring and analyzing data is real-time, supported by the dedicated data analytics component ThingWorx Analytics.<br>• Visualization of data and data analysis |

| T12. Offered AI methods | | |
|---|---|---|
| | | • Extensive data analysis capabilities<br>• Prediction (device behavior, failure, maintenance) with machine learning<br>• Learning of "normal behavior" of devices using machine learning<br>• Configuration optimization of devices through simulation (before deployment)<br>• Integration of simulation services from other providers |

| T13. Openness and Extensibility | | |
|---|---|---|
| a) | **Store** | The "PTC Marketplace" offers all software solutions and services from PTC as well as an online marketplace for third-party solutions, for example from partners in the PTC partner network. |
| b) | **App support for/by developers** | • Provision of APIs and SDKs<br>• Extensive documentation and tutorials on APIs, SDKs for all offered development tools and applications. |
| c) | **Use of “external” algorithms/data** | The SDKs of ThingWorx's various software solutions support the use of customer's own algorithms as well as the integration of third-party services, e.g. Microsoft Azure IoT. |
| d) | **AI interfaces** | See T13c. |

| T14. Systematic Configurability | | |
|---|---|---|
| | | • Model IIoT environments and workflows with ThingWorx AEP..<br>• Digital modeling of devices, employees, organizational units and workflows as "Things".<br>• "Next Generation Composer" tool for modeling applications in a browser environment.<br>• "Mashup Builder" drag-and-drop development tool for creating interactive applications, dashboards, collaborative apps and mobile apps, in a "no code" environment.<br>• The services and applications offered can be configured to a large extent according to the customer's specific needs or can be created from scratch specifically for or by the customer. |

| T15. Ecosystem support | | |
|---|---|---|
| a) | **“Multi-Sided“ platform** | • The ThingWorx IoT platform supports the networking of IoT devices with third-party IoT platforms. One focus here is MS Azure IoT.<br>• PTC offers a partner network for industry partners. |
| b) | **Open to third-party content** | • Extensive openness for the integration of third-party software and services (services, storage)<br>• Focus on the integration and "preservation" of assets, structures, software and storage services (clouds, etc.) already existing in an IIoT company |

| T15. Ecosystem support | | |
|---|---|---|
| c) | **Reference to RAMI 4.0** | Explicit reference to Industry 4.0 and RAMI 4.0 |

**T16. Other technical abilities**

- Graphical integration development
- MVC approach

**T17. References**

- Extensive information available on ThingWorx and PTC web pages and individual ThingWorx component/service web pages. Data sheets available as PDFs.
- Platform overview:
  - http://support.ptc.com/help/thingworx_hc/thingworx_8_hc/en/
  - https://www.ptc.com/de/products/iiot/thingworx-platform/thingworx-service-apps
  - http://support.ptc.com/help/thingworx_hc/thingworx_8_hc/en/index.html#page/ThingWorx%2FWelcome.html%23
  - https://www.ptc.com/de/products/iiot/thingworx-platform
  - https://developer.thingworx.com/en/resources/guides
  - https://www.ptc.com/-/media/Files/PDFs/IoT/ThingWorx-Build-Product-Brief.pdf
  - https://www.ptc.com/-/media/Files/PDFs/IoT/ThingWorx-Manage-Product-Brief.pdf
  - https://www.ptc.com/-/media/Files/PDFs/IoT/ThingWorx-Connect-Product-Brief.pdf
- Platform in context of Industry 4.0/RAMI:
  - https://www.ptc.com/de/thingworx-applications/manufacturing
  - https://www.ptc.com/en/solutions/digital-manufacturing/industry-4-0
- Overview of ThingWorx controls- and advisor applications:
  - https://www.ptc.com/de/thingworx-applications/controls-advisor
  - https://www.ptc.com/de/thingworx-applications/operator-advisor
  - https://www.ptc.com/-/media/Files/PDFs/Manufacturing/ThingWorx-Controls-Advisor_DS.pdf
  - https://www.ptc.com/-/media/Files/PDFs/Manufacturing/Operator-Advisor_Data-Sheet.pdf
- Overview on integration/use of edge devices in ThingsWorx: http://support.ptc.com/help/edge_sdk_c/r2.2.2/en/
- Overviews on PTC Marketplace, solutions and industrial partnerships:
  - https://www.ptc.com/marketplace
  - https://www.ptc.com/de/products/all
  - https://www.ptc.com/de/partners

## 3.16 Recogizer Analytics - Recogizer Analytics IoT Platform

| T1. Overview | | |
|---|---|---|
| a) | **Name of the platform** | Recogizer Analytics IoT Platform |
| b) | **Platform vendor or provider** | Recogizer Analytics GmbH, Bonn, Germany |
| c) | **Vendor summary** | *"The Recogizer IoT platform provides the ideal foundation to launch unique analytics applications. Control your production predictively, or digitize your business model with Machine-as-a-Service.*<br>*Due to its high-level scalability, our platform automatically adjusts to changing data volumes and business requirements; relying on state-of-the-art IoT Analytics platform architecture. Advanced Machine Learning ensures efficient predictions."* |
| d) | **Platform components** | • Anomaly detection<br>• Machine Learning<br>• Predictive Control<br>• Predictive Analytics<br>• Ingestion Streaming<br>• Stream Processing<br>• Dashboards, Reports, Events<br>• Persistence, Storage, Operations<br>• Data Pipelines, Quality control<br>• Graphix Engine[17] |
| e) | **Online marketplace platform** | *No information available* |
| f) | **Mobility platform** | Supports indoor maps that can be used for navigation inside buildings. |
| g) | **B2B context** | Yes |
| h) | **B2C context** | *No information available* |
| i) | **Platform users** | Developers, Industry 4.0 users such as machine operators or plant supervisors |
| j) | **Fields of application** | Production, intelligent buildings (smart buildings), AI for compressed air/compression |
| k) | **Market penetration** | Vodafone |

| T2. License information | |
|---|---|
| | Commercial, contact us (*„Sprechen Sie uns an"*) |

| T3. Protocols | |
|---|---|
| | • Any devices and sensors can be integrated via various interfaces. Various integration options for field devices and gateways (connectors).<br>• BACnet, Modbus/TCP, OPC-UA, Ether-S-Bus, https (REST API), WebSocket, MQTT<br>• 2G/3G/LTE, https/ http2, Lora, NB-IoT, VPN, communication provider-independent<br>• In principle, the vendor makes any other connection possible („Grundsätzlich machen wir jede andere Anbindung möglich."). |

| T4. Edge support | |
|---|---|
| | *No information available* |

[17] Die Bezüge zu Graphicx.ai blieben bei der Datenerfassung unklar.

| T5. IIoT devices | | |
|---|---|---|
| a) | **Device connectivity** | Any devices and sensors can be integrated via various interfaces. Various integration options for field devices and gateways via connectors. |
| b) | **Device management** | • Provisioning, registration, authentication, monitoring and management of devices<br>• Replication, partitioning, streaming<br>• Centralized management of networked devices and sensors, online and in real time. All communication points are seamlessly networked.<br>• Decommissioning of devices through remote access<br>• Monitoring of data traffic and error rates |
| c) | **Deployment, provision of software** | • Automation of software deployment<br>• Firmware-over-the-Air (FOTA) |

| T6. Security | | |
|---|---|---|
| | | **End-to-end integration and security:** The solution comes from a single source. Modern standards ensure security. |
| | | **Devices:** Roles and rights, signatures/data tracking encryption |
| | | • Provisioning, connection and authentication<br>• Device monitoring and diagnostics<br>• Integrates with existing landscape, e.g. LDAP, SSO<br>• Release |

| T7. Data protection | | |
|---|---|---|
| | | See Security (T6) |

| T8. Cloud support | | |
|---|---|---|
| | | • Hosting in certified data centers in Germany<br>• After a device is registered in the platform, it can transfer data to the cloud. („Nachdem ein Gerät in der Plattform registriert ist, kann [es Daten] in die Cloud übertragen.“)<br>• Time series are held and further processed with high availability.<br>• 99.9% availability according to SLA<br>• Multi-tenancy and client separation |

| T9. Scalability | | |
|---|---|---|
| | | *No information available* |

| T10. Digital twins / Asset Administration Shells | | |
|---|---|---|
| a) | **Digital twins** | Using graphicx.io, digital twins can be used to teach models. |
| b) | **AAS used for IoT devices** | *No information available* |
| c) | **AAS used for edge devices** | *No information available* |

| T11. Data management and data analysis | |
|---|---|
| | • Recording, monitoring, pre-processing and analysis of incoming data streams as well as events<br>• Structuring of data and meta-data by organization and assets (business logic)<br>• Calculation of key performance indicators (KPIs, virtual data points)<br>• Data flow oriented: Information in final data flow elements is automatically stored.<br>• Automated quality management of incoming data streams (vs. data sovereignty) and pre-processing of data streams |

| T12. Offered AI methods | |
|---|---|
| | • Predictive Analytics & Control with the help of machine learning methods taking into account subject-specific domain knowledge.<br>• With graphicx.ai: process improvement, reinforcement learning, anomaly detection. |

| T13. Openness and Extensibility | | |
|---|---|---|
| a) | **Store** | *No information available* |
| b) | **App support for/by developers** | Via APIs |
| c) | **Use of "external" algorithms/data** | • Integrate machine learning components easily („*Machine Learning-Komponenten einfach integrieren*“)<br>• Sophisticated analytics framework with predefined procedures that are aligned. („*Hochentwickeltes Analytics-Framework mit vordefinierten Verfahren, die aufeinander abgestimmt sind*.“)<br>• Developed by experts, adaptable to needs. One can use the platform's APIs to integrate existing systems and build their own IoT applications. („*Von Experten entwickelt, an den Bedarf adaptierbar. Man kann die APIs der Plattform nutzen, um bestehende Systeme zu integrieren und eigene IoT-Applikationen zu realisieren*.“) |
| d) | **AI interfaces** | *No information available* |

| T14. Systematic Configurability | |
|---|---|
| | • Own analyses UI/visualization level definable<br>• KPI manager for custom performance metrics<br>• Customize dashboards via reusable dashboard components<br>• Manage alarms and events<br>• IoT platform modules can be assembled based on the scope of the targeted projects and needs.<br>• Versioning of configurations is possible.<br>• With graphicx.ai: predefined HVAC Control and process Control solution packages. |

| T15. Ecosystem support | | |
|---|---|---|
| a) | **"Multi-Sided" platform** | Third-party platforms can be flexibly integrated via connectors. Diverse integration options for third-party platforms are offered. |
| b) | **Open to third-party content** | Via APIs, connectors and integration capabilities. |
| c) | **Reference to RAMI 4.0** | *No information available* |

| T16. Other technical abilities |
| --- |
| • Visualization of data, events, forecasts and insights<br>• Provides indoor maps that can be used for navigation<br>• Regular reporting<br>• Backup and recovery support<br>• Software maintenance and updating<br>• KPI support |

| T17. References |
| --- |
| https://recogizer-analytics.com/iot-plattform |

## 3.17 SAP – Leonardo

| T1. Overview | | |
|---|---|---|
| a) | **Name of the platform** | SAP Leonardo |
| b) | **Platform vendor or provider** | SAP AG, Germany |
| c) | **Vendor summary** | *„SAP Leonardo versteht sich als ein ganzheitliches System, das Unternehmen die Umsetzung digitaler Innovationsstrategien mit modernen Technologien wie maschinellem Lernen, IoT, Blockchains oder Big Data ermöglicht. Die Basis für das System bilden die Cloud-Services von SAP. SAP Leonardo darf nicht als einzelne Software oder einzelnes Produkt verstanden werden. Vielmehr verbirgt sich hinter dem Namen ein Portfolio verschiedener Services und Produkte, mit dem ein ganzheitliches digitales Innovationssystem für Unternehmen bereitgestellt wird. Unter anderem beinhaltet SAP Leonardo Anwendungen, Microservices und Cloud-Dienstleistungen für moderne digitale Technologien und Methoden wie maschinelles Lernen, das Internet der Dinge (Internet of Things - IoT), Blockchains, Analytics oder Big Data.“* (no corresponding English text found) |
| d) | **Platform components** | • SAP Internet of Things Gateway Cloud<br>• SAP Internet of Things Edge Platform<br>• SAP Thing Modeler<br>• SAP IoT Application Enablement<br>• SAP IoT Gateway Edge cloud<br>• SAP-Leonardo-Accelerator Packages<br>• Internet of Things Edge Platform SDK<br>• Internet of Things Service Cockpit |
| e) | **Online marketplace platform** | Yes, applicable for retail industry, consumer goods industry, travel industry |
| f) | **Mobility platform** | Yes, applicable in the automotive sector |
| g) | **B2B context** | Yes, focus on B2B |
| h) | **B2C context** | No focus on end users (consumers), possible application as backend in end-user oriented apps. |
| i) | **Platform users** | • IoT platforms and industry applications for enterprises, mainly "out of the box" for enterprise customers but also for companies with limited development intentions of their own (customizing the available applications)<br>• Easy development, deployment and testing capabilities with pre-configured solutions<br>• Offer "SAP Leonardo Accelerator Packages" that provide specialized application packages for the following industries:<br>○ Retail<br>○ Manufacturing<br>○ Sports and entertainment<br>○ Consumer goods industry<br>○ Transportation<br>○ Automotive sector<br>○ Travel industry<br>○ Utilities industry<br>○ Telecommunications industry |

| T1. Overview | | |
|---|---|---|
| j) | **Fields of application** | • Administration environment for managing and monitoring sensor data generated by technical objects from the Internet of Things.<br>• Development, customization and operation of cloud-based IoT business applications. |
| k) | **Market penetration** | • Global application by a wide range of users<br>• Widespread application by major customers |

| T2. License information | |
|---|---|
| | Uses open source software in various subareas (e.g. Kyma), otherwise proprietary licenses. |

| T3. Protocols | |
|---|---|
| | • HTTPS, MQTT, SNMP, Modbus, CoAP, OPC UA, Sigfox<br>• File transfer |

| T4. Edge support | | |
|---|---|---|
| a) | **Overview** | In SAP Leonardo, physical devices are modeled as "Things". Edge devices and their connected (IoT) devices are therefore also "Things" and are to be understood as such. SAP Leonardo uses an SAP IoT Gateway Edge Cloud with optional connection to Dynamic Edge (Dynamic Edge Services) that can run Dynamic Edge Applications on local edge devices. Furthermore, via the cloud-based SAP IoT Gateway Edges, data streams from connected edge devices can be bundled and sent to the SAP Cloud for further processing/evaluation.<br>One way of evaluating such local data streams is to apply rules to these data (time series) using a rule engine integrated in the SAP IoT Gateway Edge cloud. Furthermore, via the SAP IoT Gateway Edge cloud, all devices can access all services of the platform via the IoT services, including various ML services, specifically geared to IoT, as well as extensive analysis functions.<br>The basic approach to monitoring and controlling (end) devices is the exchange of "messaures" (measurements of sensor data, time series, etc.) and "commands", i.e., the triggering of actions on the (end) devices. This exchange takes place between the (end) devices and the Internet of Things Gateway Cloud or the Internet of Things Edge Platform. Meassures can contain single properties or summaries of multiple properties of a device. Meassures are always encapsulated in a "Meassure" message, which may contain additional meta-information, such as sensor identifiers or alternative sensors used to validate the measurements. Commands are data, mostly instructions, sent from the Internet of Things Gateway Cloud or the Internet of Things Edge platform to an (end) device, something after an evaluation of Meassures from a device that triggered a rule stored in the rule engine. Analogous to Meassure messages, Command messages are also encapsulated and enriched with meta-information.<br>The onboarding of devices (or their "Thing Model") can be performed both manually and automatically, whereby the activation of an onboarding always takes place only after the |

| T4. Edge support | | |
|---|---|---|
| | | successful assignment and validation of a certificate by the SAP Cloud. Based on the aforementioned adapters and software components, SAP Leonardo: Eine breite Palette von allen gängigen Protokolloptionen für Geräte- und Unternehmensanwendungen:<br>• Possibility to integrate 3rd party devices via e.g. customizable HTTP endpoints<br>• Integration of different protocols and systems via<br>  ○ IoT Edge Platform adapters<br>  ○ Eclipse Plug-Ins (IoT Edge Platform Adapter/Interceptor SDKs)<br>Via the platform-wide available IoT services, basically all edge devices can also access the complete features/functions of the SAP Leonardo Cloud via the SAP IoT Edge Gateways. This availability of IoT services enables the implementation of a wide range of functions for edge devices via the software component of the SAP IoT Gateway Edge Cloud, by requesting cloud services from the SAP Cloud:<br>• Monitoring of assets via IoT edge gateways (software component)<br>• Visualization of asset data<br>• Behavioral monitoring and analysis of assets<br>• Predictive diagnostics for assets<br>• Use rule engines for rule-based control of devices<br>• Automatic notifications of rule violations<br>• Creation of time series from sensor data for further analysis and use in rule engine<br>Sensor data from Things can be summarized and analyzed on the basis of individually defined time periods. This allows trend observations and forecasts to be made for various use cases, for example, in the maintenance of devices or machines. SAP Leonardo also provides the Query Modeler tool for analyzing time series data generated by sensors in different dimensions. |
| b) | **Communication** | The communication with (end)devices is done via the mentioned messages and commands (messages) in encapsulated form and, supported by software adapters on the SAP IoT Gateway Edge Cloud level, supports the protocols in T3. |
| c) | **Memory usage** | • Mainly cloud-based: Sensor data generated by Things present on the platform is stored in a powerful, multi-component database system developed using SAP's in-memory database, SAP HANA.<br>• Storage in the local IoT Gateway Edge Cloud is possible. |
| d) | **Specific capabilities** | • Creation of time series from sensor data<br>• Ability to create rules that respond to defined patterns/results in the time series<br>• Provision of a "Rule Modeler" app to define:<br>  ○ Rules<br>  ○ Actions triggered by user defined events<br>  ○ Templates for notifications<br>SAP Leonardo has a focus on natural language applications and offers these, or the ability to develop these natural language processing (NLP) applications, to its customers. This specialization |

| T4. Edge support | | |
|---|---|---|
| | | of SAP Leonardo can also be applied to the control of edge devices as well as to the representation of their data and furthermore possibly also to the natural language explanation of system decisions. |

| T5. IIoT devices | | |
|---|---|---|
| a) | **Device connectivity** | • Wide range of common protocol options for device and enterprise applications<br>• Ability to integrate 3rd party devices via e.g. customizable HTTP endpoints<br>• Integration of different protocols and systems via:<br>  ○ IoT Edge Platform Adapters<br>  ○ Eclipse Plug-Ins (IoT Edge Platform Adapter/Interceptor SDKs) |
| b) | **Device management** | • Secure on-boarding and off-boarding (insertion, removal) of a wide range of devices<br>• Automatic on-boarding possible |
| c) | **Deployment, provision of software** | • REST<br>• Software-as-a-Service (SaaS)<br>• Wide range of microservices for accessing SAP IoT Applications<br>• Apps for administrative tasks<br>• Apps for defining "Thing Types" (device modeling), connecting devices with their "Digital Twin" via this "Thing Type" modeling<br>• Apps for rule-based processing of events |

| T6. Security | | |
|---|---|---|
| | | **Device authorization and authentication:**<br>a. Verification of metadata of a device to be connected via a certificate for releasing the resources a device requests<br>b. The following authorization checks are performed for each new connection:<br>  i. The *instanceID* contained in the certificate must match the ID of the instance to which the Internet of Things gateway belongs.<br>  ii. The *deviceAlternateID* contained in the certificate must match the ID of the instance to which the Internet of Things gateway belongs.<br>  iii. The *deviceAlternateID* contained in the certificate must match the MQTT client ID retrieved from the MQTT metadata<br>  iv. When an MQTT client attempts to post measurement data for ingestion, the following authorization checks are performed:<br>  • The topic for which the measurement data is published must be consistent with the structure defined for the data acquisition topic.<br>  • The *deviceAlternateID* contained in the certificate must match the alternate ID value specified in the metrics collection topic.<br>c. When a MQTT client attempts to subscribe to the command topic, the following permission checks are performed:<br>  i. The target topic must match the structure defined for the command topic.<br>  ii. The *deviceAlternateID* contained in the certificate must match the alternate ID value specified in the command topic. |
| | | **Software security:**<br>a. Encrypted internal communication and data storage<br>b. Separation of SP Leonardo from customer-owned software: As a generic platform, SAP Leonardo IoT is not connected to SAP Cloud Platform Retention Management. |

| T6. Security | | |
|---|---|---|
| | | This is because SAP may not know what kind of customer-based applications have been created on SAP Leonardo IoT. Therefore, applications that a customer creates based on SAP Leonardo IoT must subscribe to SAP Cloud Platform Retention Management individually.<br>c. Distinction between Customer Zone and Cloud Zone<br>i. Customer Zone: Software running on a device that has direct access to the device data and controls operations including communication on the device. This zone also contains the device certificate including its private key for the particular device to be stored securely on the device. Since bidirectional communication can take place between the core services and the device, this zone also includes the secure processing of messages received from the core services on the device.<br>ii. Cloud Zone: The core functions of the Internet of Things Service offered by the components hosted in an SAP-driven cloud environment, the SAP Cloud Platform for Cloud Foundry environment. |
| | | **Network and communication security:**<br>a. The Internet of Things Edge Platform uses standard mechanisms to ensure secure connections between its components:<br>i. Applications can use data from Internet of Things message processing when BASIC authentication is performed over TLS. Core REST API endpoints can be accessed via BASIC authentication.<br>ii. The Edge of Platform components of the Internet of Things connect to the Internet of Things over an encrypted connection using mutual authentication based on X.509 certificates. For more information, see the Secure Device Onboarding section.<br>iii. Devices can connect to the Internet of Things Gateway Cloud (MQTT or REST) using a secure TLS where client certificate authentication is present. Here we enforce the latest version of Transport Layer Security, version 1.2.<br>iv. Security between devices and the Internet of Things Edge platform depends on the protocol implemented by the devices. The specific implementation of the Internet of Things Edge platform is responsible for using the protocol security mechanism to provide end-to-end security from devices to applications connecting to the Internet of Things service for the Cloud Foundry environment.<br>b. Communication security: SAP Cloud Platform uses encrypted communication channels based on HTTPS / TLS.<br>c. Communication via the protocols in T3 |
| | | **User rights management (Roles), Identity Management:**<br>a. The SAP Leonardo IoT platform has a two-dimensional authorization concept with object instance-based authorizations as well as functional authorizations<br>i. Object instance-based permissions (also called access permissions or "capabilities") can be used to establish a relationship between individual members of the organization and the objects that the members are allowed to access.<br>ii. Functional permissions (also called "scopes") can be used to control what types of access a user may perform to the objects accessible to him/her.<br>b. User identity management and resource access policies in the Internet of Things service are provided through a set of APIs and the Internet of Things service cockpit.<br>i. The Internet of Things service relies on mutual authentication to secure communications with users, where a user is software, an individual, or a legal entity registered in the identity management component of the Internet of Things service and using the available services.<br>ii. To ensure secure user identity management, users are assigned a unique digital identity across all system components. In addition, users can be assigned user roles |

| T6. Security | |
|---|---|
| | c. Using Principal Propagation to exchange user ID information between systems or environments in SAP Cloud Platform:<br>i. Principal Propagation from Cloud Foundry to the Neo environment<br>ii. Principal Propagation from the Neo- to Cloud Foundry environment<br>iii. On-Premise User Store<br>iv. Principal Propagation in OAuth-protected applications<br>v. Connectivity in the Cloud Foundry environment: Principal Propagation<br>vi. Connectivity in der Neo environment: Principal Propagation<br>d. User authorization:<br>i. Applications and their users require different permissions to integrate seamlessly with SAP Cloud Platform.<br>ii. Developers configure these permissions at the application descriptor file level so that security artifacts are available in the cockpit.<br>iii. Administrators use the security artifacts to create roles and group them into role collections (permission sets that are appropriate for specific user groups).<br>iv. Security artifacts allow applications to communicate with other applications, such as making or receiving calls.<br>e. Identitiy- / Trustmanagement<br>f. In the SAP Cloud Platform, identity providers provision users. They can have a different identity provider for each subaccount they own. Through the Cockpit, administrators establish the trust relationship between external identity providers and the subaccounts.<br>i. To enable SAP Cloud Platform applications to seamlessly integrate with existing on-premises identity management infrastructures, SAP Cloud Platform provides single sign-on (SSO) and identity federation capabilities.<br>ii. In SAP Cloud Platform, identity information is provided by identity providers (IdP) and is not stored on SAP Cloud Platform itself.<br>iii. Identity federation is the concept of linking and reusing a user's electronic identities across multiple identity providers.<br>iv. This allows authentication and authorization functions to be decoupled and centralized. Several important protocols have been developed to support the concept of identity federation:<br>• SAML 2.0<br>• OAuth 2.0<br>• Further protocols |
| | |

| T7. Data protection | |
|---|---|
| | Shares many aspects with security (T6). |
| | SAP does not provide legal advice in any form. SAP software supports data protection compliance by providing security functions and specific data protection-related functions, e.g., simplified locking and deletion of personal data. In many cases, compliance with applicable privacy and data protection laws is not covered by a product feature. Definitions and other terms used in this document are not derived from any particular legal source. |
| | The extent to which data protection is supported by technical means depends on secure system operation. Network security, implementation of security notices, appropriate logging of system changes, and appropriate use of the system are the basic technical requirements for compliance with data protection and other laws. |

| T8. Cloud support | |
|---|---|
| | • Cloud-based, uses SAP's cloud services (Cloud Foundry environment)<br>• Hosted in the SAP Cloud Platform<br>• Stores data in the in-memory database SAP HANA |

| T9. Scalability | |
|---|---|
| | Within the Internet of Things Edge Platform component of SAP Leonardo, the scalability aspect is supported by the scale-out mode. The platform can be configured to run in a scale-out mode, where multiple instances run in a federated cluster to distribute the computational load. All instances in the cluster are assigned to the same platform-specific ID and therefore all instances behave as a single platform from a user perspective. All instances must implement the same protocol (e.g., REST or MQTT), with each instance providing its own protocol endpoint. An IoT device sees the cluster, but not the individual instances. The instances share the input load (uplink flow) produced by the devices. Device commands are only processed by exactly one instance per time unit, even if each instance can execute all commands (downlink flow). Device model instances (see also T4a) must be known to all instances. This is made possible by the fact that all instances share the same descriptive topology information. |

| T10. Digital twins / Asset Administration Shells | | |
|---|---|---|
| a) | **Digital twins** | The platform allows digital twins e.g. for closed loop development of devices. |
| b) | **AAS used for IoT devices** | • Modeling of devices as "Things" corresponds to the concept of the AAS.<br>• Encapsulation of (IoT) devices and edge devices by modeling them as "Things".<br>• Encapsulation of messages (measurements, commands) in wrappers that contain additional meta-information about the messages and exchanging entities. |
| c) | **AAS used for edge devices** | • Encapsulation of managed IoT devices in a representation as a "Thing". This representation can also be applied to other entities, such as device networks, gateways, and even enterprise departments.<br>• Design and modeling of the encapsulation is done via middleware "SAP Leonardo Thing Modeler". |

| T11. Data management and data analysis | |
|---|---|
| | • Collection, monitoring and analysis of data is possible in real time<br>• Visualization of data and data analysis<br>• Time series analysis of data from "Things" (devices)<br>• Trend monitoring and forecasting based on data analysis<br>• "Query Modeler" for creating highly customizable time series analyses |

| T12. Offered AI methods | |
|---|---|
| | • Pattern recognition from sensor data<br>• Pattern/rule-based triggering of event reactions<br>• Creation of conversational (chat) apps, based on SAP Leonardo Conversational AI Foundation<br>• Extensive possibilities in the area of device data analysis |

| T13. Openness and Extensibility | | |
|---|---|---|
| a) | **Store** | • SAP Leonardo does not offer a direct store through which customers and developers can offer their own applications and services.<br>• SAP Leonardo offers a very wide range of (micro) services in the context of IIoT and IoT. |
| b) | **App support for/by developers** | Extensive developer support:<br>• The Cloud Foundry environment enables the creation of multilingual applications (based on the Cloud Foundry Application Runtime), e.g., with SAP Java, Python and Node.js (or custom languages based on "community buildpacks for PHP, Ruby, Go.").<br>• The SAP Cloud Platform Cloud Foundry environment is a PaaS environment that enables microservices development and orchestration.<br>• Application lifecycle management: start, stop, deploy and scale via standardized Cloud Foundry tools, the cockpit and DevOps functionalities.<br>• Library capabilities such as SAP Cloud Platform Cloud Foundry services for message exchange, data storage (persistence), etc.<br>• ABAP can be used within the Cloud Foundry environment.<br>• Native Kubernetes extensions can be brought in through the Kyma environment.<br>• Supported features: Diego runtime, SSH, Custom Domains, Docker, Running Tasks, Zipkin Tracing, Websockets, Space-Scoped Service Brokers, Route Services (only user-provided and fully-brokered services).<br>• SAP continues to provide an SDK for the Internet of Things Edge Platform: *"The Internet of Things Edge Platform SDK enables developers to extend the Internet of Things Service(s)."*<br>*"The Internet of Things Edge Platform SDK provides Eclipse-based tools, which enable you to extend the Internet of Things Edge Platform with new adapters and interceptors."* |
| c) | **Use of "external" algorithms/data** | The platform allows and supports the development of customer-specific applications. It provides a set of models, APIs and services for this purpose. |
| d) | **AI interfaces** | • Creation of time series from sensor data<br>• Ability to create rules that respond to defined patterns/results in the time series |

| T14. Systematic Configurability | | |
|---|---|---|
| | | Customers cannot create their own platform configurations, but can use customized "packages" based on customer application areas. |

| T15. Ecosystem support | | |
|---|---|---|
| a) | **"Multi-Sided" platform** | • Yes, the platform allows the integration of other platforms.<br>• (Further) networking with other cloud service providers (Azure, AWS, Alibaba) is possible.<br>• SAP Leonardo supports the development of customer-owned applications and services by providing a set of software components, APIs and SDKs. |

| T15. Ecosystem support | | |
|---|---|---|
| | | • Integration of existing customer systems is relatively easy due to the strong encapsulation of communication and device representation as well as software adapters.<br>• Networking among customers is not actively encouraged/supported.<br>• Customer-owned applications must comply with the security and quality standards of the SAP Leonardo platform |
| b) | **Open to third-party content** | • Limited, the platform allows the development of custom application configurations based on the provided application building blocks.<br>• Provides a set of APIs for custom application development (no free custom app development).<br>• However, Cloud Foundry languages as well as Kubernetes extensions can be brought in. |
| c) | **Reference to RAMI 4.0** | *No information available* |

| T16. Other technical abilities | | |
|---|---|---|
| | | • One focus of SAP Leonardo is to offer natural language processing (NLP) applications for enterprises.<br>• Microservice support |

| T17. References | | |
|---|---|---|
| | | • Overviews of the platform:<br>  ○ https://help.sap.com/viewer/product/SAP_Leonardo_IoT/1904a/de-DE<br>  ○ https://help.sap.com/viewer/product/SAP_CP_IOT_CF/Cloud/en-US<br>  ○ https://www.sap.com/germany/products/leonardo.html<br>  ○ https://www.bigdata-insider.de/was-ist-sap-leonardo-a-824039/<br>  ○ https://www.sap.com/germany/products/intelligent-technologies.html<br>• Security Platform: https://help.sap.com/viewer/7f425dfcbb474a28b9d07829f524665c/1904a/en-US<br>• Security Query Modeler:<br>• https://help.sap.com/viewer/e7dae2e1ffa44f70a2959d69f75686d5/1904a/en-US<br>• Conversational Apps: https://www.sap.com/documents/2017/09/3898957e-d57c-0010-82c7-eda71af511fa.html<br>• Complete description of the "Things" Platform (Services): https://help.sap.com/doc/a48fdbd924724b378d6f71c54c9f35b5/1904a/de-DE/leoAPI_de.pdf<br>• Feature Scope Description of the Platform: https://help.sap.com/doc/f7254d7f9e0d4dc9b54a3f5f95987a2b/1904a/de-DE/leonardo_iot_fsd_de.pdf<br>• Rule-based IoT data management: https://help.sap.com/doc/75c2de67861a40bfbc830eea4b58489c/1904a/de-DE/iot_rules_de.pdf<br>• Cloud Platform Security: https://help.sap.com/viewer/65de2977205c403bbc107264b8eccf4b/Cloud/en-US/e129aa20c78c4a9fb379b9803b02e5f6.html<br>• Internet of Things Edge Platform SDK documentation: https://help.sap.com/viewer/c4945853cc164aa385973d5938b385ac/Cloud/en-US |

## 3.18 Siemens – MindSphere

| T1. Overview | | |
|---|---|---|
| a) | **Name of the platform** | MindSphere |
| b) | **Platform vendor or provider** | Siemens AG, Germany |
| c) | **Vendor summary** | *„MindSphere bietet eine breite Palette von Protokolloptionen für Geräte- und Unternehmensanwendungen, Branchenanwendungen, umfangreiche Analysen und eine innovative Entwicklungsumgebung, die sowohl die offenen PaaS-Funktionen (Open Platform-as-a-Service) von Siemens nutzt, als auch den Zugriff auf Cloud-Dienste von Amazon Web Services (AWS) und Microsoft Azure und Alibaba bietet.“*<br><br>*„MindSphere ermöglicht durch offene PaaS-Funktionen die Entwicklung und Bereitstellung neuer Branchenanwendungen in einem vielfältigen Partner Ecosystem. Profitieren Sie von den Erfahrungen und Erkenntnissen unserer Partner. Um Ihre IoT-Strategie voranzubringen, ist keine Entwicklung Ihrerseits erforderlich.“* (no corresponding text in English found) |
| d) | **Platform components** | • MindConnect<br>• MindConnect Edge Analytics<br>• MindConnect IOT Extensions<br>• MindConnect Integration Services<br>• MindSphere Connect and Monitor Solution Package<br>• MindSphere Digitalize and Transform Solution Package<br>• MindSphere Connect and Monitor Solution Package<br>• Common Remote Service Platform Services<br>• Fleet Manager |
| e) | **Online marketplace platform** | Applicable in the context of managing IoT data of commercial IoT devices ("smart devices"). |
| f) | **Mobility platform** | Applicable to limited mobility scenarios |
| g) | **B2B context** | Yes, focus on B2B |
| h) | **B2C context** | Limited end-user application, more like an aggregator of data from end-user devices. |
| i) | **Platform users** | • Enterprise IoT platforms and industry applications, both for companies with their own development intentions and "out of the box" for enterprise customers<br>• Easy development, deployment and testing capabilities with pre-configured solutions |
| j) | **Fields of application** | • Creation and operation of small to very large IoT platforms (applications)<br>• Merging of physical web-based and enterprise systems |
| k) | **Market penetration** | • Global application by a wide range of users<br>• Widespread application by major customers (DAX 100 etc.) |

| T2. License information | | |
|---|---|---|
| | | • Siemens works with OpenPaaS.<br>• Open source software can, with the appropriate licenses, be integrated into the development of applications and services by third-party providers. |

| T3. Protocols | | |
|---|---|---|
| | | Amongst other, S7, Open Platform Communication Unified Architecture (OPC UA), LoRaWAN, Modbus, CoAP, XMPP, 6LowPan, LWM2M, AMQP |

| T4. Edge support | | |
|---|---|---|
| a) | **Overview** | Combination of edge devices and cloud services/cloud storage, implemented by the MindConnect component and its libraries and API for deploying software on edge devices. The MindConnect Edge Analytics component provides a condition monitoring system (CMS) that is used to perform analytics tasks on edge devices.<br>The processing of tasks on Edge devices is realized in MindSphere through a two-pronged approach: The provision of Edge services via a cloud (MindSphere Cloud) and the provision of a modular Edge device runtime environment (runtime) that is directly implemented on Edge devices. One focus of the runtime environment is its compatibility with the widest possible range of hardware and protocols. Another focus of the runtime environment is its ease of extensibility/application for creating new applications for edge devices by third-party vendors.<br>The core approach of edge device usage in MindSphere is to connect cloud services that can be accessed by edge devices with edge applications that run locally on the edge devices.<br>• Monitoring of assets via edge devices<br>• Visualization of asset data (states) via highly customizable, or freely developable dashboard (templates).<br>• Direct diagnostics of assets through edge devices<br>• Behavioral monitoring and analysis of assets<br>• Predictive diagnostics for assets<br>• Prescriptive diagnostics for assets, such as fill levels, etc.<br>• Root-cause analysis of asset defects<br>• Management of software updates for edge devices<br>• Implementation of analytics tasks in the edge runtime environment possible as well as by requesting cloud services by edge devices<br>• Collection, aggregation, analysis, compression and storage of asset data directly on edge devices possible.<br>• Cyclic data collection up to 192 kHz collection frequency possible by edge devices<br>• Pre-processed data can be sent from the edge devices to the MindSphere Cloud |
| b) | **Communication** | The communication of edge devices is (mainly) realized in MindSphere via the "MindConnect" component. MindConnect provides services that establish connectivity between edge devices, IoT services and storage locations (local, cloud).<br>MindConnect also provides an API for the services that allows edge devices to connect to the MindSphere platform in a customer-specific way.<br>Security features:<br>• Standards<br>  ○ ISO 27001 Information Security Management System Framework<br>  ○ IEC 62443-4-1, safe development cycle |

| T4. Edge support | | |
|---|---|---|
| | | • Hardware<br>  ○ Onboarding only with valid, unique ID and security token<br>  ○ Separation of external and internal (factory) network<br>  ○ Encrypted configuration files<br>  ○ Read-only access to automation protocols<br>  ○ Proxy support<br>  ○ Secure offboarding<br>• Software: Encrypted internal communication and data storage.<br>• Communication: TLS v. 1.2 for communication between client and MindSphere via public networks |
| c) | **Memory usage** | • Both local storage on edge devices and use of cloud storage<br>• Possibility of exchanging data with other platforms is given and actively supported by middleware. |
| d) | **Specific capabilities** | Here, basically "anything" is possible, as for edge devices almost free new applications to run on the edge devices themselves, as well as the development and deployment of cloud services for edge devices is possible. |

| T5. IIoT devices | | |
|---|---|---|
| a) | **Device connectivity** | • Wide range of all common protocol options for device and enterprise applications<br>• Integration of a wide range of protocols and systems |
| b) | **Device management** | Secure onboarding and offboarding (insertion, removal) of various types of devices |
| c) | **Deployment, provision of software** | • REST<br>• Software-as-a-Service (SaaS)<br>• Possibility to develop customer's own apps and integrate them into the platform<br>• MindSphere Store for buying and selling MindSphere applications |

| T6. Security | | |
|---|---|---|
| | | **Certification and standards**<br>• MindSphere follows the ISO 27001 Information Security Management System Framework<br>• MindSphere is certified according to IEC 62443-4-1, secure development lifecycle |
| | | **Architecture**<br>• Identity management and access control<br>  ○ RBAC<br>  ○ Coarse granular authorization - multifactor authentication<br>• Communication: TLS v. 1.2 for communication from client to MindSphere via public endpoints |
| | | **Connectivity**<br>• Hardware<br>  ○ Only with valid, unique ID and security token on board<br>  ○ Separation of external and automation networks<br>  ○ Encrypted configuration files<br>  ○ Read-only access to automation logs<br>  ○ Proxy support - secure onboarding<br>• Software: Encrypted internal communication and data storage |

| T6. Security | |
|---|---|
| | • Application and client management: Isolation and separation of clients through API gateway support, validation checks, and content security policies<br>• Availability and security controls and monitoring<br>  ○ Data classification and encryption<br>  ▪ HTTP over TLS v1.2 to communicate with MindSphere over an external network.<br>  ▪ MindSphere data is encrypted during transmission using TLS algorithms<br>  ▪ Data remains in the collected area<br>  ○ Backup and restore<br>  ▪ Usage transparency service from Siemens<br>  ▪ Data is backed up daily and retained for 30 days<br>  ▪ Data storage protection services run redundantly in at least two availability zones<br>  ○ Control and monitoring<br>  ▪ Penetration testing<br>  ▪ Threat risk analysis process<br>  ▪ Monitoring logs (audit logs) |

| T7. Data protection | |
|---|---|
| | Shares many aspects with security (T6). |

| T8. Cloud support | |
|---|---|
| | • Cloud based<br>• Implemented through cloud services, Azure, AWS and Alibaba |

| T9. Scalability | |
|---|---|
| | MindSphere supports seamless extension of existing edge device federations. Supported devices (selection<br>• Siemens SIMATIC IT automation controls<br>• SINUMERIK machine controls<br>• SIPROTEC smart grid components<br>• Climatix HVAC controllers |

| T10. Digital twins / Asset Administration Shells | | |
|---|---|---|
| a) | **Digital twins** | The platform offers digital twins for closed loop development of devices and device networks as well as for extensive further simulation, monitoring, analysis and development processes. |
| b) | **AAS used for IoT devices** | • Encapsulation of managed IoT devices, but no explicit mention of AAS.<br>• Encapsulation takes place in part via middleware<br>• The demonstrator "Experience Industry 4.0 component live" is a realistic setup of a manufacturing cell that was jointly designed and implemented by various companies under the leadership of Siemens. |
| c) | **AAS used for edge devices** | Use in demonstrator but not (currently) explicitly mentioned for actual use with edge devices. |

| T11. Data management and data analysis | |
|---|---|
| | • Collecting, monitoring and analyzing data in real time is possible.<br>• Visualization of data and data analysis |

| T12. Offered AI methods | | |
|---|---|---|
| | | • Explicit AI techniques are not specified in more detail.<br>• Extensive capabilities in the area of "product intelligence," in terms of analyzing and predicting products and device behavior |

| T13. Openness and Extensibility | | |
|---|---|---|
| a) | **Store** | With the MindSphere Store, Siemens offers a central marketplace for industrial applications and services hosted in the MindSphere Cloud. Applications and services can be offered by developers as trial versions or as a directly payable service.<br>Applications and services in the MindSphere Store can come from a variety of vendors (vendor-neutral):<br>• Siemens' own applications and services<br>• Siemens partners (ISV, OEM)<br>• Offers from Siemens partners are tested by Siemens with regard to their security, analogous to other app stores.<br>• Third-party offerings are subject to a license agreement with Siemens, which may include separate third-party usage permissions and terms. Third-party providers remain liable for the apps and services they provide.<br>• Third Party Providers must provide sufficient technical support for their Offerings.<br>• Partners and third-party providers may actively promote their offerings on the MindSphere Store.<br>Der MindSphere Store ist Anbieter-neutral. |
| b) | **App support for/by developers** | • Registration, testing, configuration, publishing and deployment of applications is supported by "cockpits" (management software) provided by Siemens.<br>• Direct deployment of applications to customers or deployment of applications via the MindSphere Cloud.<br>• Support for common development environments and platforms: Cloud Foundry PaaS and AWS Cloud Services.<br>• Developers of offerings from the Store are supported by Siemens as follows:<br>  ○ Local development of IoT applications possible in any common language and common development environment.<br>  ○ Direct upload of developed applications to the MindSphere Cloud. |
| c) | **Use of “external” algorithms/data** | • Supports the development of custom edge applications by customers and third parties<br>• Supports customer and third-party development of edge (micro) services<br>• Provides a set of APIs for development<br>• Allows native cloud development<br>• Supports exchange of data (Siemens, non-Siemens) through the MindConnect component<br>• Supports edge application development through modular edge runtime environment<br>• Supports "customer-owned" management of edge devices through integrated support functions |

| T13. Openness and Extensibility | | |
|---|---|---|
| | | • Deployment of customer's own software and third-party software through the MindConnect component |
| d) | **AI interfaces** | • Possible in the context of custom apps<br>• Not mentioned as a platform-specific capability |

| T14. Systematic Configurability | | |
|---|---|---|
| | | Customers can create their own platform configurations. |

| T15. Ecosystem support | | |
|---|---|---|
| a) | **"Multi-Sided" platform** | • Siemens actively supports the formation of an ecosystem for MindSphere.<br>• The MindSphere ecosystem is a central component of the MindSphere business model.<br>• The ecosystem is formed by integrating partners from the hardware (OEM) as well as software developers.<br>• The integration of partners is independent of the size of the partners and thus also has a focus on SMEs.<br>• The integration of industry partners is independent of the (production) domain of the industry partners.<br>• The MindSphere ecosystem currently already includes several million devices at partners as well as an extensive range of software from a large number of providers that are offered via the MindSphere store.<br>• The approach of the ecosystem in MindSphere is the operation of edge-oriented applications on the production level which is supported by services, storage capacities as well as applications on the MindSphere level.<br>• Siemens' strategy in the MindSphere ecosystem is to transparently integrate cloud services with any device, asset or production facility to enable seamless extensibility of the heterogeneous MindSphere device and asset ecosystem.<br>• MindSphere continues to support the "open-edge strategy" approach, which allows vendors to integrate cloud-enabled edge and device management capabilities into hardware.<br>• To support the growth of the ecosystem, Siemens offers a variety of APIs to encourage the development of new applications by partners and third-party vendors.<br>• Siemens supports partners in the ecosystem through a variety of resources, such as training and consulting, to help partners develop their own software. |
| b) | **Open to third-party content** | • The MindSphere platform is open to software extensions as well as entirely new third-party applications that can be integrated into the platform's ecosystem.<br>• Exchange of data (Siemens, Non-Siemens) explicitly supported by the MindConnect component.<br>• Deployment of customer's own software and third-party software through the MindConnect component |
| c) | **Reference to RAMI 4.0** | *No information available* |

| T16. Other technical abilities |
| --- |
| Extensive highly customizable capabilities in various task areas in IIoT via the application of specific product packages:<br>• MindSphere Connect and Monitor Solution Package<br>• MindSphere Digitalize and Transform Solution Package<br>• MindSphere Connect and Monitor Solution Package |

| T17. References |
| --- |
| • Overview of the Platform:<br>○ https://siemens.mindsphere.io/en<br>○ https://new.siemens.com/global/de/produkte/software/mindsphere.html<br>• Whitepaper „ MindSphere security model Version 1.0“, Siemens AG<br>• Whitepaper „MindSphere“, Siemens AG<br>https://mindsphereworld.de<br>• Information on the partner network and overview for developers and operators:<br>○ https://siemens.mindsphere.io/en/partner<br>○ https://siemens.mindsphere.io/en/about/for-developers<br>○ https://siemens.mindsphere.io/en/about/for-operators<br>○ https://siemens.mindsphere.io/en/community<br>• MindSphere store:<br>https://siemens.mindsphere.io/en/store<br>• Product packages of the platform:<br>○ https://www.plm.automation.siemens.com/global/en/products/iot/connect-monitor-capabilities.html<br>○ https://www.plm.automation.siemens.com/global/en/products/iot/digitalize-transform-capabilities.html<br>○ https://www.dex.siemens.com/mindsphere/mindsphere-packages/analyze-and-predict<br>• Documentation of the platform for developers:<br>○ https://documentation.mindsphere.io/resources/html/release-notes/en-US/135643676683.html<br>○ https://documentation.mindsphere.io/resources/html/release-notes-hardware/en-US/133001948043.html<br>○ https://developer.mindsphere.io/concepts/concept-architecture.html<br>○ https://developer.mindsphere.io/resources/mindsphere-webcomponents/index.html<br>○ https://developer.mindsphere.io/apis/index.html<br>○ https://developer.mindsphere.io/apis/advanced-assetmanagement/api-assetmanagement-overview.html<br>○ https://developer.mindsphere.io/howto/howto-app-mendix-development.html<br>○ https://design.mindsphere.io/<br>○ https://design.mindsphere.io/patterns/introduction.html<br>• Security model:<br>https://assets.new.siemens.com/siemens/assets/api/uuid:6b876b5e-5594-4da4-90e0-e9e0c6f1f1e1/version:1557483304/siemens-plm-mindsphere-security-model-wp-75966-a7.pdf<br>• GitHub Repository for MindSphere:<br>https://github.com/mindsphere |

## 3.19 Software AG – Cumolocity

| T1. Overview | | |
|---|---|---|
| a) | **Name of the platform** | Cumolocity IoT Platform |
| b) | **Platform vendor or provider** | Software AG, Darmstadt, Germany |
| c) | **Vendor summary** | *„Cumulocity IoT is the #1 low-code, self-service IoT platform—the only one that comes pre-integrated with the tools you need for fast results: device connectivity and management, application enablement and integration, as well as streaming and predictive analytics."* |
| d) | **Platform components** | Cumulocity IoT |
| e) | **Online marketplace platform** | *No information available* |
| f) | **Mobility platform** | Was used in the area of fuel consumption (fuel consumption optimization) |
| g) | **B2B context** | Yes |
| h) | **B2C context** | *No information available* |
| i) | **Platform users** | Asset manager, application user |
| j) | **Fields of application** | • Avoidance of downtime<br>• Telematics / fuel consumption<br>• Condition monitoring<br>• Real-time analytics, e.g., real-time fault detection<br>• Device and data management, remote configuration |
| k) | **Market penetration** | Deutsche Telekom, Trailar, Gardner Denver |

| T2. License information | | |
|---|---|---|
| | | Cloud-based subscription model |

| T3. Protocols | | |
|---|---|---|
| | | • Modbus, CAN bus and OPC-UA, MQTT, REST, SmartREST, SmartREST2 etc.<br>• No development required |

| T4. Edge support | | |
|---|---|---|
| | | • Deploy microservices anywhere, including to the cloud<br>• System can be virtualized or installed on edge devices/edge servers. |

| T5. IIoT devices | | |
|---|---|---|
| a) | **Device connectivity** | See protocols (T3) |
| b) | **Device management** | • Manage all devices from a single tool.<br>• Register and update any number of devices.<br>• Centrally manage error conditions, hardware information, alarms, and performance or device statistics. |
| c) | **Deployment, provision of software** | Manage software/firmware and software (device) configurations centrally |

| T6. Security | | |
|---|---|---|
| | | Industry strong security („Branchenstarke Sicherheit"), no VPN required. |

| T7. Data protection |
|---|
| • Locally-autonomous high-performance edge processing: autonomous control and sophisticated data processing on a high volume near the data source is possible.<br>• Restriction of access to managed objects<br>• Management of roles and assignment of permissions |

| T8. Cloud support |
|---|
| • Can be installed on-premise or on edge devices<br>• Multi-tenancy<br>• Microservices can be distributed to the cloud |

| T9. Scalability |
|---|
| Can grow dynamically (as needed) and can also shrink. |

| T10. Digital twins / Asset Administration Shells |
|---|
| *No information available* |

| T11. Data management and data analysis |
|---|
| • Extensible data model<br>• Real-time data processing using Apama Streaming Engine<br>• Programmable via Apama Event Processing Language (EPL) |

| T12. Offered AI methods |
|---|
| *No information available* |

| T13. Openness and Extensibility | | |
|---|---|---|
| a) | **Store** | *No information available* |
| b) | **App support for/by developers** | • Two types of Apps are supported: Web-based user interface applications and server-side business logic in the form of microservices.<br>• Certified software libraries<br>• APIs to extend Cumulocity<br>• Use of the same APIs or interface technology for all use cases (HTTP, HTTPS, REST) |
| c) | **Use of "external" algorithms/data** | Apama EPL, extensible data model |
| d) | **AI interfaces** | • https://cumulocity.com/guides/device-sdk/device-sdk-introduction<br>• https://cumulocity.com/guides/microservice-sdk |

| T14. Systematic Configurability |
|---|
| • Re-branding<br>• Platform configuration (users, security, data retention rules) |

| T15. Ecosystem support | | |
|---|---|---|
| a) | **"Multi-Sided" platform** | Dozens of connectors or more than 170 integrated enterprise/cloud-Apps to/with SAP®, Salesforce®, ServiceNow®, Microsoft® Dynamics®, Zendesk®, Zuora®, Marketo® and Microsoft® Office 365® |
| b) | **Open to third-party content** | *„The only completely open platform"*, various APIs to extend Cumulocity, e.g., IoT agents |
| c) | **Reference to RAMI 4.0** | *No information available* |

| T16. Other technical abilities |
| --- |
| • Microservice architecture (deploy it anywhere)<br>• Virtualization support through Docker containers |

| T17. References |
| --- |
| • https://www.softwareag.com/en_corporate/platform/iot.html<br>• https://cumulocity.com/guides/reference/applications<br>• https://cumulocity.com/guides/concepts/domain-model<br>• https://cumulocity.com/guides/concepts/realtime#using-epl<br>• https://cumulocity.com/guides/apama/introduction<br>• https://cumulocity.com/guides/reference/device-management<br>• https://cumulocity.com/guides/reference/sensor-library<br>• https://cumulocity.com/guides/concepts/interfacing-devices<br>• https://cumulocity.com/guides/concepts/security<br>• https://cumulocity.com/guides/edge/installation<br>• Cumolocity Web Book: Dream IoT. Achieve IoT. |

## 3.20 S&T – SUSiEtec

| T1. Overview | | |
|---|---|---|
| a) | **Name of the platform** | SUSiEtec |
| b) | **Platform vendor or provider** | Kontron Technologies, S&T group, Linz, Österreich |
| c) | **Zusammenfassung des Anbieters** | *"SUSiEtec offers…*<br>*A great number of ways of mastering precisely those challenges arising in the Insutrial IoT networks. Our objective is to meet the user's needs for a greater speed, security and ease of access to the information required."* |
| d) | **Platform components** | • SusieTech Framework<br>• SusieTech IoT |
| e) | **Online marketplace platform** | *No information available* |
| f) | **Mobility platform** | Supports mobile devices in production/manufacturing |
| g) | **B2B context** | Yes |
| h) | **B2C context** | *No information available* |
| i) | **Platform users** | Industry 4.0 personnel (machine operators, plant supervisors) |
| j) | **Fields of application** | IoT, Industry 4.0 |
| k) | **Market penetration** | *No information available* |

| T2. License information | |
|---|---|
| | "Optimized pricing using subscription model" |

| T3. Protocols | |
|---|---|
| | Configurable connectors, no detailed information found |

| T4. Edge support | | |
|---|---|---|
| a) | **Overview** | „Edge analytics" to control time-critical processes on site |
| b) | **Communication** | *No information available* |
| c) | **Memory usage** | Cache, compress, and share data |
| d) | **Specific capabilities** | *No information available* |

| T5. IIoT devices | | |
|---|---|---|
| a) | **Device connectivity** | Secure authentication and communication |
| b) | **Device management** | • Data-/Asset register, lifelong device management<br>• Bulk processes<br>• Telemetry reporting<br>• Datea monitoring and analysis in real-time |
| c) | **Deployment, provision of software** | • Yocto-based operating system (SUSiEtec OS)<br>• Configurable roll-out<br>• Software or component drivers and software can be deployed to devices<br>• Support for Docker Swarm Management<br>• REST interface |

| T6. Security | |
|---|---|
| | • Certificates, encryption<br>• Secure interface for remote updates/deployment<br>• Firewalls (adjustable via secure web interface)<br>• Yocto-based SUSiEtec Secure operating system, penetration test |

| T6. Security |
|---|
| • Secure interface for remote updates/deployment<br>• Firewalls (adjustable via secure web interface)<br>• Yocto-based SUSiEtec secure operating system, penetration test<br>• 1 week update cycle for critical vulnerabilities |

| T7. Data protection |
|---|
| Shares many aspects with security (T6):<br>• Ensures that all access is authenticated and authorized<br>• All communications are encrypted<br>• All software and firmware are updated regularly<br>• Data protection at the edge and in the cloud<br>• Watchdog functionality<br>• Emergency response to critical vulnerabilities<br>• Customized updates<br>• Notifications about updates and vulnerabilities |

| T8. Cloud support |
|---|
| • On-premise, in the cloud (MS Azure) and hybrid<br>• Software can run dedicated in the cloud (cloudlets). |

| T9. Scalability |
|---|
| Scalable to millions of parallel devices (*„Skalierbar auf Millionen paralleler Geräte“*) |

| T10. Digital twins / Asset Administration Shells |
|---|
| *No information available* |

| T11. Data management and data analysis |
|---|
| *No information available* |

| T12. Offered AI methods |
|---|
| Machine learning: The fusion of IT and OT enables autonomous action and adaptation of the machines used to new circumstances. This means autonomous utilization of sensor data in real time. (*„Machine learning: Die Verschmelzung von IT und OT ermöglicht ein autonomes Handeln und Anpassen der eingesetzten Maschinen an neue Gegebenheiten. Das heißt selbständiges Verwerten von Sensordaten in Echtzeit.“)* |

| T13. Openness and Extensibility | | |
|---|---|---|
| a) | **Store** | *No information available* |
| b) | **App support for/by developers** | • Universal Platform Apps (UPA)<br>• End-user programs on mobile devices only, if applicable |
| c) | **Use of “external” algorithms/data** | Apparently customer Apps possible, no detailed information available |
| d) | **AI interfaces** | *No information available* |

| T14. Systematic Configurability |
|---|
| • Support for functionality on different devices<br>• *“SUSiEtec can be configured flexibly and adapts to existing automation solutions to collect and analyze telemetry”* |

| T15. Ecosystem support |
| --- |
| *No information available* |

| T16. Other technical abilities |
| --- |
| • Based on Windows 10 IoT<br>• Based on Docker or isolated containers |

| T17. References |
| --- |
| • https://www.kontron.com/products/iot/iot-industry-4.0/iot-software-and-services/susietec/<br>• https://susietec.com/<br>• https://www.kontron.de/iot/iot-software-and-services<br>• SUSiEtec - The Application Ready - IoT Framework, Brochure |

## 3.21 Weidmüller - Industrial Analytics

| T1. Overview | | |
|---|---|---|
| a) | **Name of the platform** | Industrial Analytics |
| b) | **Platform vendor or provider** | Weidmüller Interface GmbH & Co. KG, Detmold, Germany |
| c) | **Vendor summary** | *"The Industrial Analytics offering from Weidmüller stands for application-oriented AI applications to help you detect and classify anomalies, thereby effectively reducing downtimes. Through predictive maintenance, you can plan service intervals in a targeted manner as and when required. What's more, you can make reliable predictions with regard to the quality of your products (predictive quality), based on seamless recordings of sensor, condition and process data. "* |
| d) | **Platform components** | Model builder (ML runtime enviornment) |
| e) | **Online marketplace platform** | *No information available* |
| f) | **Mobility platform** | *No information available* |
| g) | **B2B context** | Yes |
| h) | **B2C context** | *No information available* |
| i) | **Platform users** | Plant supervisor, if necessary also machine operator (due to ML approach) |
| j) | **Fields of application** | • Predictive Quality<br>• Condition Monitoring<br>• Predictive Maintenance |
| k) | **Market penetration** | Reference projects with Borge (air, compressors), Grenzebach |

| T2. License information | |
|---|---|
| | *No information available* |

| T3. Protocols | |
|---|---|
| | *No information available* |

| T4. Edge support | |
|---|---|
| | *No information available* |

| T5. IIoT devices | |
|---|---|
| | *No information available* |

| T6. Security | |
|---|---|
| | *No information available* |

| T7. Data protection | |
|---|---|
| | *No information available* |

| T8. Cloud support | |
|---|---|
| | • Cloud usage is optional, the ML runtime environment can also be installed runtime environment for ML models.<br>• Cloud support for example for Azure, AWS or IBM Cloud. |

| T9. Scalability | |
|---|---|
| | *No information available* |

**T10. Digital twins / Asset Administration Shells**

*No information available*

**T11. Data management and data analysis**

*No information available*

**T12. Offered AI methods**

- Model Builder: Create your own ML models without prior knowledge through automated model generation.
- Detect misbehavior in machines
- Predictive Quality

**T13. Openness and Extensibility**

*No information available*

**T14. Systematic Configurability**

*No information available*

**T15. Ecosystem support**

*No information available*

**T16. Other technical abilities**

*No information available*

**T17. References**

- https://www.weidmueller.de/de/loesungen/industrial_analytics/automated_machine_learning.jsp
- https://www.weidmueller.com/int/solutions/industrial_analytics/index.jsp
- Die digitale Transformation in der Industrie - Predictive Maintenance mit Industrial Analytics (Whitepaper)

# 4 Evaluation of the Platforms

We now analyze the platforms presented in Chapter 3 using the analysis topics from Section 2.1, i.e., we provide an overview of the results per analysis topic across all platforms and discuss cross-links. A separate sub-chapter/section is dedicated to each analysis topic. The sub-chapters are discussed according to the sequence from Section 2.1, although we group some related analysis topics thematically into common sub-chapters for ease of readability/argumentation, e.g., cloud usage (T8) and scalability (T9) or data management/data analytics (T11) and AI capabilities (T12).

When naming platforms, we usually use both the vendor and the platform name to avoid confusion. Even if "Adamos Adamos" would be correct in this respect, the duplication looks more like a typo. Therefore, we use only the shorter vendor or platform name. For long names, especially in illustrations, we may use only the vendor name, e.g., for "Recogizer Analytics", or short forms for the vendor name, e.g., "E&H" for "Endress + Hauser".

## 4.1 Overview Information

In this section, we provide an aggregated overview of the analyzed platforms based on the respective overview information (T1). In this analysis topic, we discuss the countries of origin (T1.b), the fields of use mentioned by the vendors (T1.j), the B2B context (T1.g) and the B2C context (T1.h), as well as a use as a mobility platform (T1.f).

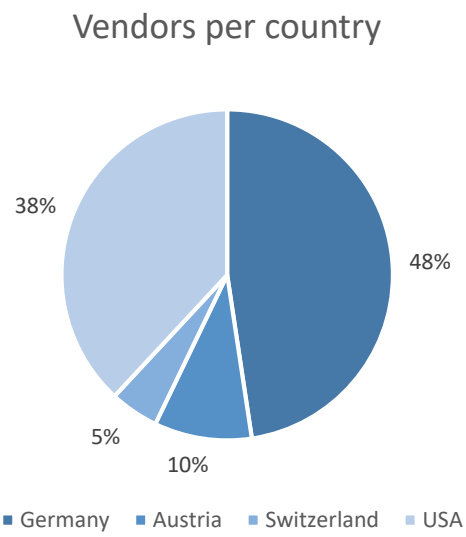



*Figure 1: Country distribution of platform vendors/providers.*

Figure 1 shows the distribution of countries of origin for the analyzed platforms. Most platform vendors are represented (with headquarters) in Germany (48%) and Europe (63%). This selection of vendors can be explained in part by a focus on "Industry 4.0", a concept which is frequently used in German-speaking countries. However, the distribution has changed significantly due to the addition of further platform vendors as a result of partner proposals in IIP-Ecosphere (see also Section 2.2). The original selection in the competitive phase of IIP-Ecosphere, which was based on the revenues of the vendors, included 57% vendors from USA and 43% from Germany. For both, the competitive phase and in this white paper, the vendor selection is international, but mainly containing vendors from Europe or Germany.

The identified **fields of application** are relatively diverse and cover both, industrial sectors and application fields. Sixteen different sectors were mentioned, in particular smart home/building/city (5), manufacturing (4), (intra-)logistics (3), and transportation systems (2). Among the applications, the

management of devices/machines and their data (9), (cloud-based) application development (8), condition monitoring (5), as well as failure safety (3), predictive maintenance (3) and energy management (3) are named in particular.

Unsurprisingly, we found a B2B context for all analyzed platforms. For one platform (IBM Watson IoT Suite, 5%) we identified a B2C context, for Google Cloud IoT Core as well as Siemens MindSphere (together 10%) there are potential indications for a B2C context, while for 24% of the platforms a B2C context is not mentioned and for the remaining 62% the B2C context information is unclear.

More than half of the platforms (57%) can be used as mobility platforms or offer corresponding services, and possible indications of mobility support can be identified for a further 29%. For one platform (PTC ThingWorx), mobility support could be ruled out based on the available information, while this is unclear for the remaining 10%.

## 4.2 Licenses

Two platform vendors do not provide any information about their licensing model. The remaining 90% can be categorized as commercial. One platform (E&H Netilion) offers a free entry-level license. 19% of all platforms surveyed offer entry-level packages. 5 platform providers (23%) offer a pay-per-use/pay-as-you-go licensing model, of which three platform providers exclusively rely on such a licensing model. 33% of the platform providers mention that their platform uses open source libraries.

## 4.3 Protocols

Currently, there is a variety of communication protocols in the field of Industry 4.0, in particular also due to the requirement to connect recent platforms with (retrofitted, legacy) machines that were procured in the past, e.g., before the age of Industry 4.0. Recently attempts have been made to achieve universal standardization here. Thus, it is not surprising that almost all platform vendors (17) have created a wide variety of extensions that either vendors, service providers or even customers can use to integrate their required protocols. While some platforms advertise more than a hundred protocols (Adamos, Emerson Plantweb, GE Predix), Siemens MindSphere offers "the largest possible number of devices and protocols." Software AG Cumolocity emphasizes that no programming is needed to use the various protocols, while Recogizer Analytics mentions that any connection is made possible.

| | Adamos | Amazon AWS IoT | Bosch IoT Suite | B&R mapp Technology | Cisco Kinetic | DeviceInsight Centersight | Emerson Plantweb | E&H Netilion | GE Predix | Google Cloud IoT Core | Harting MICA | IBM Watson IoT Suite | Microsoft Azure IoT Suite | Oracle Cloud IoT | PTC ThingWorx | Recogizer Analytics | SAP Leonardo | Siemens MindSphere | Software AG Cumulocity | S&T SUSiEtec | Weidmüller Ind. Analytics |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AMQP | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ |
| Canbus | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ |
| Fieldbus | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| HTTP/REST | ● | ● | ● | ○ | ○ | ● | ○ | ● | ● | ● | ● | ○ | ● | ● | ● | ● | ● | ● | ● | ○ | ○ |
| LPWAN | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ● | ○ | ○ | ○ |
| MODBUS | ● | ○ | ○ | ○ | ○ | ● | ● | ● | ● | ○ | ● | ○ | ○ | ○ | ○ | ● | ● | ● | ● | ○ | ○ |
| MQTT | ● | ● | ● | ● | ● | ● | ○ | ○ | ● | ● | ● | ● | ● | ● | ○ | ● | ● | ○ | ● | ○ | ○ |
| OPC-UA | ● | ○ | ○ | ● | ○ | ● | ● | ○ | ● | ○ | ● | ○ | ○ | ○ | ○ | ● | ● | ● | ● | ○ | ○ |
| Profibus | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| SNMP | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ |

*Figure 2: Summary of mentioned (relevant) protocols per platform.*

In the individual platform descriptions in Chapter 3, we identified 37 different protocol families. A selection of these is shown in Figure 2. We only include the most frequently mentioned protocol families or those most relevant to IIP-Ecosphere here, also because the listing is not complete as some vendors do not specify all implemented protocols while other vendors even do not specify a concrete protocol at all. The most frequently mentioned protocol families are: http/REST/JSON (15), MQTT (15), MODBUS (10), OPC-UA (10), and AMQP (4). From the statements of the vendors it can further be deduced that there is a trend towards a few unified protocols, e.g., OPC-UA and MQTT in addition to the ubiquitous REST for API access.

## 4.4 Edge Support

The use of edge devices is supported by most of the platforms considered. Only 3 platforms did not provide any information on this. However, the degree of support or use of edge devices varies significantly between the platforms. Figure 3 provides an overview of the various capabilities, the applications of edge devices, the support by the respective platform as well as dedicated components of the platforms to support edge devices, such as specialized operating systems or components within a platform.

Regarding storage usage of edge devices, 52% of the platforms support cloud storage, while 67% support both, cloud storage and partially persistent local storage on edge devices. Support for fog storage is explicitly mentioned by only 2 platforms.

| | Adamos | Amazon AWS IoT | Bosch IoT Suite | B&R mapp Technology | Cisco Kinetic | DeviceInsight Centersight | Emerson Plantweb | E&H Netilion | GE Predix | Google Cloud IoT Core | Harting MICA | IBM Watson IoT Suite | Microsoft Azure IoT Suite | Oracle Cloud oT | PTC ThingWorx | Recogizer Analytics | SAP Leonardo | Siemens MindSphere | Software AG Cumulocity | S&T SUSIEtec | Weidmüller Ind. Analytics |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ED cloud storage | ○ | ● | ○ | ○ | ● | ○ | ○ | ● | ● | ● | ○ | ● | ● | ● | ○ | ● | ● | ● | ○ | ○ | ○ |
| ED fog storage | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ |
| ED local storage | ○ | ● | ● | ● | ● | ● | ○ | ● | ● | ● | ○ | ○ | ● | ● | ● | ● | ○ | ● | ○ | ● | ○ |
| Bidir. Comm. | ○ | ● | ● | ○ | ● | ○ | ○ | ○ | ● | ● | ● | ○ | ● | ● | ● | ○ | ● | ● | ○ | ○ | ○ |
| 3rd party apps on ED | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ |
| Customer-Apps on ED | ○ | ● | ○ | ○ | ○ | ● | ○ | ○ | ● | ○ | ○ | ○ | ● | ○ | ● | ○ | ○ | ● | ○ | ○ | ○ |
| AI/ML for ED | ○ | ● | ● | ○ | ● | ○ | ○ | ○ | ● | ○ | ○ | ○ | ● | ○ | ○ | ○ | ● | ● | ○ | ○ | ○ |
| Long-term store ED | ○ | ● | ● | ● | ● | ○ | ○ | ○ | ● | ○ | ○ | ○ | ● | ○ | ○ | ○ | ● | ● | ○ | ○ | ○ |
| Ded. edge PF-comp. | ○ | ● | ○ | ○ | ● | ○ | ○ | ○ | ● | ○ | ○ | ○ | ● | ○ | ● | ○ | ● | ● | ○ | ○ | ○ |
| Edge OS | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Edge middleware | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ● | ○ | ○ | ○ |
| Gateway support | ○ | ● | ● | ○ | ● | ○ | ○ | ○ | ● | ● | ○ | ● | ● | ● | ● | ○ | ● | ● | ○ | ○ | ○ |
| Man. SW updates | ○ | ● | ● | ○ | ● | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| ED cloud services | ○ | ● | ● | ○ | ● | ○ | ○ | ○ | ● | ● | ● | ● | ● | ● | ○ | ○ | ● | ● | ● | ○ | ○ |
| Edge analytics | ○ | ● | ● | ○ | ● | ● | ○ | ○ | ● | ● | ○ | ● | ● | ○ | ○ | ○ | ● | ● | ○ | ● | ○ |
| Edge preprocess. | ○ | ● | ● | ● | ● | ○ | ○ | ○ | ● | ○ | ○ | ● | ● | ○ | ○ | ○ | ● | ● | ○ | ● | ○ |
| Lifecycle mgt. | ○ | ● | ● | ○ | ● | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |

*Figure 3: Edge device (ED) support by the individual platforms.*

Bidirectional communication of edge devices, i.e., sending of device data from the IoT devices controlled by the edge devices to the platform and the receiving of control instructions and updates from the platform in controlled IoT devices, is mentioned by 52% of the platforms. The number of platforms that directly support the execution of customer-specific applications (29%) as well as third-party applications (14%) on edge devices is relatively low. This low number can be partially explained

by the trend towards using web services or cloud-based services (57% of platforms). Likewise, only 33% of platforms support the execution of AI or ML procedures directly on edge devices and 38% support the long-term storage of data on edge devices. This can also be explained by the pronounced use of cloud services. What is striking here is that the aforementioned functions for executing applications, AI/ML processes and the long-term storage of data on edge devices are often supported by platforms that provide a dedicated edge management component (33%). A dedicated edge operating system is offered only by GE Predix and AWS IoT. A dedicated edge middleware is similarly rare and offered only by Bosch IoT Suite, PTC ThingWorx, SAP Leonardo, and Siemens MindSphere. Analogous to the support for a variety of protocols already noted in Section 4.3, 52% of the platforms offer gateway software for edge environments for this purpose. In addition to these gateways, to support a wide variety of protocols, 62% of the platforms support MQTT for edge devices.

Pre-processing of data to edge devices is supported by 48% of platforms. The support of edge analytics is indicated by 52% of the platforms.

Management of software updates for edge devices, support of lifecycle management of edge devices, as well as the IoT devices connected to them, are only offered by 4 platforms. Again, support for both of these functions correlates.

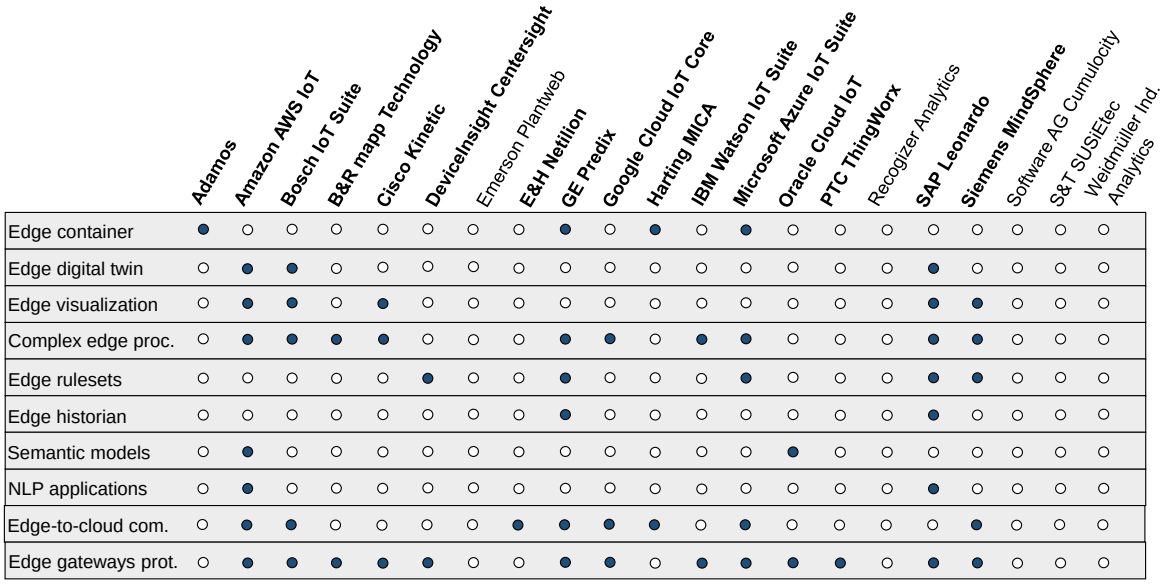



*Figure 4: Specific edge capabilities offered by the platforms.*

The general overview in Figure 3 shows that 7 of the platforms are considered to offer strong support for edge devices. These platforms are: Amazon AWS IoT, Bosch IoT Suite, Cisco Kinetic, GE Predix, Microsoft Azure IoT Suite, SAP Leonardo, and Siemens MindSphere.

In terms of supporting particular capabilities of edge devices (see Figure 4), we identified the following capabilities:

- The execution of applications directly on edge devices in containerized form, mostly implemented via Docker containers, is explicitly supported by 4 of the platforms. It is possible that other platforms that generally support deployment in containers can be added here, which may not have explicitly specified container-based deployment to edge devices but generally support containerized deployment.

- The use of digital twins, specifically related to edge devices, such as for their simulation or for the realization of device shadows, is only supported by 4 of the platforms considered, namely Amazon AWS IoT, Bosch IoT Suite and SAP Leonardo.
- Visualization of edge federations, i.e., edge devices and the IoT devices they control as a device federation, is also supported by only 5 platforms (24%).
- Strikingly common for a particular edge capability is support for processing data, i.e., going beyond simple data preparation to complex processing of data, such as analytics capabilities, directly on edge devices. 48% of the platforms mention support this functionality for edge devices.
- The application of rule sets on edge devices, such as for simple tax decisions, is supported by 24% of the platforms considered.
- A rare functionality is the support of historian databases on edge devices (supported by only 2 platforms). This is likely an effect of the preference for storing larger amounts of data, typically required for historian databases, in cloud-based solutions.
- Semantic modeling of devices, device federations, and processes for edge devices is offered by only 2 platforms, namely Amazon AWS IoT and Oracle Cloud IoT. Both platforms use this support to further support graphical modeling tools, such as process modeling for edge devices.
- The creation and use of natural language (NLP) applications on edge devices is also only supported by 2 platforms, again Amazon AWS IoT as well as SAP Leonardo.
- The possibility of direct communication between edge devices and cloud services is supported by 38% of the platforms. This communication can be used by edge devices to proactively address web services with messages, for example alerts, instead of just passively responding to a query from web services.
- The provision of edge gateways to offer a wide range of protocols for edge devices occurs in 62% of the platforms. This comparatively high level of support allows for easily incorporating the largest possible number of protocols and connected IoT devices using these protocols, especially legacy structures in existing IIoT and IoT environments.

Two of the platforms considered, Amazon AWS IoT and SAP Leonardo, stand out for their high level of support for particular edge functionality, which is also reflected in their generally broad support for edge devices.

## 4.5 IIoT Devices

Most platform descriptions (95%) indicate a respective support for IIoT devices. Figure 5 illustrates the individual support per platform.

| | Adamos | Amazon AWS IoT | Bosch IoT Suite | B&R mapp Technology | Cisco Kinetic | DeviceInsight Centersight | Emerson Plantweb | E&H Netilion | GE Predix | Google Cloud IoT Core | Harting MICA | IBM Watson IoT Suite | Microsoft Azure IoT Suite | Oracle Cloud IoT | PTC ThingWorx | Recogizer Analytics | SAP Leonardo | Siemens MindSphere | Software AG Cumulocity | S&T SUSiEtec | Weidmüller Ind. Analytics |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3rd party devices | ○ | ○ | ● | ○ | ● | ○ | ○ | ○ | ● | ○ | ○ | ● | ● | ● | ● | ○ | ● | ● | ○ | ○ | ○ |
| On/off-boarding | ● | ● | ● | ◖ | ● | ○ | ○ | ○ | ● | ● | ● | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ |
| Autom. assignment | ● | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ● | ● | ○ | ○ | ● | ● | ○ | ● | ○ | ○ | ○ | ○ |
| Remote acc./conf. | ● | ● | ● | ● | ○ | ● | ○ | ● | ● | ● | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Monitoring | ○ | ● | ○ | ○ | ● | ○ | ● | ● | ● | ● | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ● |
| Lifecycle | ○ | ● | ● | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ |
| Backup/Restore | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| REST-API | ○ | ● | ● | ○ | ● | ● | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ● | ○ |
| OTA update | ○ | ● | ● | ○ | ○ | ● | ○ | ○ | ● | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ● | ● | ● | ○ |
| Bulk update | ○ | ○ | ● | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ |

*Figure 5: Support for IIoT devices per platform.*

We now summarize the named capabilities by sub-topic:

- Device connections (Figure 5, first row):
  - 29% of the considered platforms detail the technology used or required to connect IIoT devices, e.g. Amazon Greengrass Framework, Bosch IoT Gateway, B&R's dedicated services or devices (GateManager, Machine Pool Management System, KeySwitch) or Kinetic's gateways.
  - Except for Harting MICA, all platforms probably support third-party devices or third-party protocols. However, this is only explicitly mentioned by 43% of the platforms.
- Device management (Figure 5, rows 2-7):
  - 42% of platforms mention a (specific) form of onboarding and offboarding of IIoT devices. Of these, 7 platforms (33% of all platforms) offer techniques for automated assignment of IIoT devices to a management structure, e.g. via device templates.
  - 43% of the platforms mention support for remote control or remote access to IIoT devices.
  - 43% of platforms mention some form of (runtime) monitoring for IIoT devices. Google Cloud IoT Core talks about real-time monitoring.
  - Five platforms (24%) provide some form of lifecycle management for IIoT devices.
  - Two platforms (10%) support backup, restore, or rollback operations for IIoT software or configurations.
- Deployment (Figure 5, rows 8-10):
  - 38% of platforms support OTA updates for IIoT devices.
  - 33% offer a REST interface for deployment, most of them in conjunction with a cloud service (SaaS).
  - Three platforms (14%) allow bulk deployment operations.
  - 19% of the platforms support container-based deployment, using Docker or to deploy individual functions (Amazon AWS IoT), microservices (Deviceinsight Centersight), or machine learning models (Google Cloud IoT Core).
  - 14% of the platforms use specific libraries or operating systems on the IIoT devices, e.g., FreeRTOS (Amazon AWS IoT), automation runtime kernel (B&R mapp Technology), or Yocto Linux (S&T SUSiEtec).

Amazon AWS IoT and Google Cloud IoT Core support transparent access to devices (twins) that are temporarily offline. Furthermore, Amazon AWS IoT offers voice integration with Alexa and SAP Leonardo ships with specific chat functionalities.

## 4.6 Security

In this section, we discuss the results for the analysis topic "Security". We highlight the following three aspects here: 1) protecting the integrity of software and information, 2) preventing unauthorized access to network services, and 3) protecting the confidentiality, authenticity, or integrity of information through cryptographic mechanisms. These three aspects are explicitly mentioned in the list of measures from Annex A of the ISO/IEC 27001 standard and are covered by the thematic questions for T6 in Section 2.1.

Integrity is an important component of software security as "prevention of unauthorized modification of information". As shown in Figure 6, almost two-thirds of the platforms (62%) name functions for protecting the integrity of software and information. Only 14% of the platforms offer no support when it comes to protecting the integrity of software and information.

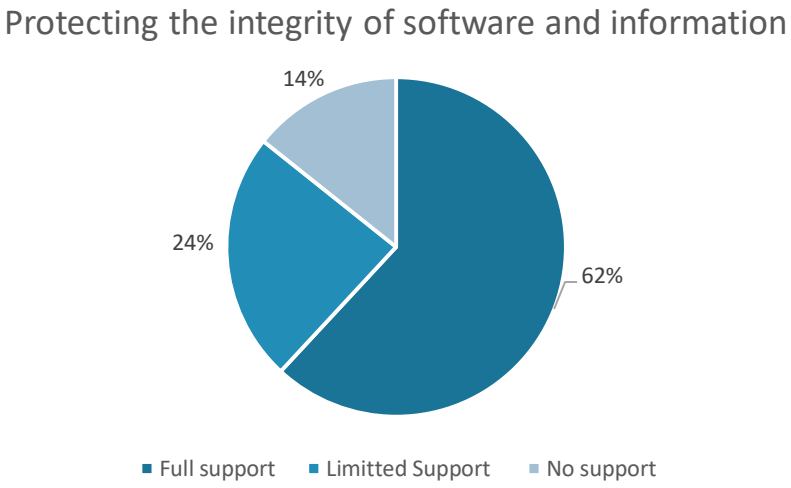



*Figure 6: Protection of the integrity of software and information.*

Figure 7 provides evidence that a majority of platforms (86%) offer appropriate mechanisms to prevent unauthorized access to network services. In the course of our analysis, we found that only 14% of the IIoT platforms do not specify any mechanisms to prevent unauthorized access to network services.

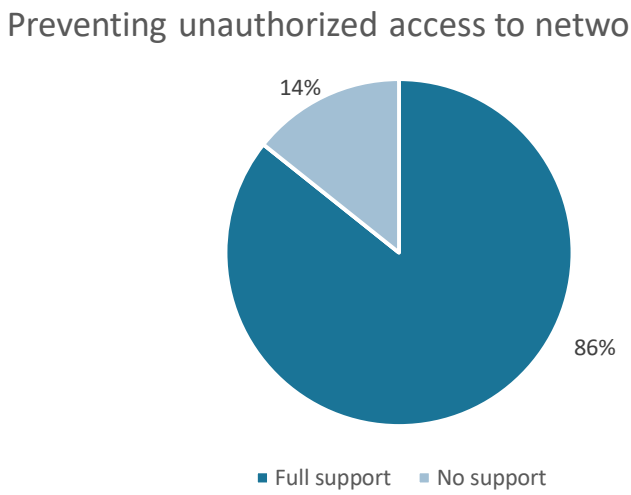



*Figure 7: Unauthorized access to network services.*

Often a cryptographic mechanism can be used for different purposes, e.g. to protect confidentiality, authenticity or integrity of information. Based on our analysis, only two platforms (10%, DeviceInsight Centersight and Weidmüller Analytics) do not provide any mechanisms for protecting the confidentiality, authenticity, or integrity of information using cryptographic mechanisms. 90% of the platforms, on the other hand, provide corresponding support.

## 4.7 Data Protection

In this section, we discuss the findings on data protection of the platforms examined. A number of requirements for processing of personal data arise from the GDPR. Not all of these requirements can be addressed by purely technical measures; however, many require effective technical support to fulfill them. In the following, three aspects will be discussed: 1) the ability to identify personal data (to understand the applicability of the GDPR), 2) limited storage and retention period, and 3) data protection through technology design and through privacy-friendly default settings.

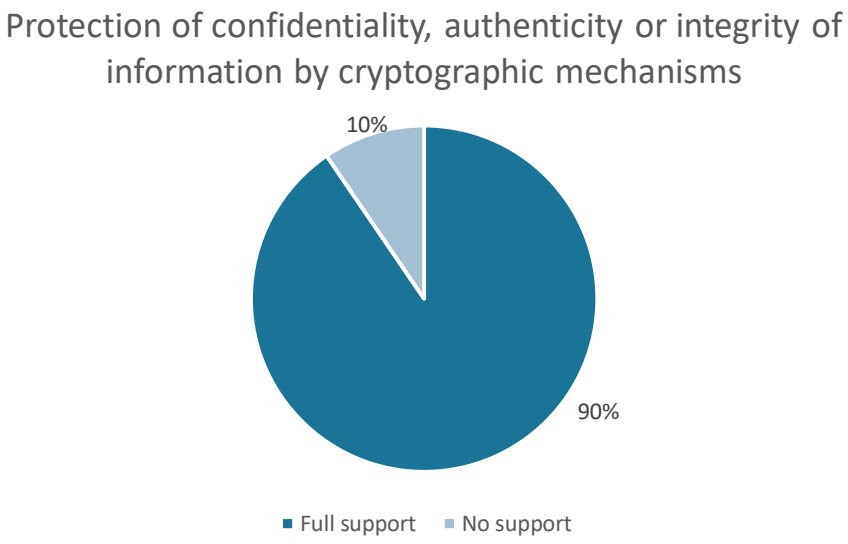



*Figure 8: Confidentiality, authenticity or integrity of information through cryptographic mechanisms.*

Only a quarter (28%) of the platforms studied provide appropriate mechanisms to detect the processing of personal data. Almost half of the platforms offer limited support. 24% of the platforms do not offer any possibility to detect the dissemination of personal data.

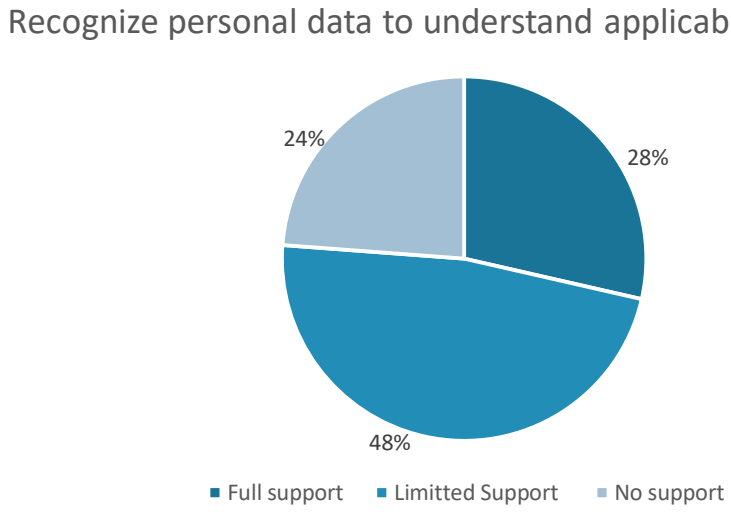



*Figure 9: The recognition of personal data.*

In view of the principles governing the processing of personal data, personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed (Article 5, GDPR). After that, they must be deleted or their storage limited. A majority of the platforms surveyed (71%) designate appropriate mechanisms to support limited storage, retention period and limited processing of personal data. Only four platforms do not offer any support (B&R mapp Technology, Deviceinsight Centersight, S&T SUSiEtec and Weidmüller Analytics).

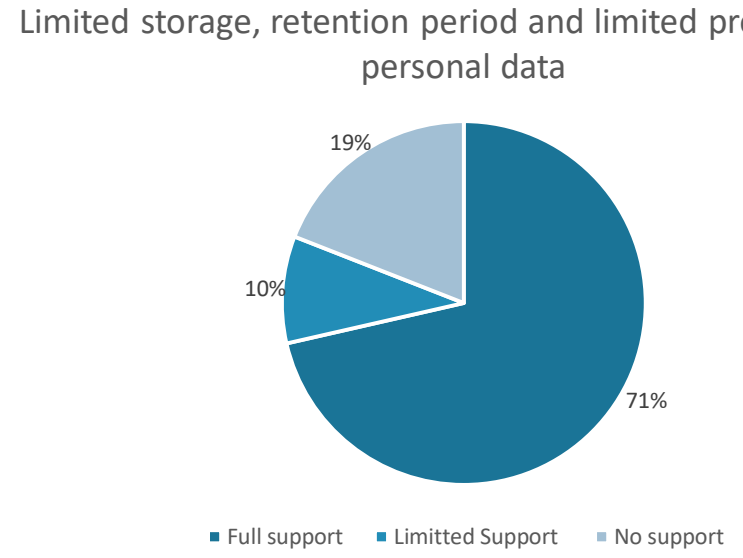



*Figure 10: Limited data storage and processing.*

Data protection by design is not a new principle. However, with the legal obligation of the GDPR, there is a legal motivation (Article 25) to implement data protection by design. Only two platforms (10%) name suitable mechanisms for this purpose. 38% of the platforms offer no support.

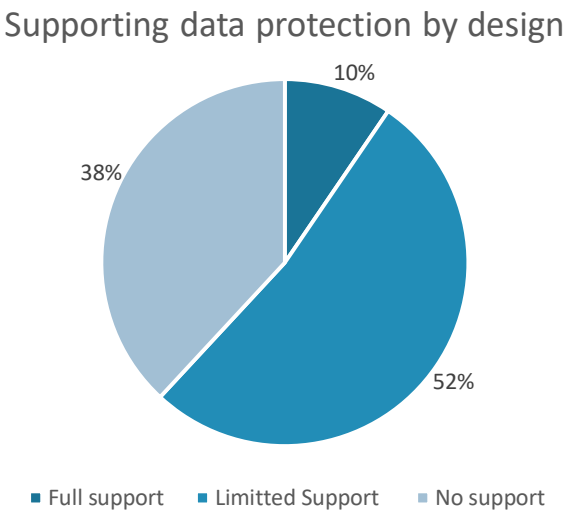



*Figure 11: Article 25 GDPR - Data protection by design.*

## 4.8 Cloud Support and Scalability

We discuss now the results for cloud usage and platform scalability. We have combined these two analysis topics here, because scalability is often argued or realized through cloud technology.

95% of the platforms offer integration with cloud technology. Only for Harting MICA such support was not clearly described ("MICA connects machines with cloud services"). For 19% of the platforms (Adamos, B&R mapp Technology, S&T SUSiEtec, Weidmüller Industrial Analytics) cloud support is mentioned as optional. For the other platforms, it can be assumed that the respective platform runs in a (vendor) cloud on a mandatory basis. 24% of the platforms allow on-premise installation, whereby only for Adamos optional cloud integration and on-premise installation are mentioned. 15% of the platforms explicitly state that they support multi-tenancy. Only B&R mapp Technology requires a special (optional) device for cloud connection, the "Orange Box". The top four rows in Figure 12 represent the cloud capabilities mentioned per platform.

| | Adamos | Amazon AWS IoT | Bosch IoT Suite | B&R mapp Technology | Cisco Kinetic | DeviceInsight Centersight | Emerson Plantweb | E&H Netilion | GE Predix | Google Cloud IoT Core | Harting MICA | IBM Watson IoT Suite | Microsoft Azure IoT Suite | Oracle Cloud IoT | PTC ThingWorx | Recogizer Analytics | SAP Leonardo | Siemens MindSphere | Software AG Cumulocity | S&T SUSiEtec | Weidmüller Ind. Analytics |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Cloud-based | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ○ | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| Cloud optional | ● | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ● |
| On premise | ● | ○ | ○ | ○ | ○ | ● | ◖ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ● | ○ |
| Multitenant | ● | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ |
| Scalable | ● | ● | ● | ● | ● | ● | ● | ○ | ● | ● | ○ | ● | ● | ● | ● | ○ | ● | ● | ● | ● | ● |
| Via On-Offboarding | ○ | ● | ● | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ● | ● | ○ | ○ | ○ |
| Via Cloud | ○ | ● | ○ | ○ | ○ | ● | ○ | ○ | ● | ● | ○ | ● | ● | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| At runtime | ● | ○ | ○ | ○ | ○ | ● | ○ | ○ | ● | ● | ○ | ● | ● | ● | ○ | ○ | ● | ○ | ○ | ○ | ○ |

*Figure 12: Cloud usage and scalability per platform*

Many platforms name the supported cloud providers, but some do not name all of them, e.g. Adamos refers to its Cloud Connector Framework, which provides integrations for 30 cloud providers. Often platform vendors that are cloud providers themselves name their own cloud here. Figure 13 shows the frequency for the identified cloud providers with Microsoft Azure mentioned most frequently.

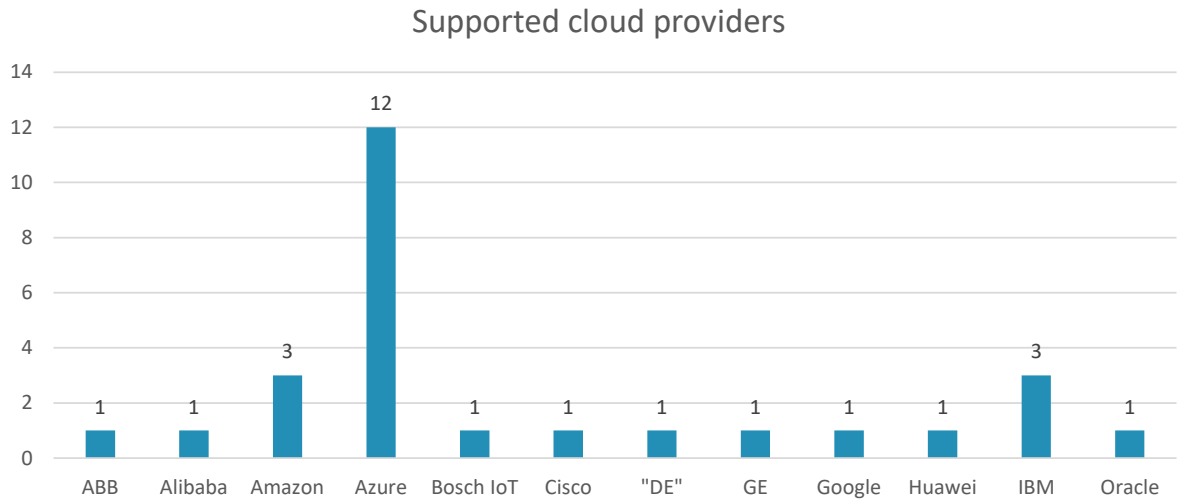



*Figure 13: Explicitly named cloud provider support ("DE" denotes unspecified cloud infrastructure in Germany).*

81% of the platforms make statements about scalability. 29% of the vendors relate this statement to the addition or removal of IIoT devices, four of which exclusively mention the IIoT devices as a reason for scalability. 38% of vendors also cite runtime scalability, such as load balancing. 33% argue scalability through cloud capabilities. The bottom four rows in Figure 13 represent the scalability capabilities mentioned per platform.

## 4.9 Digital Twins / Asset Administration Shell

The use of digital twins for the digital representation of an entity, such as a machine, an IoT device or even a process, allows for simulating the represented entity [15] The possibility of simulation can in turn be used to design and test new or further developments of an entity on the basis of its digital twin before this development is integrated into the active productive process. Thus, the use of digital twins in development and simulation can avoid potentially costly failures that can occur when developing directly on a production system. Furthermore, the use of digital twins allows the application of so-called digital shadows. Digital shadowing is a parallel representation of an entity in a production system by its digital twin, which allows to represent the current state of this entity in parallel to the production system. This representation allows the rapid recovery of states of entities in the production system, should they suffer disruptions or failures, based on the last correct state of the digital twin of the affected entity.

- 7 of the platforms considered do not provide any information on the use of digital twins or related approaches. 4 platforms directly mention digital twins as a supported functionality of the platform, while our discussion below will reveal that the concept of digital twins, albeit in modified forms, is supported by 12 of the platforms (57%), which underlines the importance of such a capability, at least for simulating devices.
- 12 platforms mention the use of digital twins or a form of digital representation of entities, mostly devices, to simulate these entities. The Google Cloud IoT Core and IBM Watson IoT Suite platforms each mention only the possibility of a "device simulator" here, but this is to be understood as a variant of a digital twin.
- The development of new devices as well as the evolution of devices, device configurations up to business processes based on their digital twin is supported by 8 platforms (38%).
- Digital shadows of entities, again mostly devices, are explicitly supported by 6 platforms (27%). Bosch IoT Suite does not explicitly name digital shadows, but implicitly indicates the possibility of supporting digital shadows.

Various platforms point to particular use cases and capabilities of using digital twins that they support. For example, B&R mapp Technology offers 3D simulation of devices, as well as mockup interfaces (including user interfaces) based on their digital twins. GE Predix and Microsoft Azure IoT provide the ability to create federations of digital twins, which enables the simulation of device federations up to production lines. This capability is further supported in the Microsoft Azure IoT platform by providing a "Spatial Intelligence Graph" and a proprietary modeling language (DTDL) for digital twins. Oracle Cloud IoT explicitly offers support for predictive digital twins, i.e. predictive simulation on digital twins for the realization of e.g. predictive maintenance. SAP Leonardo and Siemens MindSphere each offer their own middleware for modeling and deploying digital twins.

| | Adamos | Amazon AWS IoT | Bosch IoT Suite | B&R mapp Technology | Cisco Kinetic | DeviceInsight Centersight | Emerson Plantweb | E&H Netilion | GE Predix | Google Cloud IoT Core | Harting MICA | IBM Watson IoT Suite | Microsoft Azure IoT Suite | Oracle Cloud IoT | PTC ThingWorx | Recogizer Analytics | SAP Leonardo | Siemens MindSphere | Software AG Cumulocity | S&T SUSIEtec | Weidmüller Ind. Analytics |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Digital Twin | ● | ○ | ● | ● | ○ | ○ | ○ | ● | ● | ● | ○ | ● | ● | ● | ● | ● | ● | ● | ○ | ○ | ○ |
| AAS | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ |
| Similar to AAS | ○ | ● | ● | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ● | ● | ● | ○ | ● | ● | ○ | ○ | ○ |
| Similar to edge AAS | ○ | ● | ● | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ● | ● | ● | ○ | ● | ● | ○ | ○ | ○ |
| DT simulation | ● | ○ | ● | ● | ○ | ○ | ○ | ○ | ● | ● | ○ | ● | ● | ● | ● | ● | ● | ● | ○ | ○ | ○ |
| DT development | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ● | ● | ● | ● | ○ | ● | ● | ○ | ○ | ○ |
| DT shadowing | ○ | ● | ● | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ● | ● | ● | ○ | ○ | ● | ○ | ○ | ○ |
| DT specific applic. | ○ | ○ | ○ | ● | ○ | ○ | ○ | ● | ● | ○ | ○ | ○ | ● | ● | ○ | ○ | ● | ● | ○ | ○ | ○ |

*Figure 14: Digital Twin (DT) support and use of the Asset Administration Shell (AAS) in the platforms.*

A fundamental prerequisite for the realization of digital twins or similar approaches to the digital representation of entities is a platform-wide, uniform representation of the information available about the entities within the platform. Ideally, such a representation of the information about an entity (or, more broadly, a "thing") is also unified across platforms and thus standardized [23]. Such an approach of a cross-platform, standardized, representation of information about entities is currently being pursued in the context of the Industry 4.0 initiative in the form of the creation of the Asset Administration Shell (AAS) [1, 24].

This platform analysis therefore also evaluated the extent to which the platforms considered either already use the AAS representation form or use forms of entity information representation similar to the AAS. The direct use of the AAS standard was not explicitly mentioned by any of the platforms considered; only Siemens MindSphere implicitly showed that integration of the AAS is possible by using the AAS in a demonstrator.

The use of information representations, which are similar in concept to the AAS, in some cases even almost corresponding, is explicitly mentioned by 7 platforms. A term frequently encountered here is "Things Modeling". This approach pursues the platform-wide uniform modeling of the information representation of a "Thing", i.e. an entity. This corresponds to the concept of the AAS, but is implemented in different variants by the individual platforms. Amazon AWS IoT, Bosch IoT Suite, PTC ThingWorx and SAP Leonardo, for example, explicitly use the phrase "Things Modeling" and a correspondingly similar approach in the platform-wide uniform representation of information about entities. Here, Microsoft Azure IoT cites the Digital Twin Definition Language (DTDL) it uses as the fundamental concept of information representation. Oracle Cloud IoT, GE Predix as well as Siemens MindSphere make no explicit reference to the use of a "Things Modeling", but also show similarities in their approaches to modeling entities within the platforms to the AAS approach. For example, Siemens

MindSphere mentions the encapsulation of managed IoT devices using middleware, and the Oracle Cloud IoT and GE Predix platforms each also take an approach similar to the AAS in their approaches to using digital twins.

An application of the Asset Administration Shell or a similar approach to information representation on edge devices is supported by the 8 platforms just mentioned, i.e., the edge devices and their properties are represented in terms of the respective information models.

The degree of flexibility of this representation or the "Thing Model" and, thus, its flexibility (also in the sense of systematic configurability, T14), can currently only be derived to a limited extent from the available documents. It is therefore interesting that two platforms explicitly mention the adaptability of their data model for data analysis. If unified models were used here, this could also apply to "Things Modeling".

## 4.10 Data Management, Data Analysis and AI Capabilities

In this section, we summarize the results for the capabilities on 1) data management and data analytics and 2) (building on) artificial intelligence. Figure 15 presents the results per platform for these two aspects.

In terms of data management and data analysis (the top 8 rows in Figure 15), we identified the following capabilities:

57% of the platforms describe themselves as real-time capable in terms of data collection and data analysis. Of these, 5 platforms (23% in total) use terms that indicate soft real-time, such as "near real-time" or "almost real-time." The remaining 2 platforms speak only of "real-time." 33% of the platforms describe their data processing as stream-based, meaning that they apply an approach that can be used to realize data analysis (typically in soft) real-time or in a distributed manner.

38% of the platforms name techniques for configuring or adapting data analysis[18] (see also T14 in Section 4.12). Two platforms (Adamos, Software AG Cumolocity) describe that the underlying data model can be adapted or extended. A special form of customizing the data analytics capabilities is data flow customizability, especially for platforms that offer stream-based data analytics. This ability has been named by two platforms (Cisco Kinetic and Recogizer Analytics).

Further two platforms (Adamos, Google Cloud IoT Core) name customizable data retention rules as a technical capability (beyond the privacy policy of the respective platform). 19% of the platforms support the collection or analysis of time series. Specific capabilities include time-based (temporal) data analytics (Azure IoT) or meta-data management and analysis (Recogizer Analytics). For four platforms (19%), we could not identify any references to data management or data analysis capabilities.

[18] In Figure 15 named “Cust. analysis”, i.e., customizable analysis.

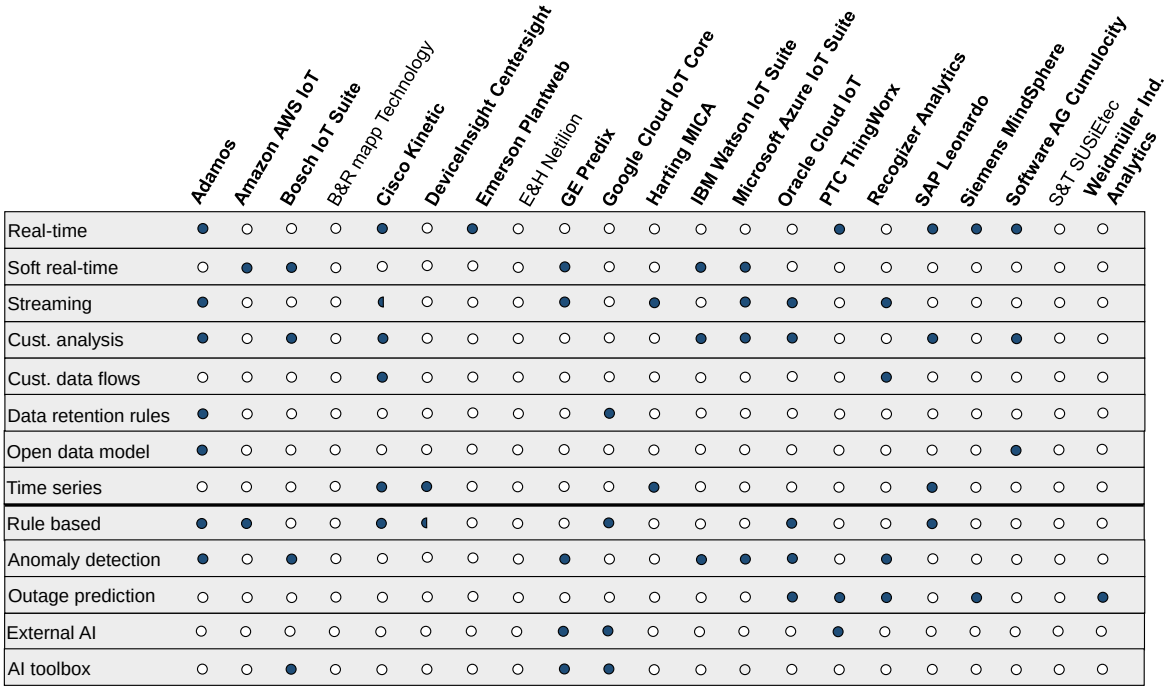



*Figure 15: Data management and analytics capabilities (top) and AI support (bottom) per platform.*

Regarding AI functionality or AI techniques (the bottom 7 rows in Figure 15), we found the following capabilities:

Seven of the platforms (33%) make no statement about AI capabilities or give indications that AI methods are envisaged fur future developments. 33% of the platforms use rule-based approaches. Not shown in Figure 15 are other AI methods, as these are rarely mentioned explicitly. Examples are stream-based ML (Adamos), recommendation-based methods (GE Predix), sentiment-based methods (Microsoft Azure IoT Suite), neural networks (Microsoft Azure IoT Suite) or reinforcement learning (Recogizer Analytics). Google Cloud IoT Core offers so many different frameworks or libraries that extracting the actual capabilities is difficult, but it is likely that the current standard techniques such as neural networks are suitably supported.

33% of the platforms integrate procedures for anomaly detection, 19% for behavior prediction and ThingWorx offers procedures for learning normal behavior. 14% of the platform support the use of external AI procedures, and another 14% (overlap for Predix and Google Cloud IoT Core) support the application of AI through specific (sometimes fixed) AI components or AI building blocks. Other features not shown in Figure 15 are: Configuration options for individual (built-in) AI procedures (Bosch IoT Suite and Google Cloud IoT Core), execution of AI procedures on edge devices or as containers (see also Section 4.4).

## 4.11 Openness / Extensibility

This section looks at the openness of the platforms studied, for example, in terms of the ability to integrate external applications or data, as well as the extensibility of the platforms, e.g., by adding new components, supporting developers in creating or marketing their own applications in an online marketplace.

A first focus of the survey with regard to openness and expandability of the platforms examined is the provision of a store, i.e., an online marketplace. 48% of the platforms offer such a store in various forms. The platforms Adamos, Amazon AWS IoT, Google Cloud IoT Core, Harting MICA, IBM Watson IoT Suite, Microsoft Azure IoT, PTC ThingWorx and Siemens MindSphere either offer a store directly in the platform or offer platform services and applications via the store of their respective parent

company, such as AWS Marketplace, Google Cloud Marketplace or the IBM Product Store. Bosch IoT Suite uses the AWS Marketplace to offer its services, while GE Predix integrates its store into the development environment for applications and services.

38% of the platforms offer their platform services via their store. Bosch IoT Suite only offers services, while Adamos offers no services (only applications). Likewise, 38% of the platforms offer applications or ready-made software solutions in their stores. Bosch IoT Suite does not offer any applications (only services) and the Adamos platform only offers applications. 6 platforms (29%) allow the marketing of services and applications from third-party providers via their stores.

As mentioned at the beginning of this section, support for the development of services and applications within a platform is an essential feature of the extensibility of a platform, which is why various forms of this support by the platforms examined are considered below. The possibility of integrating platform services from other platforms into a platform is considered separately in Section 4.13 on ecosystem building.

3 platforms did not provide any information on possible support for developers in the development of new services and applications for the platform. 17 platforms, i.e. 81% of those who provided information on this point, with the exception of Harting MICA, which at least did not explicitly state this information, provide SDKs and APIs of the respective platform for developers. This strong support from developers is pleasing, but also not surprising, since the platforms profit directly from further development and a portfolio of services and applications that grows as strongly as possible, and ultimately also from the ecosystem (see Section 4.12) and the associated growth in user numbers. 52% of the platforms continue to provide templates for services, processes, and applications for developers in addition to SDKs and APIs. 48% of the platforms support developers by providing tutorials. These tutorials are offered in various forms, from websites with walkthroughs of development processes to video tutorials and direct training by platform vendors. Also 48% of the platforms explicitly name the provision of comprehensive documentation on the platform technology, the standards used and other aspects of the platform for developers. 3 platforms, Bosch IoT Suite, GE Predix and Harting MICA, explicitly mention the support of platform-specific communities of developers. 5 platforms offer developers platform-specific code repositories, such as Git repositories. However, it should be noted here that the IBM Watson IoT Suite platform currently only offers the Git repository provided as archived. It is clear from the figures mentioned that supporting developers is a core concern of the clear majority of the platforms considered.

| | Adamos | Amazon AWS IoT | Bosch IoT Suite | B&R mapp Technology | Cisco Kinetic | DeviceInsight Centersight | Emerson Plantweb | E&H Netilion | GE Predix | Google Cloud IoT Core | Harting MICA | IBM Watson IoT Suite | Microsoft Azure IoT Suite | Oracle Cloud IoT | PTC ThingWorx | Recogizer Analytics | SAP Leonardo | Siemens MindSphere | Software AG Cumulocity | S&T SUSIEtec | Weidmüller Ind. Analytics |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Store | ● | ● | ● | ○ | ○ | ○ | ○ | ○ | ● | ● | ● | ● | ● | ○ | ● | ○ | ○ | ● | ○ | ○ | ○ |
| Service store | ○ | ● | ● | ○ | ○ | ○ | ○ | ○ | ● | ● | ○ | ● | ● | ○ | ● | ○ | ○ | ● | ○ | ○ | ○ |
| Solution store | ● | ● | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ● | ● | ● | ○ | ● | ○ | ○ | ● | ○ | ○ | ○ |
| 3rd party store | ● | ● | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ● | ○ | ● | ○ | ○ | ● | ○ | ○ | ○ |
| Dev.sup. SDK/API | ● | ● | ● | ● | ● | ● | ○ | ○ | ● | ● | ○ | ● | ● | ● | ● | ● | ● | ● | ● | ● | ○ |
| Dev.sup. templates | ○ | ● | ● | ○ | ○ | ○ | ○ | ○ | ● | ● | ● | ● | ● | ● | ● | ○ | ● | ● | ○ | ○ | ○ |
| Dev.sup. tutorials | ○ | ● | ● | ○ | ○ | ○ | ○ | ○ | ● | ● | ○ | ● | ● | ● | ● | ○ | ● | ● | ○ | ○ | ○ |
| Dev.sup. docu. | ○ | ● | ● | ○ | ○ | ○ | ○ | ○ | ● | ● | ○ | ● | ● | ● | ● | ○ | ● | ● | ○ | ○ | ○ |
| Dev. communities | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ● | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Dev. repositories | ○ | ● | ● | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ● | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Ext. algroithms | ● | ● | ○ | ● | ○ | ● | ○ | ○ | ● | ● | ● | ○ | ● | ○ | ● | ○ | ● | ● | ● | ● | ○ |
| Ext. data | ● | ● | ● | ○ | ● | ● | ○ | ○ | ● | ○ | ● | ● | ● | ● | ● | ○ | ● | ● | ● | ○ | ○ |
| Iface. To Pf-AI | ● | ● | ○ | ○ | ● | ○ | ○ | ○ | ● | ● | ○ | ● | ● | ● | ● | ○ | ● | ○ | ● | ○ | ○ |
| Customer AI | ○ | ● | ● | ○ | ○ | ○ | ● | ○ | ● | ○ | ○ | ○ | ● | ● | ● | ● | ○ | ● | ● | ○ | ○ |
| Open Source SW | ○ | ● | ● | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Progr. support | ○ | ● | ○ | ○ | ● | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ● | ● | ○ | ○ | ○ |

*Figure 16: Openness and extensibility of the platforms.*

Other important aspects regarding the openness and extensibility of a platform are the possibility of using external algorithms or external software solutions as well as the possibility of integrating external data into services and applications that are developed for the application or into existing services and applications on a platform. 13 of the platforms considered (62% of all platforms) allow the integration of external algorithms or software solutions, although B&R mapp Technology only states this implicitly by specifying the use of an "open architecture". 67% of all platforms allow external data to be integrated into the platform's services and applications.

The openness of a platform is also reflected in the provision of interfaces to the services and applications of the platform. Here, the provision of interfaces to AI services and AI applications of the platforms was considered in particular as part of the analysis (due to the special perspective of the IIP-Ecosphere project). 52% of the analyzed platforms offer interfaces to their respective AI services and applications. The openness in the context of the use of AI in the platforms is also reflected in the fact that 48% of the platforms allow its use either in the form of the platform's own AI procedures, which can be customized by the customer, or even (14%) the use of external, non-platform AI applications.

Another aspect of the openness of a platform is the use of Open Source software. 3 platforms, Amazon AWS IoT, Bosch IoT Suite and Google Cloud IoT Core state here that they use Open Source software, at least in parts, within the platform. The Amazon AWS IoT platform even uses an Open Source operating system, "Free RTOS", in parts of the platform.

A final option for supporting developers that we consider in this analysis is the provision of special programming support. 3 platforms, Amazon AWS IoT, Cisco Kinetic, and PTC ThingWorx, provide "no-code" or "low-code" support for developing services and applications for the platform. DeviceInsight Centersight offers strong source code reuse support and Siemens MindSphere offers strong application programming support.

## 4.12 Systematic Configurability

As already mentioned in Section 2.1, there are various possibilities around systematic configurability to realize, from "simple" configuration files up to (complex) configuration models. By this breath but also due to the non-uniform use of terminology, a "configuration" can be for example in the one extreme a configuration file and in the other extreme a validated model instance. Therefore, it is not easy to capture and compare capabilities in this topic. Nevertheless, because of the IIP-Ecosphere perspective, we are interested in indications to the techniques and approaches used. In our analysis, we made sure that the respective platform provides the user with suitable mechanisms that are beyond pure programming via APIs or deploying software on devices.

Comparing the platforms, it is noticeable that 19% do not make any (identifiable) statements about systematic configuration, i.e., 81% of the platforms realize one or more configuration techniques in our view. The following techniques or approaches were identified:

- 8 platforms (38%) allow customization of the respective functions, be it applications, data analyses, rules, execution schedules or KPIs through special editors. PTC ThingWorx (5%) allows modeling of the IoT environment (e.g. including employee objects or organizational units). Adamos (5%) allows users to define or restrict access to APIs. B&R mapp Technology and Oracle Cloud IoT (10%) provide configuration options for the properties of platform components and services, respectively.
- 9 platforms (42%) provide preconfigured packages or solutions that allow the user to more easily implement an IoT task that has already been solved. Of these, 7 platforms allow packages or solutions to be further configured and, thus, adapted.
- Easy customization of existing solutions can be achieved by configuring the presentation of the data, e.g., to enable reusable dashboard widgets. This was identified in the documents of 4 platforms (19%), namely Adamos, Cisco Kinetic, PTC ThingWorx and Recogizer Analytics IoT Platform. For Cisco Kinetic and PTC ThingWorx, this customization appears to be applicable to pre-configured packages and solutions, respectively.
- We found indications for a "platform configuration" for 6 platforms (29%). However, the respective statements do not allow us to draw any conclusions about what exactly is configured. This could be basic settings, such as network protocols or addresses. For such basic settings, we would assume that each platform offers corresponding options, e.g. in the form of configuration files, but this is not explicitly mentioned in the available materials (rather than in user manuals). However, it could also be the re-branding of the platform's appearance (Software AG Cumolocity) or more complex cases such as the presence of platform components or services (mentioned in Recogizer Analytics IoT Platform).
- One platform (B&R mapp Technology) provides tools for testing the configuration.
- Recogizer Analytics allows to version the (platform) configuration.
- Further potential mechanisms that indicate systematic configuration capabilities have already been mentioned in other analysis topics, such as "no code" or "low code" programming, configuration of data flows, adaptation of data models, or modeling of digital twins.

Based on the capabilities identified, we conclude that a relatively wide range of mechanisms and techniques are used to customize platforms. Figure 17 summarizes the capabilities per platform. How systematically these mechanisms are applied and how consistent the resulting (overall) configuration of a platform is cannot be deduced from the available information. It is positive in terms of configuration analysis and consistency that at least one platform mentions tools for testing configurations.

| | Adamos | Amazon AWS IoT | Bosch IoT Suite | B&R mapp Technology | Cisco Kinetic | DeviceInsight Centersight | Emerson Plantweb | E&H Netilion | GE Predix | Google Cloud IoT Core | Harting MICA | IBM Watson IoT Suite | Microsoft Azure IoT Suite | Oracle Cloud IoT | PTC ThingWorx | Recogizer Analytics | SAP Leonardo | Siemens MindSphere | Software AG Cumulocity | S&T SUSIEtec | Weidmüller Ind. Analytics |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Apps, pkgs., solutions | ○ | ● | ● | ○ | ● | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ● | ● | ○ | ● | ○ | ○ | ○ | ○ |
| Dashboard, UI | ● | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ● | ○ | ○ | ○ | ○ | ○ |
| Services, components | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ |
| Service combination | ○ | ◖ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ |
| Function, aggregation | ● | ● | ○ | ● | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ● | ● | ○ | ○ | ○ | ◖ | ○ |
| Function (security) | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| IoT model | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ |
| Platform | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ● | ○ | ○ | ◖ | ○ | ● | ● | ○ | ○ |
| Re-branding | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ |
| Preconf. apps, solutions | ○ | ● | ● | ○ | ● | ○ | ○ | ○ | ● | ○ | ● | ○ | ○ | ● | ● | ● | ● | ○ | ○ | ○ | ○ |
| Test of configuration | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Versioning | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ |

*Figure 17: Overview of configuration capabilities per platform.*

Furthermore, it can only be concluded indirectly at which points in the software lifecycle configurations are permissible or how these affect an installed and executable platform. It could be expected that function and dashboard changes are possible both before actual operation of the platform (i.e., at setup time) as well as during operation (potentially at fixed points in time). The extent to which runtime changes are actually supported and whether this may even lead to (manual) runtime adaptations of the platform (or to inconsistencies or runtime problems) cannot be inferred from the available material.

## 4.13 Ecosystem Building

A platform ecosystem, whether in platform-centric or cross-platform manner, is based on the extension mechanisms offered by a platform as considered in Section 4.10 as well as on the possibilities for integrating services from other platforms and third-party providers. The creation of ecosystems based on a single platform, but especially also cross-platform, provides a platform with a number of advantages because, as already mentioned in Section 4.10, the building of an ecosystem promotes the new and further development of services and applications in and around a platform, which in turn increases the number of users as well as the degree of dissemination of the platform.

The term "multi-sided platform" stands for a platform that offers the capability of networking the platform or its applications and services with other platforms and their applications and services. 67% of the platforms can, to varying degrees, be characterized as a "multi-sided platform". The degree to which a platform is able to network with other platforms is highly dependent on the focus of its ecosystem approach. Here we found that there is a clear distinction between platforms that build an ecosystem for their own platform, with limited ability to network with other platforms, and platforms that clearly aim to build an ecosystem through strong networking with other platforms. The 4 platforms Amazon AWS IoT, Harting MICA, IBM Watson IoT Suite and Oracle Cloud IoT focus on their own ecosystem. 12 platforms offer the possibility of ecosystem formation with a focus on networking with other platforms.

| | Adamos | Amazon AWS IoT | Bosch IoT Suite | B&R mapp Technology | Cisco Kinetic | DeviceInsight Centersight | Emerson Plantweb | E&H Netilion | GE Predix | Google Cloud IoT Core | Harting MICA | IBM Watson IoT Suite | Microsoft Azure IoT Suite | Oracle Cloud IoT | PTC ThingWorx | Recogizer Analytics | SAP Leonardo | Siemens MindSphere | Software AG Cumulocity | S&T SUSiEtec |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Multi-sided | ● | ● | ● | ○ | ● | ● | ● | ○ | ● | ○ | ● | ○ | ● | ○ | ● | ● | ● | ● | ● | ○ | ○ |
| Focus on plattform | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ● | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Int. 3rd PF services | ○ | ○ | ● | ○ | ● | ○ | ● | ○ | ○ | ○ | ● | ○ | ○ | ○ | ● | ○ | ● | ● | ● | ○ | ○ |
| Customizing | ○ | ● | ● | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ● | ● | ○ | ○ | ● | ● | ● | ● | ○ | ○ |
| 3rd party solutions | ● | ● | ○ | ● | ○ | ○ | ○ | ● | ● | ● | ● | ● | ● | ● | ● | ● | ○ | ● | ● | ○ | ○ |
| 3rd party services | ● | ● | ● | ○ | ● | ○ | ● | ○ | ● | ○ | ● | ● | ● | ● | ● | ● | ● | ● | ● | ○ | ○ |
| 3rd party data | ● | ○ | ○ | ○ | ● | ○ | ○ | ○ | ● | ○ | ○ | ○ | ● | ● | ● | ● | ○ | ● | ● | ○ | ○ |
| Ref. to RAMI 4.0 | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ |
| Only interfaces | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Partner network | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ● | ● | ● | ● | ● | ○ | ○ | ● | ○ | ○ | ○ |

*Figure 18: Ecosystem building capabilities per platform (PF).*

Beyond the possibilities for open extension of platform services and applications within a single platform considered in Section 4.11, the degree to which services from other platforms can be networked and integrated into a platform itself varies. 38% of platforms integrate services of other platforms. The most common form of integration here is the integration of cloud services of other platforms. For example, the Bosch IoT Suite, Cisco Kinetic, Emerson PlantWeb, PTC ThingWorx and SAP Leonardo platforms integrate various cloud services from providers such as Amazon AWS, Microsoft Azure, IBM Watson and Alibaba (see also Section 4.8). The Harting MICA, Siemens MindSphere and Software AG Cumulocity platforms only mention the integration of general cloud services in this point, without further details on specific providers.

43% of the platforms allow the customization of platform applications and also the integration of customer applications into the platform. A detailed look at the possibility of developing and integrating third-party applications, services and data into the platforms revealed the following picture:

67% of the platforms allow the development and integration of applications and services by third-party providers. One limitation that became apparent in this regard is the limitation of third-party providers in a platform to (industry) partners of the platform. 4 platforms, Harting MICA, IBM Watson IoT Suite, Microsoft Azure IoT Suite, and Oracle Cloud IoT limit the ability to integrate third-party applications to applications built by platform partners. In part, this restriction is tied to validation and certification mechanisms of partner applications by the platform, similar to mechanisms in App stores such as Google Play.

The integration of third-party services into the platform is allowed by 71% of the platforms. Again, the same restrictions on services from platform partners apply as shown in the previous section.

A significantly smaller number of platforms allow the integration of third-party data into the platform. Only 9 platforms (43%) allow the use of third-party data. Again, for the Microsoft Azure IoT Suite and Oracle Cloud IoT platforms, third-party data can only be integrated into the platform if these third-party providers are platform partners.

In addition to the close partner relationships of the 4 platforms mentioned above, which only allow third-party applications and services from their respective platform partners, a total of 8 platforms (38%) offer partner networks for companies. Advantages of such a partnership are a close cooperation between the partner company and the platform (vendor) in the integration of partner offerings as well

as the partner-specific adaptation of platform services to the needs of the platform partners. The long-term commitment of platform partners to the respective platform can also be seen here as an approach to forming an ecosystem not only between the platform and its partners, but also between the platforms partners themselves.

Deviceinsight Centersight and Google Cloud IoT Core limit their claims about the ability to integrate with other platforms to stating that they provide interfaces to broad areas of each platform.

A reference to the RAMI 4.0 architecture, a relevant basis for Industry 4.0 concepts and for IIP-Ecosphere, is only mentioned by the PTC ThingWorx platform. It can be assumed that this is due to the relative novelty of this architecture, since architecture references from other platforms, similar to references to the AAS, certainly list architectures related to RAMI 4.0, such as support for KPI in the Oracle Cloud IoT platform.

## 4.14 Other Technical Abilities

For the other technical capabilities (T16), platform characteristics that were not explicitly addressed in the other topics were recorded during the data collection. We aim at identifying particular platform characteristics that either further distinguish the analyzed platforms or that might be of interest for our work in IIP-Ecosphere. Due to this (partially subjective) approach which serves more for complementing the overview, it cannot be assumed that this analysis topic in particular is fully covered. The following capabilities (see also Figure 19) were identified:

- 8 platforms (38%) use container-based virtualization techniques: Adamos, Amazon AWS IoT, Cisco Kinetic, GE Predix, Harting MICA, Microsoft Azure IoT Suite, Software AG Cumolocity and S&T SUSiEtec. Of these 8 platforms, 5 rely on Docker. Two of these 8 platforms use Kubernetes for container management.
- 38% of the platforms use microservices, either to realize platform functions or as an API for extensions. At first glance, one might assume that these are exactly the platforms that also use containers as a virtualization technique. That also seems to be true but for two exceptions: Deviceinsight Centersight uses microservices but does not mention a virtualization technique and S&T SUSiEtec uses containers without microservices.
- Most platforms allow customers to create their own programs, e.g., to define analytics. Two of the platforms (Adamos and Amazon AWS IoT) manage the application lifecycle in the process. Five platforms (24%) provide graphical programming approaches, B&R mapp Technology allows direct (visual) programming on the machine HMI, and Cisco Kinetic integrates an (explicit) “no code” development approach.
- Three platforms (Deviceinsight Centersight, Oracle Cloud IoT, Recogizer Analytics IoT Platform) offer specific support for defining or analyzing KPIs.
- Google Cloud IoT Core, Harting MICA and Recogizer Analytics support location-based services.
- To integrate edge or IoT devices, it may be necessary to install vendor-specific software or even a specific IoT operating system. Amazon AWS IoT and GE Predix mention their own or a specially compiled IoT operating system, while SUSiEtec requires Windows 10 IoT.
- Two platforms (Amazon AWS IoT, SAP Leonardo) provide some form of speech processing.
- Centersight and PlantWeb integrate virtual reality functionalities with reference to maintenance support.
- Even though Adamos uses the keyword "adaptive" in its name, B&R mapp Technology is the only platform that talks about an adaptive capability, namely self-optimizing controllers.
- Google Cloud IoT Core and Amazon AWS IoT allow addressing IoT devices that are actually offline (transparent device shadow).
- Harting MICA offers special functionality for radio-frequency identification (RFID).

- Adamos protects its APIs through a special security mechanism.

| | Adamos | Amazon AWS IoT | Bosch IoT Suite | B&R mapp Technology | Cisco Kinetic | DeviceInsight Centersight | Emerson Plantweb | E&H Netilion | GE Predix | Google Cloud IoT Core | Harting MICA | IBM Watson IoT Suite | Microsoft Azure IoT Suite | Oracle Cloud IoT | PTC ThingWorx | Recogizer Analytics | SAP Leonardo | Siemens MindSphere | Software AG Cumulocity | S&T SUSIEtec | Weidmüller Ind. Analytics |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Container | ● | ● | ○ | ○ | ● | ○ | ○ | ○ | ● | ○ | ● | ○ | ● | ○ | ○ | ○ | ○ | ○ | ● | ● | ○ |
| Docker | ● | ● | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ● | ○ |
| Kubernetes | ● | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Microservices | ● | ● | ○ | ○ | ● | ● | ○ | ○ | ● | ○ | ● | ○ | ○ | ○ | ○ | ○ | ● | ○ | ● | ○ | ○ |
| API protection | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| SW lifecycle | ● | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Graphics prog. | ● | ● | ○ | ● | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ |
| KPI support | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ● | ○ | ○ | ○ | ○ | ○ |
| NLP support | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Self-optimization | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Augmented reality | ○ | ○ | ○ | ○ | ○ | ● | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Edge OS | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● |
| Edge offline supp. | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Location-based | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ● | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ |
| RFID | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Blockchain | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ● | ○ | ○ | ○ | ○ |

*Figure 19: Other technical abilities per platform.*

It is also interesting to note that IBM initially included blockchain functionality in Watson IoT Suite, but has since discontinued it. SAP Leonardo continues to offer blockchain functionality.

# 5 Threats to Validity

Survey-based analyses such as this whitepaper may be subject to influences that affect the validity of the data presented. At various points in this paper, we have already indicated and addressed these issues. In this section, we summarize and discuss the potential problems. In doing so, we use the usual categories, construct validity, internal validity, inferential validity, and external validity.

**Construct validity** refers to the selection of expressions and factors to capture the questions.

- This overview is based on an analysis of a representative set of platforms (as a construct). However, as explained at the beginning, not all possible IoT platforms [7] can be analyzed. The number is just too large [13] and the market too dynamic [7]. This is also not necessary, as this overview is not intended to reflect the market, but to investigate the relevant platforms in the context of the IIP-Ecosphere project. This has been done by including, on the one hand, the economically relevant platforms and, on the other hand, the platforms found to be practically relevant by partners.
- The wrong factors may have been analyzed for answering the question on current state of IoT platforms. The addressed analysis topics are based on discussions among the IIP-Ecosphere partners on the vision of the platform to be created in the project. The analysis topics cover the envisioned core contributions of the platform and are, thus, relevant to the project. It is likely that the analysis topics are less appropriate for other questions, although other questions are also not intended to be covered by this overview.
- The used platform documents may not contain any or sufficient information to answer the analysis topics sufficiently or comprehensively. This is possible as we have based this review on websites and promotional material from the platform vendors, i.e. publicly available material at the time of review. This decision was made deliberately. Alternatively, interviews or conversations could be used as in [7]. Both approaches allow vendors to influence the results, although we assume that websites and promotional material, while used to commercially promote their own products and therefore present them in a realistic (possibly rather positive) light, also have less potential to influence the validity of such a review. However, we also accept that the materials used were not prepared for the purpose of such a work and, thus, may be incomplete from our point of view.
- The platform documents used contain varying degrees of technical detail. Some platform documents are written more from a marketing perspective, while others describe technical instructions and programming interfaces. This can lead to a bias in how each platform is represented. Conversely, the use of promotional material can lead to a different bias, as vendors might tend to present their work better, but for business reasons naturally also try to present the respective platform as comprehensively as possible. This could only be circumvented by analyzing the actual platform implementations, which is often not possible for resource, licensing and availability reasons, and could in its own way bias a result, as complex platforms require a lot of detailed knowledge to find and analyze the relevant features. We are aware of these possible biases and refer especially in the analyses also to the statements in the materials, not to the actual realized capabilities of the individual platforms.
- Since the documents were not prepared specifically for this study, the structure of the individual documents is sometimes rather diverse. This means that it may not be easy to map the actual functionality of a platform to the analysis topics we are looking for, which can lead to a bias in the information presented. Therefore, we approached the collection of raw data in the most general way possible, i.e., even if information appeared to fit an analysis topic at first glance, we continuously checked the mapping during the conduction of the extraction and

corrected it if necessary. Therefore, we are convinced that this agile approach has enabled us to identify a suitable fit in most cases.

- Not all available material is considered when extracting the answers to the analysis topics. We compensate for this risk by using the deep search strategy explained in Section 2.3, i.e., we deliberately search all sub-documents accessible from the main documents. Nevertheless, it is conceivable that individual documents are not linked or not linked correctly and cannot be found by a deep search. We compensate for this by performing an additional search with Google, which identifies several alternative entry documents if necessary, and consider these documents in our analysis.
- In some places, vendors present development plans and future plans, e.g., a planned integration of artificial intelligence methods. It can be difficult to separate these plans from actual capabilities or those currently under development. Generally, future statements are identifiable through linguistic means and low information content and can typically be excluded when compiling the results.

The **internal validity** asks the question whether the result has arisen due to causal relationships with the expressions and factors.

- The information used for extraction and analysis could have been different for each author, as the vendors may have changed the documents or web pages while conducting the research. Given the time period of just under two and a half months for data extraction, we assume that no significant web page information was changed during this time and thus all authors were working with the same information. To ensure this, the web pages were stored locally and made available to the authors in a uniform manner.
- Different personal views on the data may lead to different decisions during the raw data collection or data categorization and, thus, may influence the analysis results. We assume that we avoided this by sufficient communication among the authors. However, cross-validation between authors, as this is common in systematic literature analyses, was not performed here for reasons of resource availability. In any case, the results are very useful for IIP-Ecosphere in particular, even without such validation.
- Multilingual web pages may contain different content for different languages. We have relied here on the default browser language ("German", or English as a substitute), saved the corresponding web pages, made them available to all authors, and refrained from checking multilingual web pages for consistency. Original texts and literal quotations have been taken (where available) from the language variant of the materials corresponding to the language of the respective version of this document.

**Conclusion validity** questions whether conclusions are valid and not just based on random results. The conclusions drawn in this study are essentially based on the data analyses discussed in Chapter 4, which are based on the extracted raw information, for which we have discussed the validity above. The derivation of conclusions in Chapter 4 is essentially based on categorizations of the raw data. In the categorization process, it is possible that the wrong categories are chosen or that platform capabilities have been assigned to the wrong categories due to different terminology in the vendor materials. To avoid this, we performed the classification openly, i.e., by building the classification incrementally during the analysis, by adding new capabilities successively, and by re-analyzing previously processed platforms for the new categories. We checked unclear terms accordingly, or added new categories in case of doubt to avoid unintended misinterpretations.

**External validity** is concerned with the generalizability and transferability of the derived results. To enable further generalization, it would be necessary to analyze as many platforms as possible. As already discussed for internal validity, an analysis of all IIoT platforms is unrealistic for various reasons.

Nevertheless, to strengthen external validity (in the project context), we analyzed both, the platforms with the highest revenue and additional ones relevant to IIP-Ecosphere. From IIP-Ecosphere's point of view, this study therefore depicts a relevant and comprehensive picture of current platforms and, thus, helps to argue and substantiate the next realization steps in terms of industrial relevance.

# 6 Summary

Concepts and work around Internet-of-Things (IoT), Industrial Internet-of-Things (IIoT) or Industry 4.0 are fueling the next industrial revolution, which should ultimately lead to a comprehensive digitization of industrial production to better equip industry for the future. Cloud capacities, edge computing, digital twins and comprehensive, automated (real-time) data analyses are technical means that are seen as prerequisites for this revolution. Initially, this leads to extremely complex platforms that must be suitably set up, maintained, and, for reasons of flexibility, also reconfigured securely and consistently at run-time. Far more revolutionary, however, is the use of artificial intelligence methods that learn independently, recognize previously hidden patterns and can also deal with unforeseen situations. The aforementioned technical means form the systematic basis for using AI, but also require approaches to security and data protection in order to secure and protect the resulting technical systems from a wide variety of perspectives (including legal issues) and, finally, also approaches to explain the decisions that machines then make autonomously in such environments. The technical platforms that enable the next industrial revolution must provide suitable, integrated capabilities in all these areas. But not only in these areas, but also beyond them, because cooperation, collaboration and even the exchange of (production) data or compute resources are capabilities that companies are already thinking about now and what they will potentially desire in the future.

IIP-Ecosphere aims to achieve an innovative leap in the field of industrial production based on networked, intelligent, autonomous systems. The goal is to build a novel ecosystem - the "Next Level Ecosphere for Intelligent Industrial Production" - that enables a "next level" of intelligent industrial production. A core activity is to build an integrative, virtual platform that enables future concepts in the field of intelligent production to be explored and demonstrated. For this, it is essential to know the current state of projects, standards and industrial platforms and to consider them appropriately into the work in IIP-Ecosphere.

This white paper presented an analysis of 21 industrial IIoT platforms in terms of 16 topics relevant to IIP-Ecosphere. The platforms were selected collaboratively, both in terms of market penetration and relevance for the project partners. Thus, 63% European vendors are predominantly represented, while the remaining platforms are offered by US companies.

Below, we summarize the various detailed results as highlights:

- The analyzed platforms are predominantly commercial and usually cover a wide range of protocols such as MQTT, MODBUS, OPC-UA or AMQP. Most platforms describe their capabilities for the integration of IIoT devices, whereby the individual capabilities certainly differ in the areas of (automatic) onboarding and offboarding, monitoring, lifecycle management or software deployment. 38% of platforms are now (partially) implemented using container technology, often Docker. In addition to almost ubiquitous REST interfaces, 38% of platforms now also rely on microservices or microservice-based architectures.
- 57% of the platforms describe themselves as real-time capable, especially with regard to data collection and data analysis. One third of the platforms rely on stream-based techniques and enable customizations of the data analyses, two platforms even modifications to the underlying data model. 19% of the platforms describe capabilities for processing time series data.
- To enable scalability of the processes used, the collected data is often stored directly in a cloud. 95% of the platforms offer integration with cloud technology, but only 19% describe cloud technology as optional. 24% of the platforms enable an on-premise installation, i.e. an on-site installation, with only one platform giving indications that an exclusive on-premise installation without cloud connection is possible.

- Central collection and analysis of production data is often not sufficient. Pre-processing close to production up to complex analyses, pattern recognition or AI decisions in real-time are becoming increasingly important. Consistently, more than 85% of platforms rely on edge devices, i.e., industrial- and production-grade miniaturized IT solutions. However, the range of edge capabilities of platforms is broad: 67% of platforms support direct data storage on edge devices, 57% also allow the platform to control edge devices, 48% enable data processing on edge devices, 38% mention AI methods to be deployed on edge devices, and 29% even allow custom functions to run on edge devices. Moreover, edge capabilities are also often directly coupled with cloud technology, e.g., for storage or further processing.
- The concept of the digital twin is often cited for (virtual) development of new as well as for evolution of existing production facilities. 57% of the platforms are familiar with this concept, although its implementation is interpreted quite differently. 33% of the platforms also support so-called digital shadows, i.e., parallel execution of the digital twin. 38% of the platforms apply technologies to describe the associated information models. The concepts used in this context are similar to the Industry 4.0 Asset Administration Shell [1, 24]. However, we currently see neither trends towards the application of common reference architectures such as RAMI 4.0, the integral use of Asset Administration Shells, nor (analogous to [23]) the standardization of digital twins.
- AI processes are now understood to be a central component of future Industry 4.0 platforms. So far, 33% of the platforms mention AI capabilities, with the actual methods offered often not detailed or hidden behind numerous frameworks. 48% of the platforms allow customizations or customer-specific AI realizations here, while (not completely overlapping) 14% of platforms show efforts to offer AI procedures in such a way that customers can easily select, parameterize and combine them. However, uniform cross-platform interfaces have not yet been identified in the area of AI processes.
- Even without AI, mechanisms for security and data protection are essential within Industry 4.0 platforms. Almost two-thirds of the platforms name functions to protect the integrity of software and information, 86% describe suitable mechanisms to prevent unauthorized access to network services, and only two platforms state no mechanisms to protect the confidentiality, authenticity, or integrity of information through cryptographic mechanisms. Only 28% of platforms provide appropriate mechanisms to detect the processing of personal data, while 48% implement selected mechanisms for this purpose. 71% of platforms provide approaches to limit the retention period of data. Only two platforms appear to implement data protection through technology design and data protection-friendly default settings.
- Industry 4.0 platforms are often rather complex, in terms of their installation, their maintenance or adaptation. Systematic approaches for configuration can help here. With respect to customization techniques, 81% of the platforms appear to be customizable. However, we cannot conclude whether this also takes into account the consistency of complex, interacting customizations. At least one platform mentions tools for testing its configurations.
- Many of the platforms surveyed present themselves to be open for extensions or even for collaboration with other platforms in one way or another. 48% of the platforms offer a store for extensions, although in some cases only partner companies are allowed to post solutions. 81% offer various forms of development support. For 62% of the platforms it is stated that external components can be used and in 67% external data is possible. However, it is not always the case that platforms that build up an ecosystem also attempt to collaborate across ecosystems or platforms.

In summary, we can conclude that the basic functions are adequately covered by most of the platforms analyzed. This is particularly true for the support of a wide variety of communication protocols in the

Industry 4.0 environment or for cloud integrations. Even newer trends such as artificial intelligence have already been reflected in the platform implementations. However, it should be emphasized that newer standard-based protocol families such as OPC-UA or UMATI have not yet really become established. In addition, the openness or extensibility of the platforms often seems to be limited, especially with regard to new components, AI processes, or collaboration between platforms, which can certainly be explained by the increased quality and safety requirements in the production environment. Nevertheless, we see several broader challenges that motivate further work, in particular in the IIP-Ecosphere project.

- Creation of an open, open-source-based ecosystem that integrates existing platform installations and provides cross-platform add-on services for them (as needed). In the process, open integration of a large number of players who support this ecosystem.
- Development of an open and extensible (micro-)service and container-based platform architecture using RAMI 4.0 as well as standardized interface descriptions (e.g. Industry 4.0 Asset Administration Shell). In this context, critical user decisions (such as a mandatory cloud integration) shall not be anticipated by the platform vendor, but should be seen as possible variants to be decided by the user.
- Support of parameterizable, extensible and flexibly combinable AI methods that can be distributed and deployed dynamically (also automatically at runtime) in a factory plant. The special requirements of AI methods, such as resource-intensive training, but also of data analysts who want to access data flexibly in order to develop suitable AI solutions, must be taken into account. What is needed here are unified or standardized interfaces that enable cross-platform use of the AI methods.
- Standardization of the description and use of computing resources (edge, on-premise, cloud) so that different platforms can provide/use resources in a unified and cross-platform manner.
- Secure and consistent data exchange between platform components and platforms, also taking into account data sharing scenarios, resource sharing beyond the cloud, and data usage control.
- Systematic configurability, especially for complex platform aspects such as data provisioning and storage, data conversion, AI usage, component or container distribution. This requires suitable mechanisms for consistency checking and consistency assurance as well as mechanisms for implementing consistent configuration decisions at installation time or during run-time. Consistent decisions should lead to the complete removal of unneeded components such as cloud connectors, in particular to increase user confidence in the platform and to avoid latent security problems.

# 7 References

[1] Plattform Industrie 4.0, Die Verwaltungsschale im Detail, 2019, https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation/verwaltungsschale-im-detail-pr%C3%A4sentation.html

[2] Adari S., Falk S., Sampson C., Germany's evolving platform landscape, Accenture / Working Group on Digital Business Models in Industrie 4.0, 2019

[3] Bitkom, Welche Hemmnisse sehen Sie beim Einsatz von Industrie-4.0-Anwendungen in Ihrem Unternehmen?, 2019, https://de.statista.com/statistik/daten/studie/830813/umfrage/hemmnisse-beimeinsatz-von-industrie-40-anwendungen-in-deutschland/

[4] BMWi, Wachstumspfade bei der Digitalisierung von Geschäftsmodellen in Industrieunternehmen, 2019, https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation/Wachstumspfade-Digitalisierung-Gesch%C3%A4ftsmodelle.pdf

[5] M. Bremmer, IIoT-Plattformen – ein unreifer Nischenmarkt, Computerwoche, 2018, https://www.computerwoche.de/a/iiot-plattformen-ein-unreifer-nischenmarkt,3545047

[6] DIN e.V., Deutsche Normungsroadmap Industrie 4.0, Version 3, 2018

[7] T. Krause, O. Strauß, G. Scheffler, H. Kett, K. Lehmann, T. Renner, IT-Plattformen für das Internet der Dinge (IoT), Fraunhofer IAO, 2017, http://publica.fraunhofer.de/documents/N-470532.html

[8] Gabriel P., Potenziale der künstlichen Intelligenz im Produzierenden Gewerbe in Deutschland, Institut für Innovation und Technik, 2018, https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/potenzialekuenstlichen-intelligenz-im-produzierenden-gewerbe-in-deutschland.pdf

[9] Gartner, Reviews for Industrial IoT Platforms Market, https://www.gartner.com/reviews/market/industrial-iot-platforms

[10] E. Günthör, Sieben Industrie 4.0-Plattformen, die Sie kennen sollten, 2019, https://factorynet.at/a/sieben-industrie-40-plattformen-die-sie-kennen-sollten

[11] H. Hejazi, H. Rajab, T. Cinkler, L. Lengyel, Survey of Platforms for Massive IoT, IEEE Intl. Conference on Future IoT Technologies, 2018

[12] B. Henne, 5 Dinge die Plattformen für die Implementierung einer IIoT-Architektur können müssen, https://industrie.de/industrie-4-0/fuenf-dinge-die-plattformen-fuer-die-implementierung-einer-iiot-architektur-koennen-muessen/

[13] I-Scoop, IIoT platforms and ecosystems: Industrial IoT platform evaluation, https://www.i-scoop.eu/internet-of-things-guide/industrial-iot-platform-ecosystem/

[14] ITOperations, IT/OT convergence, https://searchitoperations.techtarget.com/definition/IT-OT-convergence

[15] W. Kritzinger, , M. Karner, G. Traar, J. Henjes, W. Sin, Digital Twin in manufacturing: A categorical literature review and classification" IFAC-PapersOnLine 51.11 (2018): 1016-1022.

[16] K. Lichtblau, Plattformen – Infrastruktur der Digitalisierung, Vereinigung der Bayerischen Wirtschaft e.V., 2019

[17] K. Lichtblau, T. Schleichermacher, H. Goecke, P. Schützdeller, Digitalisierung der KMU in Deutschland - Konzeption und empirische Befunde, https://www.iwconsult.de/fileadmin/user_upload/projekte/2018/Digital_Atlas/Digitalisierung_von_KMU.pdf

[18] P. P. Ray, A survey of IoT cloud platforms, Future Computing and Informatics Journal, 1, Seiten 35-46, 2016

[19] Reference Architecture Model Industrie 4.0, https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/rami40-an-introduction.html

[20] K. Schmid, H. Eichelberger, C. Kröher, Domain-Oriented Customization of Service Platforms: Combining Product Line Engineering and Service-Oriented Computing, Journal of Universal Computing, 19 (2), 2013

[21] F. van der Linden, K. Schmid, E. Rommes, Software Product Lines in Action, Springer, 2007

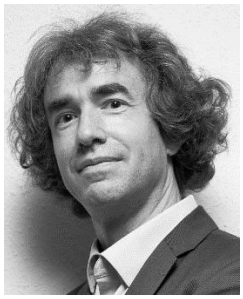
[22] B. Ullrich, F. Klarstetter, Anbieter von IIoT-Plattformen im Überblick, Cloudcomputing Insider, 2018, https://www.cloudcomputing-insider.de/anbieter-von-iiot-plattformen-im-ueberblick-a-767711/

[23] VDI Statusreport, Simulation und digitaler Zwilling im Anlagenlebenszyklus – Standpunkte und Thesen, Februar 2020

[24] ZVEI, Beispiele zur Verwaltungsschale der Industrie 4.0-Komponente – Basisteil, 2016, https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2016/November/Beispiele_zur_Verwaltungsschale_der_Industrie_4.0-Komponente_-_Basisteil/Beispiele-Verwaltungsschale-Industrie-40-Komponente-White-Paper-Final.pdf

## Über die Autoren

**Dr. Christian Severin Sauer** is a postdoctoral researcher in the Software Systems Engineering group at the Institute of Computer Science, University of Hildesheim. His research interests focus on domain knowledge elicitation and modeling for explanatory and context-sensitive AI applications. He studied at the University of Hildesheim and received his PhD in Computer Science from the University of West London. During his PhD, he investigated and developed methods for knowledge elicitation and knowledge modeling for explanatory and context-sensitive AI applications.



**Dr. Holger Eichelberger** is deputy head of the Software Systems Engineering group at the Institute of Computer Science at the University of Hildesheim. He conducts research in the areas of software product lines, model-based engineering, performance monitoring, and performance analysis. In particular, he is interested in the integration of these areas to create adaptive software systems. In IIP-Ecosphere he leads the think tank "Platforms" as well as the AI Accelerator. He studied computer science at the University of Würzburg, where he received his PhD on the automatic layout of UML diagrams.

*Photographer: Daniel Kunzfeld*

**Dr. Amir Shayan Ahmadian** is a postdoctoral researcher at the Faculty of Computer Science at the University of Koblenz-Landau. His research interests focus on the challenges of designing and implementing secure and privacy-friendly software systems as well as on the current developments in Industry 4.0. He studied computer science at the University of Paderborn and received his PhD in computer science from the University of Koblenz-Landau. During his doctorate, he developed a methodology to operationalize the principle of "data protection through technology design".

**Dr. Andreas Dewes** holds a PhD in experimental quantum computing from the Sorbonne University of Paris and the French Nuclear Energy Agency (CEA). He has founded several software companies and is the CEO of KIProtect GmbH, which develops advanced technical software solutions for data protection and data security. Within IIP-Ecosphere, KIProtect GmbH is developing a solution for the secure and privacy-compliant use of industrial & IoT data together with the consortium project partners and associated companies.

**Prof. Dr. Jan Jürjens** is Professor of Software Engineering at the Institute of Software Engineering at the University of Koblenz-Landau and Director of Research Projects at the Fraunhofer Institute for Software and Systems Technology ISST. He studied mathematics at the Universities of Bremen and Cambridge, received his PhD in computer science from the University of Oxford, was a postdoctoral researcher at the Technical University of Munich, as well as a Royal Society Industrial Fellow at Microsoft Research (Cambridge) and a non-scholarship Research Fellow at Robinson College (University of Cambridge), becoming a Senior Member there in 2009, and most recently a professor at the Technical University of Dortmund before joining Koblenz. He is the author of the book "Secure Systems Development with UML".