Available online at www.sciencedirect.com

ScienceDirect

IFAC Papers Online CONFERENCE PAPER ARCHIVE

IFAC PapersOnLine 56-2 (2023) 8197–8202

Electricity System Built on Cyber-physical Enterprises: Architecture Analysis ⋆

Petri Kannisto * **Antti Supponen** * **Sami Repo** *
David Hästbacka *

* *Tampere University, Tampere, Finland (e-mail: [petri.kannisto,antti.supponen,sami.repo,david.hastbacka]@tuni.fi).*

Abstract: Energy distribution systems can improve in adaptiveness by applying the concepts of cyber-physical systems (CPS), cyber-physical enterprise, and service-oriented architecture. With these paradigms, the information and communications technology (ICT) systems can respond to changes in the requirements and conditions of the environment, improving responsiveness to the fluctuation of electricity production from renewable energy sources (RES). This paper analyzes the suitability of a CPS architecture for the electricity distribution system. The novelty comes from a service-oriented model where customers and microgrids can sell services to one another and operators, building added value on existing energy resources. The architecture is analyzed with a coordinated voltage control (CVC) use case. The results suggest that the architecture can open new possibilities in utilizing energy resources and enables a customer-driven, distributed scheme instead of the strict operator-centric hierarchy of the contemporary systems.

Keywords: Cyber-physical Energy Systems (CPES), Cyber-physical Systems (CPS), Interoperability, Service-oriented Architecture (SOA), Smart Grid, Coordinated Voltage Control (CVC), Industry 4.0

1. INTRODUCTION

The conventional electricity network is strictly hierarchical, and to respond to the adaptiveness needs of the future, it should evolve to a scheme of cyber-physical enterprises. Adaptiveness is necessary due to the increase of renewable energy sources (RES) that lack control capabilities (Dreidy et al., 2017). For adaptiveness, the enterprises should utilize the energy resources provided by microgrids and customers capable of reacting to the needs of the market, power system, and electricity grid (Tikka et al., 2019). Such customers could even share resources among one another. The goal can be reached with the cyber-physical electricity system, built upon cyber-physical systems (CPS) and cyber-physical enterprises. Such enterprises sense changes in the environment and react accordingly (Panetto et al., 2019). In the energy scope, this approach both enables adaptiveness and lets the customers easily add and remove resources for control efforts.

This paper presents a service-oriented architecture for the cyber-physical enterprise network of the future electricity system and analyzes the architecture with a use case in coordinated voltage control (CVC). The work starts from envisioning the architecture and its requirements. Next, the CVC use case is explained to indicate how the enterprise-to-enterprise service scheme can facilitate the development and management of electricity-related communication systems. Thus, the research objective is: *Analyze the suitability of a cyber-physical service architecture for enterprises in the electricity domain, based on a coordinated voltage control use case.* That is, the research method is constructive. The construct is the architecture concept, and its analysis is based on the benefits compared to an earlier design.

This paper has the following parts. Section 2 elaborates the background. Section 3 explains the suggested CPS architecture. Then, Section 4 introduces the use case for the analysis in Section 5. Finally, Section 6 discusses the results, followed by a conclusion in Section 7.

2. BACKGROUND OF SERVICES AND CPS

Inherently, a CPS assumes interaction between the physical world and its cyber counterpart. For this, a CPS can be considered have five layers, the "5C": connection, conversion (data to information), cyber, cognition, and (self-)configuration, enabling self-awareness, prioritization, optimization, and resilience (Lee et al., 2015). A CPS can consist of other CPSs, forming a system of systems (Lezoche and Panetto, 2020). In smart grids, CPSs face multiple challenges, including the heterogeneity of communication protocols and lack of methods for safety, security, reliability, and resilience (Jha et al., 2021). Earlier, CPSs in the energy domain have been called *cyber-physical energy systems* (CPES), e.g., (Park et al., 2020).

Earlier studies present architectures for services, CPSs, and electricity systems, but unlike this work, they lack the combination of CPSs and a distributed, non-hierarchical service approach for the entire electricity system. Tanjimuddin et al. (2022) have researched the suitability of

⋆ This work was funded by the projects 'Distributed Management of Electricity System' (DisMa, Academy of Finland grants no. 322673 and no. 322676) and 'Integrated Automation for Distribution Grid and DERs' (INGA, Business Finland, 3310/31/2022).

10.1016/j.ifacol.2023.10.1000

a service framework for single-microgrid control. In the grid scope, the platform SOGNO and the subsequent project PLATONE have taken electricity distribution (in the scope of Distribution System Operators or DSOs) towards services and Internet communication (Pau et al., 2022). However, they lack the CPS viewpoint as well as dynamic discovery and orchestration, which are becoming important in the volatile smart grids of the future. Lu et al. (2019) have suggested a service architecture for CVC. Still, this is limited to a single-enterprise scope. Usually, the service solutions studied are centralized. For example, Ge et al. (2022) propose a plan-based approach for resilient microgrids, whereas Sanduleac et al. (2022) have studied a centrally coordinated energy community.

3. CYBER-PHYSICAL ELECTRICITY SYSTEM

3.1 Electricity System Architecture

To meet the research objective, this study suggests an architecture to utilize the potential of the customers in the electricity network. Currently, this potential service offering remains unexploited due to the operator-centric approach in electricity (the operators being, e.g., DSO, Transmission System Operators (TSO), or aggregators). However, the customers could sell services to one another, e.g., for power management, energy cost optimization, or balance management, when a customer fails to use all the energy it has either purchased or produced. They should be able to form *microgrids* where the participants sell services to one another, or the services could be provided between microgrids. The microgrid can be physical or virtual, lacking physical borders. On the other hand, even the operators would benefit from a scheme that facilitates service business by relaxing the current hierarchy. Although the item being sold is ultimately either energy or power management, the services still necessitate control over scheduling and magnitude, requiring the cyber element.

Fig. 1 illustrates the architecture, covering both cyber and physical. In the physical world, electricity is produced and consumed, and the environment faces repeated, sometimes unexpected changes. Renewable energies cause more of challenge in managing the system due to fluctuation. For this management to be effective, the cyber world should provide services that are traded with Internet tools via a communication framework. The services include, e.g., voltage control, frequency control, and balance management. They are provided by residential or commercial actors or microgrids, and the service consumers are either other microgrids or operators. Regarding the communication framework, it should enable interoperability, and there should be tools to offer, discover, and manage the services for each need. This necessitates an information model, communication protocols and messaging systems, and various functions to support the services: descriptions, registry, orchestration, and configuration. Although the concept is simple on a high level, it sets requirements regarding communications between the actors to enable timely service delivery as agreed by the participants.

Besides the main functionality, the architecture must fulfil a number of auxiliary features. It should enable the supervision and logging of communication to enable the tracking

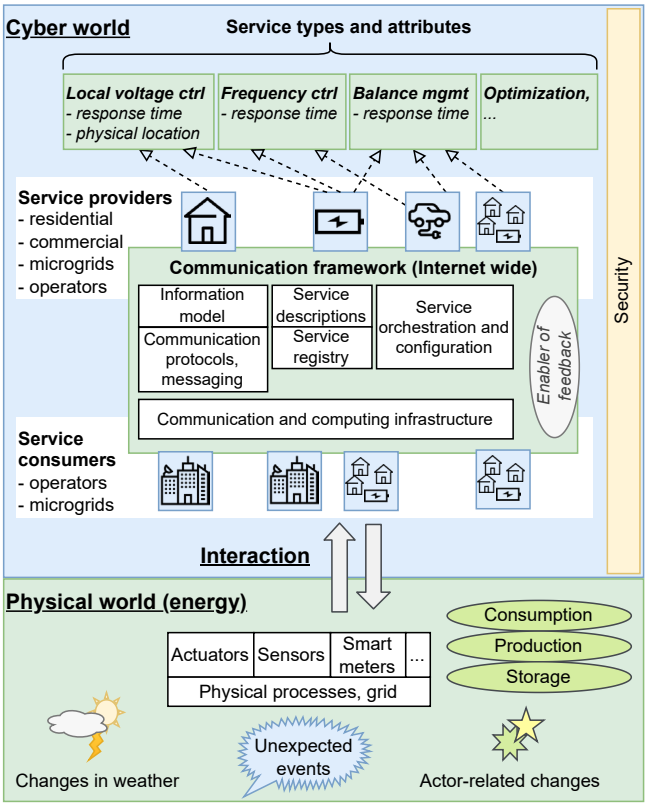

Fig. 1. Conceptual CPS architecture for electricity distribution services

of what happens in the system of systems. This facilitates recovery from fault situations and enables the correction of balance errors, which are common in electricity systems. Regarding security, there should be mechanisms for confidentiality, integrity, and availability. Confidentiality is essential in electricity systems where the data typically associates to a person. Availability is necessary as unexpected downtime can result in physical damage. The concrete security measures include, e.g., authentication, access control, encryption, and redundancy. The measures must span both the framework and the service instances.

Regarding the implementation technologies for the services, multiple candidates exist. Restful interfaces (e.g., HTTP) are suitable for request-response communication. Respectively, repeated Internet-level data deliveries are more efficient with message brokers decoupling the communication, such as MQ Telemetry Transport (MQTT) and Advanced Message Queuing Protocol (AMQP), some implementations of which are highly scalable. Obviously, some safety-related applications require deterministic, short latencies for which some real-time capable alternative is required. Existing domain-specific standards provide information models, including at least IEC 61850 for substation automation and IEC 61968 for the common information model (CIM) in energy management.

3.2 Enterprise Interoperability

The proposed architecture, i.e., the cyber-physical electricity system, can be characterized as a complex, composite interoperability problem. Interoperability must be reachable from devices and data to organizations and busi-

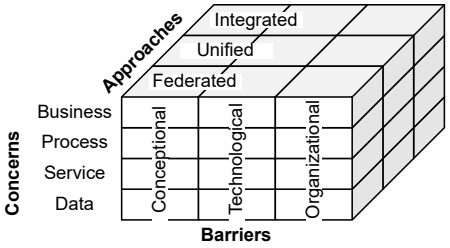

Fig. 2. Framework for enterprise interoperability; modified, re-drawn from (Chen et al., 2008)

nesses. The problems can be illustrated with Framework for Enterprise Interoperability (FEI; see Fig. 2). Elaborated by Chen et al. (2008) and standardized in ISO 11354-1, FEI has three interoperability dimensions: concerns, barriers, and approaches. In this work, FEI was chosen instead of Reference Architectural Model Industrie 4.0 (RAMI 4.0; Adolphs et al. (2015)), because this lacks a dimension for barriers and approaches in enterprises.

Interoperability concerns cover *data* and its interpretation, *services* (both computational and business services), business *processes*, and finally organizational (*business*) matters, such as decision-making, legislation, and culture (Chen et al., 2008). In the cyber-physical electricity system, business processes cause difficult challenges as there are currently no standards to align cross-organizational business processes with concrete technological systems. The enterprises are siloed and have little mutual interaction. Eventually, enterprise interoperability is reached only by aligning processes and technology. The topmost level, business, is risky but maps primarily to negotiations and cultural factors rather than technology.

Interoperability barriers are either *conceptual* (semantic and syntactic), *technological* (computers, infrastructure, etc.), or *organizational* (responsibilities and organizational structures) (Chen et al., 2008). Regarding the suggested architecture, conceptual barriers are most significant due to their abstract nature. To reach common concepts, there must be standards or at least commonly agreed specifications. Technological barriers can be overcome by simply choosing an appropriate technology. Organizational barriers cause a need for a neutral entity for governance, maintaining of the common architectural rules. If this role cannot be taken by any existing organization, a new non-profit consortium could be formed.

Interoperability approaches cover three methods that directly affect the scalability of the architecture: *integrated* approach assumes a common data format, agreed by the participants communicating; *unified* approach means that there is a common format but only as a meta-model; and *federated* approach refers to cases where no common data model exists and any mappings are created as needed (Chen et al., 2008). In this study, the approach must scale to large networks, which leaves any federated point-to-point approach unusable. The integrated approach provides the best digitalized interoperability due to a common data model and business processes, but this can be too complex due to the heterogeneous business environment. Therefore, the unified approach is a potential compromise. Not every customer or actor is likely to specify its own information model, but there could be a few alternatives depending on technology suppliers and geographical areas. This necessitates a mapping technique, such as ontologies, to translate the communication on the fly.

4. VOLTAGE CONTROL USE CASE

For a concrete use case, this section explains a coordinated voltage control (CVC) scheme for a medium voltage network, originally introduced by Kulmala et al. (2014). This use case was realized as a proof-of-concept demonstration (Ruuth et al., 2022), which ran continuously for 6 months.

The coordinated voltage scheme attempts to minimize voltage quality issues in an electricity distribution network. In short, the variable power of loading and generation causes voltage fluctuations, which have an adverse effect on electricity quality. Voltage control generally refers to control schemes for generation units (and other voltage control capable resources) that consider the terminal voltage of the unit and adjust, e.g., the reactive power output of the generator. In coordinated voltage, the control decisions of a network area are made jointly and in an optimized way. Therefore, CVC is dependent on the underlying communication architecture to facilitate its functionalities.

The conceptual system of the CVC design is visualized in Fig. 3. The principal components of the CVC system are Substation Automation Units (SAU), which cover the edge computing hardware that run the numeric CVC algorithms. These units are controlled by DSOs via a Supervisory Control and Data Acquisition (SCADA) system, which in turn receives static information from distribution management system (DMS). These systems are higher in the control hierarchy than SAUs that receive operational parameters (e.g., voltage limits and network models) from them. SAUs in turn gather information from Intelligent Electric Devices (IED) and Automated Meter Reading (AMR) infrastructure. Additionally, they send control commands to various Automatic Voltage Regulators (AVR) of the network connected resources.

Algorithmically, CVC offers two distinct functionalities: state estimation and optimal power flow (OPF) calculation. State estimation is a numeric algorithm to deduce the

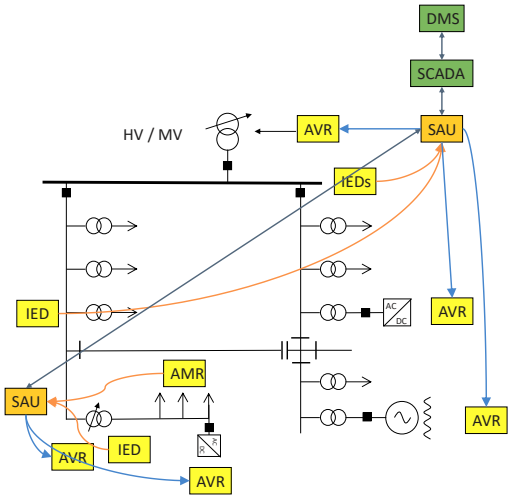

Fig. 3. Concept of coordinated voltage control

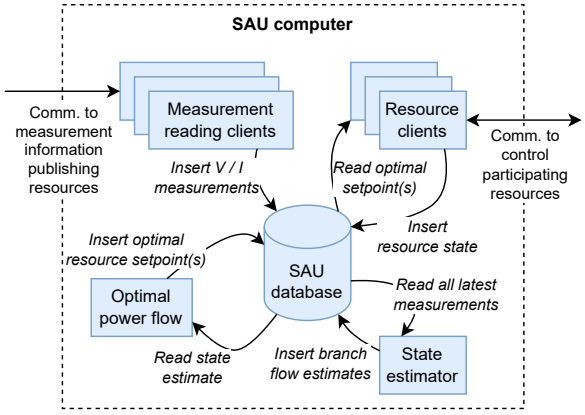

Fig. 4. SAU internal algorithms and workflow

nodal voltages and branch currents of the entire network based on sparse measurements. OPF algorithm in turn calculates the best possible setpoints for network's primary controllers based on the estimated state.

Fig. 4 visualizes the algorithms and their interaction with the resources. There is a centralized database that enables communication between the functions. State estimation receives measurements from the resources, and OPF sets control values based on the state. To gather the measurements, multiple software clients are required. They exchange information between the SAU and the external resources, which are, in practice, AVRs and IEDs. AVRs participate in the actual control actions (e.g., generator reactive power control) whereas IEDs and AMR usually gather monitoring data from the network.

The design has two major deficiencies. First, the client applications were created as device specific in the demonstration, which means that each resource was controlled by a single tailor-made application. Therefore, the integration of new controllable resources is a manual task with a significant workload. Second, the parametrization of the internal functionalities of SAUs and models is static. This reduces usability, since the control approach is unable to adapt to, e.g., network switching state changes.

5. ANALYSIS OF ARCHITECTURAL BENEFITS

Fig. 5 shows a re-design for the CVC use case built upon the proposed CPS-based service architecture. The upper part shows the services, providers, and consumers. Of the services, localized CVC, measurements and monitoring, and primary control appear in the earlier design too. The architecture facilitates service trading between enterprises as shown with flexibility services in the figure. This service can be provided by, e.g., an aggregator.

In the re-design, the framework crosses physical borders with services that are provided by some actors and consumed by others. For each service, a suitable communication protocol is selected considering the timing requirements and scheme. For example, a non-critical monitoring task is easiest to implement with MQTT, whereas any quick, deterministic control necessitates an alternative, such as a protocol from IEC 61850. Respectively, MQTT can deliver arbitrary payloads and thus allows for freedom in information structures. To help in inter-organizational

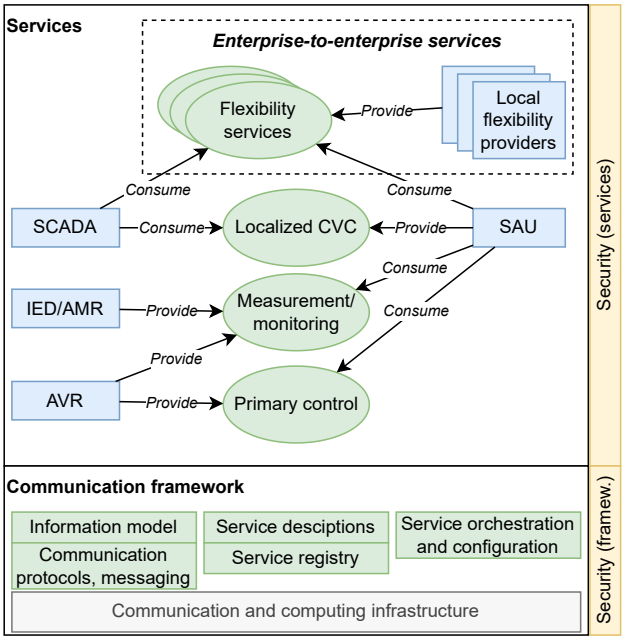

Fig. 5. CVC re-designed with the CPS architecture

communication, the payload can be a record with contextual metadata or encrypted for additional security.

The benefits stem especially from loose coupling between the systems, making the approach dynamic. A new service consumer can join the framework by simply knowing the target address. As new services appear, the consumers receive the information about this via service registry and orchestration. This is easier compared to legacy approaches where the network nodes either are configured manually or can only operate in a local network. On the other hand, the framework guarantees security with authorization.

The following paragraphs analyze the CPS architecture by assessing how this can benefit the CVC scheme. The requirements referred to were elaborated in Section 3.

Service business between customers, including microgrids, should be supported (Section 3.1). In the earlier CVC, service trading is difficult due to point-to-point connections and a strict operator binding. The suggested framework facilitates service business with more of resources available for voltage control. Besides, the CVC system can easily sell its service to customers in the network.

Supervision and logging should be supported (Section 3.1). Even the earlier CVC, the SAU (see Fig. 4) or any other node can implement such logging, but the scope is limited to the node itself. In contrast, in the suggested architecture, all the communication regarding CVC occurs through the communication framework. This brings a centralized element, making it straightforward to log and supervise customer messaging and activity. A centralized logging system, attached to a communication framework, has earlier appeared in (Kannisto et al., 2022).

Security measures are necessary (Section 3.1). In CVC, the communication can be trustworthy only if the service can rely on the external data and services. Thus, each system connecting to the communication framework must be authenticated, data encryption is necessary, and access

control must be in place to prevent malicious attempts. If the security fails, the consequences can be physical (e.g., denial of service or inappropriate functionality due to false data) or information related (e.g., exposure of private data). The earlier CVC integrates with clients point-to-point, and any security features are built separately for each link. In contrast, in the suggested communication framework, there is a single approach for security measures. This facilitates the management of system identities and access, improving consistency and interoperability. The security approach can be, e.g., a centralized chain-of-trust mechanism to alleviate the burden of individual component configurations. The concrete security measures should be present both in the framework level (generic measures, such as authorization and data encryption) and in the CVC-related items (based on item-specific needs).

To accomplish resilience, there must be redundant, alternative communication channels. This will keep the framework and services available if a failure occurs. On the other hand, each service should be designed to tolerate unavailability. Furthermore, if a required connection is lost, each system should fail to a safe state.

Interoperability concerns should be met: data, service, process, and business (Section 3.2). In CVC, data and services are delivered between the CVC system and the surrounding enterprises. The invocation of services involves business processes, which should be considered as well, and a business, i.e. people-to-people, viewpoint. The earlier CVC relies on point-to-point connections and therefore forces the concerns to be met separately for each link. Fortunately, the CPS architecture helps this situation by meeting the concerns in the network-wide scope. As a limitation, the current architecture focuses on technology and thus has a limited attention on processes and business.

Interoperability barriers should be overcome: conceptual (syntactical and semantic), technological (communication infrastructure), and organizational (responsibilities and structures) (Section 3.2). In each, the CVC scheme has relied on a combination of operator-centric hierarchy and point-to-point connections. The suggested architecture can enhance the situation regarding each barrier. Conceptual barriers are met with common information models that are a necessity to reach interoperability in CVC (e.g., IEC 61850 for substations and IEC 61968 for energy management). Technological barriers are crossed with a common infrastructure for communication between the systems and enterprises. However, organizational barriers receive little support in this technology-oriented study. These aspects could thus be researched further with business focus.

The interoperability approach must be scalable (Section 3.2). Scalability is a necessity because the number of CVC-related service providers and consumers is arbitrary and this condition applies to any other service types as well. This was not realized in the CVC scheme that relies on the federated approach, i.e., point-to-point that necessitates a laborious effort for each communication link. Instead, the CPS-based communication framework builds upon either the integrated or unified approach. This choice requires further research. The integrated approach requires most agreements between enterprises, whereas the unified approach enables mappings as needed, relaxing the need for a single consensus but increasing work when the communication links are being established and maintained.

In summary, the analysis suggests that the CVC use case can receive considerable benefit from the suggested CPS architecture. Still, the use case is limited in scope and lacks a concrete evaluation for all the aspects, which means that additional proofs of concept are required. Fortunately, the communication requirements of services can be assumed similar in other electricity-related use cases too.

6. DISCUSSION

The results showed that the suggested architecture is beneficial in the CVC use case. However, no other use cases were considered. Although other use cases likely have similar requirements, a future study could cover more.

Although Section 3 named candidate technologies, these necessitate future research. Rest, MQTT, and AMQP were named. Due to the tool support and knowledge base of such Internet technologies, these are cheaper to maintain compared to hard-real-time-capable alternatives, such as fieldbuses. Still, the criticality of each function must be assessed to decide if a determinism is necessary. Regarding information models, there are domain-specific candidates, such as IEC 61968 and 61850. However, additional data structures become important for enterprise interoperability if the existing models lack applicable organization-related structures. Furthermore, supporting technologies are necessary. Arrowhead framework provides tools for authorization in a multi-enterprise service-oriented architecture (Varga et al., 2017) as well as for orchestrating connections in industrial CPSs (Hästbacka et al., 2022). For the infrastructure of enterprise integration, International Data Spaces (IDS) and Gaia-X provide tools for data sharing with data sovereignty and autonomy (Pettenpohl et al., 2022; Tardieu, 2022). They help in reaching legal interoperability in a digitalized way, promising to reduce organizational barriers. Overall, although the existing technologies provide essential pieces, it remains future work to complete and experiment with the architecture.

The network of cyber-physical energy systems is not only technology but forms a digital business ecosystem. This is more demanding compared to an open market, which requires no coordination, and a hierarchical supply chain or vertically integrated organization, which has a low modularity (Pidun et al., 2019). A future study could include the ecosystem viewpoint and therefore extend the coverage to business aspects, as this would include more of interoperability concerns and barriers in the FEI cube.

7. CONCLUSIONS

This paper suggested and analyzed a cyber-physical system architecture for a use case in the future energy system. In the architecture, the actors of the electricity system are cyber-physical enterprises that must adapt to changes in at least two ways: (1) in the physical world, maintain the stability of the electricity system with the services provided and (2) in the cyber world, adapt to changes in the environment and maintain interoperability.

Based on the results, the service-oriented CPS architecture is suitable for a coordinated voltage control use case. This

use case has requirements similar to other services in the electricity system, such as frequency control and balance management where the physical service is ultimately either energy or power management. It can be therefore argued that the architecture has a wide applicability in customer- or microgrid-produced services. Compared to the contemporary, DSO-centric electricity system, the advantages of the architecture include adaptiveness and the ease of instantiation of services in the absence of a forced hierarchy. This encourages customers to use their local resources for the good of the whole energy system.

For future work, the architecture could be designed more extensively, considering both organizational business requirements and concrete technologies. More of use cases could be included and proven with demonstrations.

REFERENCES

Adolphs, P. et al. (2015). Reference architecture model industrie 4.0 (RAMI4.0). VDI/ZVEI.

Chen, D., Doumeingts, G., and Vernadat, F. (2008). Architectures for enterprise integration and interoperability: Past, present and future. *Comput. Ind.*, 59(7), 647–659. doi:10.1016/j.compind.2007.12.016.

Dreidy, M., Mokhlis, H., and Mekhilef, S. (2017). Inertia response and frequency control techniques for renewable energy sources: A review. *Renew. Sust. Energ. Rev.*, 69, 144–155. doi:10.1016/j.rser.2016.11.170.

Ge, P., Teng, F., Konstantinou, C., and Hu, S. (2022). A resilience-oriented centralised-to-decentralised framework for networked microgrids management. *Appl. Energy*, 308, 118234. doi:10.1016/j.apenergy.2021.118234.

Hästbacka, D., Halme, J., Barna, L., Hoikka, H., Pettinen, H., Larrañaga, M., Björkbom, M., Mesiä, H., Jaatinen, A., and Elo, M. (2022). Dynamic edge and cloud service integration for industrial IoT and production monitoring applications of industrial cyber-physical systems. *IEEE Trans. Ind. Inf.*, 18(1), 498–508. doi:10.1109/TII.2021.3071509.

Jha, A.V., Appasani, B., Ghazali, A.N., Pattanayak, P., Gurjar, D.S., Kabalci, E., and Mohanta, D.K. (2021). Smart grid cyber-physical systems: communication technologies, standards and challenges. *Wireless Netw.*, 27, 2595–2613. doi:10.1007/s11276-021-02579-1.

Kannisto, P., Heikkilä, V., Hylli, O., Attar, M., Repo, S., and Systä, K. (2022). SimCES platform for modular simulation: Featuring platform independence, container ecosystem, and development toolkit. *SoftwareX*, 19, 101189. doi:10.1016/j.softx.2022.101189.

Kulmala, A., Repo, S., and Järventausta, P. (2014). Coordinated voltage control in distribution networks including several distributed energy resources. *IEEE Trans. Smart Grid*, 5(4), 2010–2020. doi:10.1109/TSG.2014.2297971.

Lee, J., Bagheri, B., and Kao, H.A. (2015). A cyber-physical systems architecture for Industry 4.0-based manufacturing systems. *Manuf. Lett.*, 3, 18–23. doi:10.1016/j.mfglet.2014.12.001.

Lezoche, M. and Panetto, H. (2020). Cyber-physical systems, a new formal paradigm to model redundancy and resiliency. *Enterp. Inf. Syst.*, 14(8), 1150–1171. doi:10.1080/17517575.2018.1536807.

Lu, S., Repo, S., Salmenperä, M., Seppälä, J., and Koivisto, H. (2019). Using IEC CIM standards and SOA technology for coordinated voltage control application. In *2019 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, 1–5. doi:10.1109/ISGTEurope.2019.8905541.

Panetto, H., Iung, B., Ivanov, D., Weichhart, G., and Wang, X. (2019). Challenges for the cyber-physical manufacturing enterprises of the future. *Annu. Rev. Control*, 47, 200–213. doi:doi.org/10.1016/j.arcontrol.2019.02.002.

Park, K.T., Kang, Y.T., Yang, S.G., Zhao, W.B., Kang, Y.S., Im, S.J., Kim, D.H., Choi, S.Y., and Do Noh, S. (2020). Cyber physical energy system for saving energy of the dyeing process with industrial internet of things and manufacturing big data. *Int. J. Precis. Eng. Manuf.-Green Tech.*, 7, 219–238. doi:10.1007/s40684-019-00084-7.

Pau, M., Mirz, M., Dinkelbach, J., Mckeever, P., Ponci, F., and Monti, A. (2022). A service oriented architecture for the digitalization and automation of distribution grids. *IEEE Access*, 10, 37050–37063. doi:10.1109/ACCESS.2022.3164393.

Pettenpohl, H., Spiekermann, M., and Both, J.R. (2022). International data spaces in a nutshell. In *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage*, 29–40. Springer. doi:10.1007/978-3-030-93975-5_3.

Pidun, U., Reeves, M., and Schüssler, M. (2019). Do you need a business ecosystem. Boston Consulting Group.

Ruuth, K., Supponen, A., Mutanen, A., Repo, S., Røsland Rosenørn, K., and Møller, M. (2022). Lessons Learnt in Implementation of Coordinated Voltage Control Demonstration. In *CIRED 2021 - The 26th International Conference and Exhibition on Electricity Distribution*, 1702–1706. doi:10.1049/icp.2021.1788.

Sanduleac, M., Ionescu, C., Mandis, A., Gropa, V., Efremov, C., and Sanduleac, V. (2022). Solutions for digital interaction of a resilient energy community in a service-oriented framework. In *2022 International Conference and Exposition on Electrical And Power Engineering (EPE)*, 1–6. doi:10.1109/EPE56121.2022.9975792.

Tanjimuddin, M., Kannisto, P., Jafary, P., Filppula, M., Repo, S., and Hästbacka, D. (2022). A comparative study on multi-agent and service-oriented microgrid automation systems from energy internet perspective. *Sustain. Energy Grids Netw.*, 32, 100856. doi:10.1016/j.segan.2022.100856.

Tardieu, H. (2022). Role of Gaia-X in the European data space ecosystem. In *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage*, 41–59. Springer. doi:10.1007/978-3-030-93975-5_4.

Tikka, V., Mashlakov, A., Kulmala, A., Repo, S., Aro, M., Keski-Koukkari, A., Honkapuro, S., Järventausta, P., and Partanen, J. (2019). Integrated business platform of distributed energy resources – case Finland. *Energy Procedia*, 158, 6637–6644. doi:10.1016/j.egypro.2019.01.041.

Varga, P., Blomstedt, F., Ferreira, L.L., Eliasson, J., Johansson, M., Delsing, J., and de Soria, I.M. (2017). Making system of systems interoperable – the core components of the Arrowhead framework. *J. Netw. Comput. Appl.*, 81, 85–95. doi:10.1016/j.jnca.2016.08.028.