A REFERENCE ARCHITECTURE FOR CYBER-PHYSICAL FLUID POWER SYSTEMS: TOWARDS A SMART ECOSYSTEM

Dominik Martin\(^1\)*, Johannes Kunze von Bischhoffshausen\(^2\), Anna Hensel\(^1\), Johan Strandberg\(^2\)

\(^1\)Karlsruhe Institute of Technology, Kaiserstraße 89, 76133 Karlsruhe, Germany
\(^2\)Trelleborg Sealing Solutions Germany GmbH, Schockenriedstr. 1, 70597 Stuttgart, Germany

* Corresponding author: Tel.: +49 721 608-48967; E-mail address: dominik.martin@kit.edu

ABSTRACT

Technological advances (e.g., high speed communication, artificial intelligence) and affordable computing and sensor hardware have become a key driver of developments like “Industry 4.0” or the “Industrial Internet of Things” (IIoT). Large numbers of machines and products are equipped with sensors to constantly monitor their condition, log usage data or trigger control processes. IIoT has been largely adopted by OEMs in various industries (such as automotive, machinery industry, or healthcare and medical), turning their product into cyber-physical systems. However, the resulting potential is not yet accessible to component manufacturers. Overall, horizontal integration of the value chain is still in its infancy. Specifically, IIoT for fluid powers just started in recent years with first research projects and commercial solutions. This work presents a reference architecture for cyber-physical fluid power systems which depicts how horizontal integration can be achieved and which potentials thus can be released. The architecture is validated in an industrial use case. Furthermore, the paper at hand discusses which components of the architecture should be addressed by which actor in the fluid power ecosystem in order to leverage opportunities from the IIoT.

Keywords: Reference architecture, Fluid power systems, Cyber-physical systems, IIoT

1. INTRODUCTION

Due to rapidly advancing technological developments in a wide variety of areas (e.g., high speed communication, artificial intelligence) and at the same time the decreasing costs for hardware (i.e., sensor and computing), digitization and networking are shaping the current trends in the industrial landscape [1–3]. This development is discussed under different terms: Industrial Internet of Things (IIoT) and Industry 4.0 are the most common ones. All these terms are united by the idea that increasing networking holds the potential to create completely new products and services or establish data-based business models that allow companies to open up new business areas.

Many companies, especially OEMs (Original Equipment Manufacturer), focus on vertical integration, i.e., the flexible and seamless networking of production facilities, machines and products within their own company [4–6]. The aim is to equip physical assets, whether production machines or end products, with sensors and actuators. By integrating and, thus, leveraging networking and communication capabilities so-called cyber-physical systems (CPS) emerge [7,8].

However, horizontal integration, i.e., networking across company borders, is still at a very early stage of development [5,9]. It is precisely the fear of competition, data theft, the loss of the own supremacy and ultimately increased costs through innovation that prevents the research and development of new innovative products and solutions based on existing but so far insufficiently used data. Success stories of corporate giants such as Google, Apple and Amazon show the enormous potential of data-based business models. Yet, traditional industries still are reluctant to take this step towards horizontal integration and networking [10–12].

In view of this enormous business potential illustrated by concepts and initiatives in this context, there is a need for a uniform framework, standards and guidelines, which ideally represent...
a future-oriented holistic picture of the industrial communication of tomorrow. This is of enormous importance in order to reduce the increasing complexity caused by an increasing number of devices and networks as well as to avoid isolated solutions. In addition, uniform approaches contribute to cost reduction in the medium and long term, since the development of individual solutions is avoided [13]. For this reason, we aim to propose a reference architecture which takes these issues into account.

While there has been extensive research on high-level architectures for the IIoT as well as for cyber-physical systems, no generalizable architecture for cyber-physical fluid power systems has been proposed yet. Thus, this work presents a reference architecture for cyber-physical fluid power systems addressing networking as well as cross-company integration aspects. The architecture is validated in an industrial use case. Furthermore, this work discusses which components of the architecture should be addressed by which actor in the fluid power ecosystem in order to leverage opportunities from the IIoT.

2. RELATED WORK

Two terms are of great importance in the Industry 4.0 and IIoT context: cyber-physical systems and reference architectures. Cyber-physical systems (CPS) are “intelligent system[s] connecting the physical and the digital/cyber world through influence and control using sensors and actuators” [7]. Connectivity as one of the main functions of a CPS enables real-time data acquisition from the real world and direct feedback from the cyber world. Analysis and intelligent data management shape the cyber world. The advantages of a CPS are manifold. For example, the presence of digital twins of physical components in the cyber world allows components to predict by themselves when they will fail or break down by comparing their status to the status of other components [14,15]. Consequently, components and machines have the ability to schedule maintenance for themselves. In practice, however, such applications are still rare [16].

Therefore, reference architectures in the area of Industry 4.0 strive to most ideally represent a generalized overview and serve as guidelines and best practices for the actors involved. Reference architectures serve as a kind of guide for system development. It provides basic definitions and specifies commonalities for all systems based on it.

An example of a well-known reference architecture—although not in the context of IIoT but rather from the area of network protocols—is the Open Systems Interconnection model (OSI model) of the International Organization for Standardization (ISO) [17]. However, since it focuses only on the pure communication mechanisms, it is not sufficient for the description and classification of specific aspects in the context of IIoT.

Therefore, we conducted an in-depth structured literature search looking for reference architectures that also address horizontal integration aspects in terms of data exchange and access management among different companies participating in a common value chain.

Actually, there are a number of architectures in the field of fluid power systems [18,19], but none of them addresses integration or data-related aspects.

In regard to IIoT-related reference architectures, in literature there exist various generic architectures, however, two particular ones actually dominate: The Reference Architectural Model Industrie 4.0 (RAMI 4.0) [20] proposed by the Working Group for Industry 4.0 and the Industrial Internet Reference Architecture (IIRA) [13] of the Industrial Internet Consortium (IIC). Both of them strive to define standards for communication and interaction in the IIoT context.

RAMI 4.0 covers essential elements of Industry 4.0 concept as a three-dimensional layer model. In RAMI 4.0 a production object can be recorded over its entire life cycle. This reference architecture offers a uniform wording and a common understanding across all actors involved in the Industry 4.0 context. On the vertical axis, production objects and their data are displayed in six layers. There are two horizontal axes on each of the six layers. On one axis, the production objects are arranged according to hierarchical levels in production. On the other axis data about the production objects are recorded over the life cycle. In this way, objects can be arranged precisely in the model along these three axes.

Similarly, the goal of the very generic IIRA is “to achieve broad consensus in driving device and product interoperability and deploying large
industrial control systems” [21]. The IIC aims to depict a comprehensive architecture generally applicable. Therefore, it does not formulate concrete guidelines or implementation aspects.

Both architectures are very high-level and therefore offer only limited applicability in practice. Since existing reference architectures neither do explicitly consider the involvement of e.g., suppliers to a sufficient extent nor provide applicability to a typical fluid power system use case, we propose a novel reference architecture described in Section 4.

This architecture should not only represent a pure architectural structure but should also provide practical recommendations for action regarding information and data exchange between the actors involved. We see our architecture as an extension to common reference architectures, such as RAMI 4.0. However, our proposed architecture starts at a different, more detailed level and should provide practical recommendations for actions in terms of the organization of the parties involved, data flows and access management. Above all, in comparison to RAMI 4.0, it does not classify components according to certain criteria. Our architecture allows for the derivation of different types of implementation. It is therefore designed to be general and extensible, covering a specific area of Industry 4.0: the interaction between the OEM, its customers and its suppliers—especially applicable to the context of fluid power systems.

3. THE FLUID POWER ECOSYSTEM

3.1. Fluid Power Today

Despite the potential of digitization and increasing networking, so far there has been little horizontal integration and networking along all industries, but also in the fluid power domain.

Traditionally, a value chain is characterized by bidirectional exchange between the actors along the chain. While product specifications are passed through the supply chain by the OEM or end customer via Tier 1 supplier to Tier 2 supplier and so forth, the manufactured components flow back in the opposite direction, which are assembled by the OEM to become an end product. However, data that arises during the production of components as well as domain expertise, for instance, is usually not passed on to neighboring actors in the supply chain. Similarly, data that is created or gathered by a product at the end customer is usually collected either by the end customer himself or by the OEM and is not made accessible to the suppliers. This problem is particularly prevalent in the area of fluid power solutions, since very few of the companies operating in this area actually manufacture end products.

3.2. Digitization Impact

The increasing development within the industry towards intelligent and networked products creates a number of new opportunities for companies to expand their portfolio. The competitive boundaries are blurring and expanding towards the inclusion of more and more functions. These additional functions do not necessarily correspond to the original core competence of a company that previously specialized in a pure core product [22]. For example, a wind power turbine can be serviced or maintained in reasonable time before damage occurs by enriching condition monitoring capabilities. Through networking and system-wide consideration, additional services can be created that allow the operator or manufacturer to offer, for example, weather forecasts based on the data collected.

Figure 1: Pure Products turn into Systems of Systems based on [25]
Discrete isolated products are increasingly becoming complex systems of systems in which the company is only one player among many. The development shown in Figure 1 allows the manufacturer to offer bundles or packages of linked services or devices that increase the total value for the customer.

3.3. Fluid Power in Future

Thus, while some companies are trying to expand their portfolio and offer additional enriching products and services, others which do not follow this trend will certainly face threats. Even companies which have previously acted as OEMs can lose their role in favor of system integrators who specialize in linking several products and services to increase the overall product/package value [22].

Networked intelligent CPS thus provide the opportunity to rethink the existing value creation structure. It should be in the interest of all actors not to block each other through isolation, but to generate holistic added value for the customer through joint initiatives. The value chain of the future should therefore not be dominated by bidirectional exchange alone but should rather become a value creation network in which all stakeholders have the opportunity, through shared data access, to offer new services that benefit the overall product or system. Figure 2 depicts exemplarily the additional exchange of data and domain expertise—for instance encapsulated in algorithms or findings based on the application of data analytics or artificial intelligence techniques.

4. REFERENCE ARCHITECTURE

Most CPS consist of multiple components manufactured by several suppliers and combined into the final product/cyber-physical system (CPS) by the OEM. The CPS are equipped with sensors to constantly monitor their condition, log usage data or trigger control processes. To make use of this data to the full extent it must be made available not only to the OEM, but also to the component manufacturers. Possible use cases include value-added services such as predictive maintenance or product optimization based on data of components in use. While there has been extensive research on reference architectures for cyber-physical systems in general, no generalizable architecture taking into account the component manufactures, especially in the context of cyber-physical fluid power systems, has been proposed yet.

Such a reference architecture must consider all parties involved from a data perspective. These parties are: The CPS itself, the OEM producing the CPS and the tiers of component manufacturers supplying their components to the OEM. Bearing in mind the complexity resulting from the multitude of suppliers, simplicity of implementation is crucial for the applicability of the pursued reference architecture.
Figure 3: Reference Architecture for Cyber-physical Fluid Power Systems

To realize this, we propose the reference architecture depicted in Figure 3. The reference architecture aims to present a framework of actors around a cyber-physical fluid power ecosystem especially focusing on data exchange aspects.

It is based on the following key assumption: each party involved must make additional arrangements regarding data availability exclusively with those parties with whom the respective party is already in direct contact. This idea is already addressed by Schöggl et al. [23]. As we are looking at cyber-physical systems, we can assume that the data exists. For simplicity, we do not take into account legal issues, for example, concerning data privacy.

4.1. Structure of the Reference Architecture

The CPS consists of sensors and actors which collect data on different components. The sensor and actuators are controlled by either local MCUs (microcontroller units) or an asset MCU and made available to the IoT cloud. While the local MCU is mainly used for sensor/actor control and edge analytics, the asset MCU acts as firewall and handles security and communication aspects. The OEM is responsible for the existence of the IoT cloud and the data transfer from the assets to the cloud. Additionally, the OEM has full access rights to all data in the IoT cloud and manages the access rights for the Tier 1 suppliers, however, explicitly not for any of the Tier 2 and Tier 3 suppliers. Managing also the access rights for the Tier 2 suppliers would violate the assumption made above. The Tier 1 suppliers, in turn, manage the access rights for their corresponding Tier 2 suppliers and so on. In many use cases such as predictive maintenance, insights generated from e.g., a Tier 2 supplier might be of interest for the Tier 1 supplier, the OEM or even the customer owning the CPS [24]. Therefore, the insight generated by the Tier 2 supplier would be stored in the IoT cloud and made accessible to all corresponding players in the layers above.

Consequently, the reference architecture depicted in Figure 3 can be divided into three main parts: The data is stored in the IoT cloud; the horizontal axis describes the data transfer from the CPS into the IoT cloud and vice versa; and the vertical axis describes the availability management of the data.

4.2. IoT Cloud

The IoT cloud is the central storage point for all data. All data exchange between the CPS, the OEM, the Tier 1, the Tier 2 and the Tier 3 suppliers takes place indirectly via the IoT cloud. The OEM has full access to all data in the cloud. However, the Tier 1, 2 and 3 suppliers access a filtered/sliced version. Thus, they have limited access to the data in the cloud depending on their needs. The process of access rights management is described in Section 4.4. Having one central storage point for all data is beneficial in many aspects: Data validity is ensured because there exists only one version of the data and there are no copies of partial data. It is also advantageous because traceability and transparency is guaranteed and flexibility with regard to changing suppliers is ensured.
4.3. Horizontal Axis

The horizontal axis shows the interaction between the CPS, the OEM and the IoT cloud. The product a customer buys from the OEM is either named CPS or asset in this paper. Examples for assets in the field of mobile hydraulics are excavators or wind turbines. Each asset provides continuous data gathered through multiple sensors. However, some components do not directly provide sensor data themselves because they are not fitted with a sensor. Data on these components can be made available indirectly through sensor data of other components. For example, if a seal in a hydraulic pump is not fitted with a sensor directly, other sensors installed in the pump might provide relevant data concerning the seal. E.g., pressure data from the pump could provide information on the condition of the seal. Thus, all data needs to be transferred to the cloud by the OEM or its customer automatically. Thus, every asset generates a data stream into the cloud. The OEM determines which part of the data may be accessed by a certain Tier 1 supplier. The customer and the Tier 1 suppliers are not in direct contact in terms of data transfer and communication. Both are contractual partners of the OEM, but the reference architecture does not require any coordination between them. We call this property independence, which is expressed by the orthogonality of the horizontal axis (customers) and the vertical axis (tiers of suppliers) in Figure 3.

4.4. Vertical Axis

The vertical axis shows the interaction between the OEM, the IoT cloud and the suppliers. The OEM owns the admin rights and administrates the access rights for the Tier 1 suppliers. In other words, the OEM regulates which data a particular Tier 1 supplier can access. Each Tier 1 supplier administrates the access rights for the corresponding Tier 2 suppliers and so on (see Figure 4).

A Tier 1 supplier only grants a particular Tier 2 supplier access to data that is relevant or of interest for this particular Tier 2 supplier. Extending the example in Section 4.3, if a Tier 3 supplier is the seal manufacturer, a Tier 2 supplier passes the hydraulic pump data to the Tier 3 supplier. In order to obtain the greatest added value from the data, the suppliers have access to data that is generated directly by their component and to indirect data. The grant of access rights being done by the party in the next highest level ensures that complexity is kept on a low level. In addition, the possibility of violations of data protection is minimized, since each party involved only has access to the data that is relevant and of concern to it. Again, we abstract from legal issues.

Figure 4: Data Access Management

The parties have direct access to the data available to them. This means that a Tier 1 supplier does not forward the data to a Tier 2 supplier but grants him access to the specific data in the IoT cloud. The Tier 2 supplier thus accesses the data in the cloud directly. This is advantageous so that, for example, there are no duplicates of data and supports data validity. Figure 5 shows the vertical axis exemplarily for two layers and several suppliers.

Figure 5: Vertical Axis of the Reference Architecture

This vertical axis does not only represent the data access rights management but also the handling of insights generated by the suppliers. A particular supplier is an expert for its product and, therefore, can create additional value, that we call insights. Based on the available data, a certain party such as a Tier 2 supplier might generate these insights. Examples include results of predictive models, descriptive analytics or other...
data augmentations. In particular, insights that arise from the application of data analytics or artificial intelligence methods can have enormous added value for other actors in the value chain. Access to this knowledge is therefore exchanged for access to the necessary raw data. Insights generated by a certain party and relevant to other parties are stored in the IoT cloud and linked to data they are based on. A party automatically has access rights to insights if it has access rights to all data the insights are based on. This implies that a certain party always has access rights to the insights from the corresponding parties on the levels below. These insights could be used to generate further insights. Access rights to insights that do not fulfill the condition above can of course be assigned manually.

5. USE CASE

We evaluate the proposed reference architecture on an exemplary use case from the fluid power industry.

The value creation ecosystem around a certain CPS from the area of offshore infrastructure for oil and gas is exemplarily represented by three independently operating companies. While the OEM (acts in our use case also as Tier 1 supplier) manufactures the end product as well as the corresponding hydraulic system, the Tier 2 supplier is responsible for the hydraulic cylinders and the Tier 3 supplier for the included sealing systems.

The proposed reference architecture is applied exemplarily in a joint research project. The aim of the project is to research an AI-based algorithm for monitoring the condition of the sealing system assembled in the hydraulic cylinder. However, the domain expertise required to develop such an algorithm lies with the sealing system manufacturer (Tier 3), who is dependent on the usage data (pressures, velocities, etc.) and failure data of the entire system.

Finally, an AI-based condition monitoring system was successfully developed by the sealing system manufacturer based on the data provided by the OEM / Tier 1 indirectly via Tier 2. In return, these findings are transferred back to the OEM via Tier 2 by leveraging communication mechanisms provided by the IoT cloud, who can, for instance, offer a maintenance service based on this information. While the data exchange and preprocessing still required a significant amount of manual effort, the next step in this use case will be an automation of the entire data exchange.

6. CONCLUSION AND OUTLOOK

Today’s potential, which results from the emerging networking capabilities of several products in the field of fluid power systems depicts the necessity for companies to agree on horizontal integration in order to exploit this potential and, consequently, to remain competitive in the future.

Thus, the paper at hand proposes a uniform, easy-to-implement reference architecture that allows companies in a value creation ecosystem around a core product / cyber-physical system to develop additional innovative products and services. This is achieved by the exchange of data and insights created through the application of data analytics and artificial intelligence techniques. An important aspect of the proposed architecture is the inclusion of the entire value chain or the entire value creation ecosystem. Only through value co-creation holistic benefits can emerge, which provide appropriate incentives to share data and the insights, respectively. Besides aspects of horizontal integration, the architecture also addresses the importance of seamless communication between the cyber-physical systems and a central IoT cloud.

The conducted evaluation based on an exemplary application from the field of fluid power systems shows the added value that results from the application of the proposed architecture. Especially when suppliers can contribute to the overall value of a product, by generating additional insights based on their domain expertise, a simple and structured data exchange between the players must be ensured.

However, this work also has limitations. On the one hand, it is in the nature of reference architectures to draw only an abstract picture of an ideal world. On the other hand, the implementation or application of our proposed architecture is primarily the responsibility of the OEM, who first has to transfer data to the suppliers before they can feed back their findings. In addition, the OEM is also responsible for moderating and providing an IoT cloud, but it can be assumed that in most cases this already exists anyway. In general, we are convinced that isolation in terms of data disclosure will not be a valid option in the future to remain competitive.
The realization of our proposed reference architecture, however, reveals new business opportunities.

REFERENCES


