BEÜ Fen Bilimleri Dergisi
9 (4), 1865-1871, 2020

BEU Journal of Science
9 (4), 1865-1871, 2020

Derleme Makalesi / Review Article

Towards a Testbed for Dependable Power Distribution Grids

Kubilay DEMİR[1*], Hauke SASCHA[2]

[1]Bitlis Eren University, Department of Electrical Electronics Engineering, Turkey
[2]Landshut University of Applied Sciences, Germany
(ORCID: 0000-0001-5355-2472) (ORCID: 0000-0001-7822-0191)

Abstract
The evolution of power grids into digitized smart grids (SGs) brings about promising opportunities but also considerable challenges. On the one hand, smart grids promise more efficient, sustainable and reliable operation while providing more market functions and better customer service. On the other, however, the distributed nature of power generation in SGs poses challenges w.r.t. dependable distributed command and control (C2), digital service provisioning, and secure and reliable data communication. Distributed C2 of systems such as SGs hinges on reliable, timely and secure data communication. Thus, future SGs will be fully digitized. As such, for dependable SGs, novel, secure, resilient methods and communication protocols must be developed. In order to do so, a novel hardware-in-the-loop simulation testbed should be developed and used to validate the research that is capable of accurately modelling both the digital IT networks that control the SG, as well as the SG's power infrastructure -- from big transformer substations to pro-sumer households. There is a general lack of hardware integrated test-beds that focus on the distributed control and wireless edge networks for smart grids. In this paper, we demonstrate a cyber-physical testbed development framework, which we believe to help the researchers to in the development future cyber-physical testbeds. Our assessment also revels the need for such testbed for implementation of future SG applications.

Keywords: Smart grid, communication, reliability, dependability, digitalization.

Güvenilebilir Dağıtım Şebekeleri için Dijitalleşme

Öz
Güç şebekelerinin sayısallaştırılmış akıllı şebekelere (AŞ'ler) evrimi gelecek vaat eden fırsatlar ve aynı zamanda önemli zorluklar yaratmaktadır. Bir yandan, akıllı şebekeler daha fazla pazar işlevi ve daha iyi müşteri hizmeti sunarken daha verimli, sürdürülebilir ve güvenilir bir operasyon vaat ediyor. Öte yandan, AŞ'lerde elektrik üretiminin dağınık doğası, güvenilir dağıtılmış komuta ve kontrol (K2), dijital servis sağlama ve güvenli ve güvenilir veri iletişimi açısından zorluklar doğurmaktadır. AŞ'ler gibi dağıtılmış K2 sistemleri, güvenilir, zamanlı ve güvenli veri iletişimine dayanır. Böylece, gelecekteki AŞ'ler tamamen dijital hale getirilecektir. Bu nedenle, güvenilir AŞ'ler için yeni, güvenli, esnek yöntemler ve iletişim protokolleri geliştirilmelidir. Bunu yapabilmek için, hem AŞ'yi kontrol eden dijital BT (bilişim teknolojileri) ağlarını hem de AŞ'nin güç altyapısını doğru bir şekilde modelleyebilecek araştırmayı doğrulamak için yeni bir çevrim içi donanım simülasyonu testi geliştirilmeli ve kullanılmalıdır -- büyük trafo merkezlerinden tüketici hanelerine kadar. Akıllı şebekeler için dağıtılmış kontrole ve kablosuz kenar ağlara odaklanan, genel donanım entegre edilmiş test ortamları eksikliği vardır. Bu yazıda, gelecekteki enerji ağlarının temel taşı olduğuna inandığımız siber-fiziksel bir test ortamı öneriyoruz. Değerlendirmlerimize göre: fiziksel elektrik şebekesi birimlerini BT teknolojileri ile beraber çalıştıran bir test ortamı, AŞ uygulamaları için çok daha realistik sonuçlar verecektir.

Anahtar kelimeler: Akıllı elektrik tesisleri, güvenilirlik, haberleşme, dijtalleşme.

1. Introduction

Power generation and distribution systems are among the largest and most complex cyber-physical system of systems ever deployed, both technologically and administratively (see Figure 1). Over the better part of a century, the basic tenets of overall systems design in this domain have changed little.

---

[*] Corresponding author: kdemir@beu.edu.tr

Received: 19.12.2019, Accepted: 28.05.2020

Complexity has been handled by implementing a hierarchical design approach: energy is generated by massive power station and delivered via tightly controlled transmission and distribution grids, thus segregating power generation and consumption. Furthermore, institutional systems operators control the generation, grid resources, and their mutual coordination using dedicated industrial control systems. Due to the penetration of renewable energy resources into the entire power grid, this is changing [1,5].

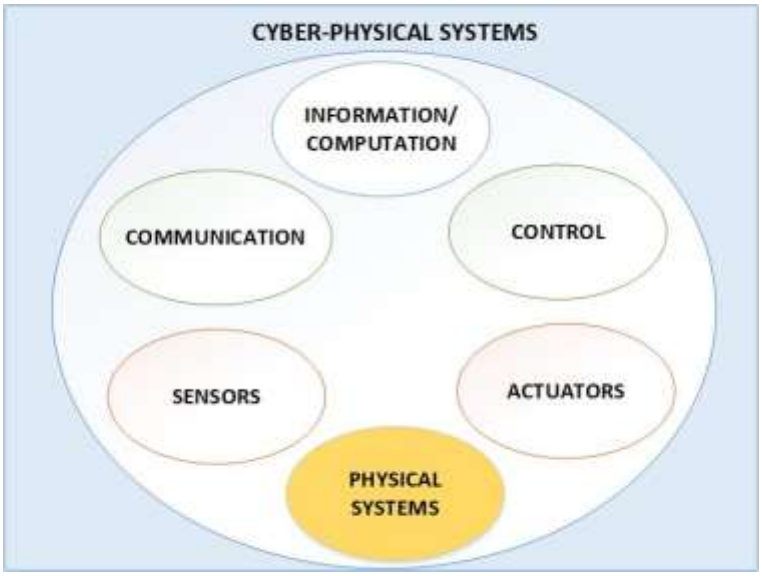

Figure 1. Illustration of Cyber-Physical Systems

The centrally managed power grid is in the process of being transformed into an adaptive, distributed, fully digitized power infrastructure, the Smart Grid. The trend towards distributed power generation is not only envisioned to yield a more efficient, dependable and resilient power grid, but also to lessen the reliance on fossil fuels for power generation. Thus, control structures for the distribution grid must be capable of handling the demands imposed by the massive incorporation of distributed sustainable energy sources such as solar and wind power [1,2,5].

As energy production is now pushed towards the edge of the network, i.e., occurring in the low-voltage distribution grid, new opportunities and challenges arise. On the one hand, distributed energy production offers benefits with regard to higher autonomy of local energy grids, potentially giving distribution grid operators more independence from the transmission grid. As a consequence, less energy has to be drawn from the transmission grid, resulting in reduced strain on system components, such as transformers, and reducing the investment that will be needed for the expansion of transmission lines and traditional centralized power generation capacity [1]. Less reliance on centralized systems is foreseen to provide dependability benefits, particularly with regard to digital control systems [1].

On the other hand, distributing energy generation brings about new challenges in a number of fields, ranging from regulatory questions, to the need for new business models, to power infrastructure and IT investments, and secure, dynamic, dependable, distributed, digital control mechanisms [2].

Reliable, secure C2 and communication protocols, in conjunction with the testbed demonstrator, in turn, enable the development of (value-added) digital services on the energy network. Realtime simulations in both the IT and Power Systems side integrate with physical grid and IT hardware components. The components required and their integration into the proposed lab infrastructure are listed further down. There is a general lack of hardware integrated test-beds that focus on the distributed control and wireless edge networks for smart grids. In this paper, we present a cyber-physical testbed framework, which we believe to be a cornerstone of future energy networks.

The rest of the paper are organized as follows. Research goals and methodology is presented in section 2, underlying the basic principles and operating fundamentals to implement the proposed testbed. Section 3 defines the proposed testbed. Section 4 presents the work plan and research results, along with along with probable research topics that can be conducted on the testbed. We finally conclude the paper and discuss the future research directions in section 5.

2. Methodology and Testbed

In construction of the cyber-physical testbed, the focus should be on the investigation and development of a digital infrastructure and integrated physical platform for dependable distribution-side smart grid services. This comprises:

- Analyses of the required distribution of IT hardware and software systems,
- Analyses of the communication systems and protocols necessary to link the distributed IT systems.
- Analyses of the physical resources (power components) that can be integrated with cyber systems.
- Development of a hardware integrated cyber-physical simulation testbed.

The aim in the building such a testbed should be as follows:

- Enhancement of existing and development of novel methods, protocols and software systems for distributed coordination and control for the smart grid,
- Monitoring and analyzing the effects of cyber-attacks over the physical systems by using the developed testbed.

Given the nature of smart grids as part of a critical infrastructure operated under heavy regulation in an established market environment, the conducted researches running on the testbed should comply with the number of constraints [3]. Considering these constraints, assessment of the researches running on the testbed should be able to the researcher to answer the question of how digitization in low-voltage energy grids can be used to yield a distributed power system that is more dependable, secure, efficient, sustainable and resilient than traditional energy networks. To answer this question, the researchers can use techniques from the fields of computer science, such as distributed systems design, software engineering, computer networks and communication, and dependable systems, and apply it to the electrical engineering field of power generation and distribution. Moreover, regulatory aspects are taken into account during systems development. IT investment and integration costs should be also balanced against a benefits analysis when proposing the deployment of systems [2].

2.1. Methodology

Methodologically, the proposed testbed-construction research is conducted in three phases, each of which builds upon the previous phase in a bottom-up approach:

Phase 1: Pro-Sumer Household Coordination and Control; During this phase, the researchers should determine the demands of distributed coordination required at the home level. This includes the integration of energy producing systems (e.g., photovoltaics), energy consumers (e.g., Electric Vehicles), and energy stores and buffers (e.g., home batteries) into a home-level control and coordination system. At this level, the technical constraints with regards to aspects such as communication latency, security and resilience to attacks are more controllable than in later phases, providing a base for the development of protocols and systems [2,3].

Phase 2: Neighborhood Distribution Systems Coordination and Control; Moving from a single household to a complete segment on the low-voltage distribution grid, the methods, protocols and systems developed in the previous is extended and, where necessary, complemented with new systems for the coordination of distributed resources. At this level, the distribution grid provider with its power infrastructure components becomes an active participant in the coordination. Ancillary services (frequency and voltage control, scheduling and dispatching, etc.) have to be taken into account at this level [1,2]. Additionally, communication on this level occurs over larger area, possibly using various different types of network (protocols) and carriers, and has to be coordinated developing new protocols. The feasibility of implementing a local energy exchange and services platform on top of the coordination system, i.e., the local digitized energy control center, should also be investigated.

Phase 3: Distribution-Transmission Grid Interoperation; Finally, interoperation between the transmission grid and the digitized distribution grid should be investigated. In particular, the researchers should look at how to achieve integration of smart, potentially self-sufficient microgrids, distribution grids and the transmission grid. This includes ensuring basic ancillary services required to guarantee overall network stability, the digital services required between distribution grid customers, the distribution grid operator and the transmission grid operator, and the digital infrastructure that has to be deployed for efficient and dependable operation. Beyond these basic services, higher-level data driven services for various scenarios should be integrated into the local energy control center. These scenarios cover potential services between distribution and transmission grid operator, such as a virtual power plant operation mode of the distribution grid, as well as service interfaces between pro-sumer distribution grid customers and the energy market which are mediated by the distribution grid operator [1,2]. Regulatory, business and power & IT investments are main factors are taken into account during development.

To handle the above-mentioned three phases during the construction of the testbed integrating simulation, emulation, and physical systems, 3 steps below should be followed:

- what kind of devices, software and protocols do we have to develop for a SG pro-sumer household, challenges etc.
- then moving on to integration of SG pro-sumers into the local distribution grid, challenges of C&C for the distribution grid for the operator, required development and invest in local and regional power control systems, potentially business side, Deterlab large network and real-time simulations, etc.
- then moving on towards challenges wrt interoperation of pro-sumers, distribution grid operator and transmission operator.

2.2. Testbed

The foundation of implementing these phases is a robust integrated simulation framework with hardware-in-the-loop. Realtime simulations in both the IT and Power Systems side should integrate with physical grid and IT hardware components [4,7]. There is a general lack of hardware integrated test-beds that focus on the distributed control and wireless edge networks for smart grids, which we believe to be a cornerstone of future energy networks. To fully implement an energy and communication grid testbed we need to include power infrastructure and control systems, in addition to the dataflow and communication IT infrastructure.

For the power side, the researcher should focus on creating a real-time hardware-in-the-loop test bed using such as EV batteries and other electrical system components with a Real-Time Digital Simulator (RTDS). RTDS is capable of simulating high voltage transmission systems in the safety of software and distribution grids on scales impractical to physically model in a lab. Connected with real hardware large quantities of simulated smart grid data can be generated by both the simulation and real-world devices in unison synchronized with NTP and GPS timestamps. This allows a realistic integration of distributed generation resources to both the edges and intermixed with existing established multi-bus transmission and distribution systems, many of which have anonymized models available online for free [4,7].

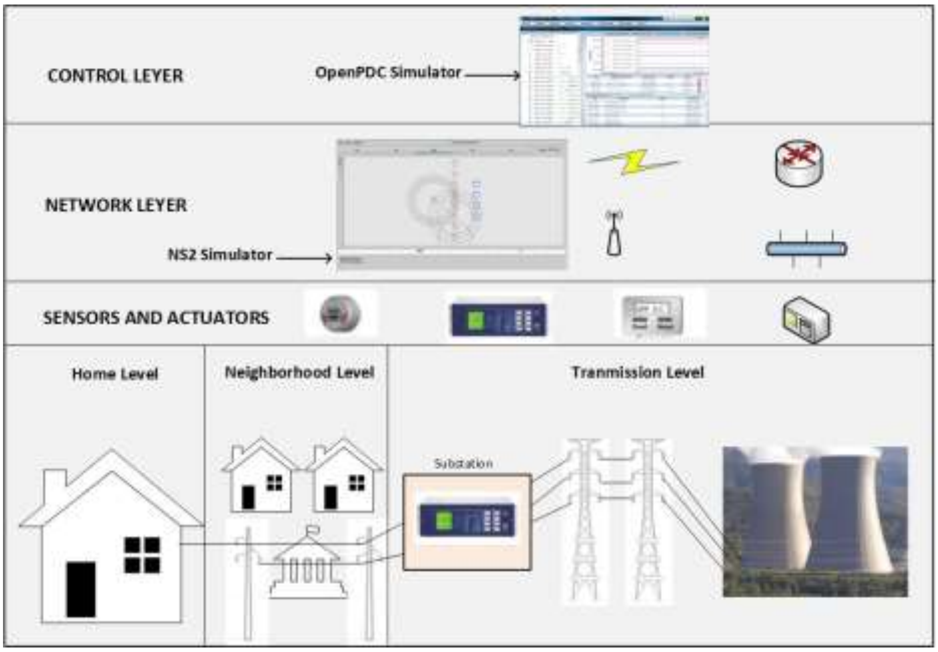

Figure 2. The proposed Cyber-Physical test bed architecture

We envision the communication side of smart distribution grids taking the form of a neighborhood area network (NAN) wireless communication being the basis for communication command and control processes from a power distribution network (PDN) as depicted in Figure 2. Some test-beds support wireless communication but all for indoor communication. There is a lack of similar testbeds for wide area outdoor networks, which support outdoor wireless sensor networks (WSN) deployment and/or usage of cellular carrier networks [4,7]. Analysis is needed on the type and quality of service system operators would need to negotiate for in a service level agreement, as some devices and applications need bandwidth, while others instead require latency or uptime guarantees. Cisco Fog routers, which are equipped with cellular modems and standard WiFi frequencies, in addition to the ability to run custom code, make a useful testbed component for testing code running across a wireless network. For more advanced wireless testing, software defined radios provide access to custom configurations of wireless spectrum and protocols.

To emulate the full wired network attack surface, Deterlab can create large networks with varying attributes and computing capacity to act as a WAN and PDN transfer medium for the data. It's capability to spin up virtual machines on nodes defined throughout a network simulator (NS) graph allows for inserting code for data processing, overlay networks, or adversarial network members [4,7]. This WAN network, in tandem with wireless networking components, is key to testing the full scope of security risks and implications to a mixed public private utility network.

Phase 1 Using these components the researchers should begin phase 1 by accurately modeling a pro-sumer household and its connection to the PDN. They then create a complete hardware-in-the-loop setup based on the model system implemented at the existing power infrastructure hardware. They can implement the testbed to control and receive feedback from the existing hardware systems, which include photovoltaics, batteries, and EVs connected to an energy bus system. They then analyze this system to understand it's operation under standard conditions and under attack scenarios, from which we determine the requirements for reliable operation of this pro-sumer household. From this they can amend and extend the design of the command and control infrastructure, for instance by installing further devices such as code running edge routing technology. This yields a model of a pro-sumer household connected to a smart distribution grid.

Phase 2 From the phase 1 model, the researchers build up a complete distribution grid with multiple pro-sumer households tweaking their parameters to see the impact on their neighbors, the distribution grid, and renewable generation sources. From this they look at modeling small, localized control centers and the interactions with control entities on the distribution grid. They should look specifically at the control data flow between command components on the distribution grid, focusing on the components of the system that benefit from digitizing. Based on this research they theorize changes in the overall control topologies, suggesting hierarchical approaches and methodologies for distributing control logic to computation systems located across the distribution network.

Phase 3 focuses on the interconnect between the distribution and transmission grid at the substation level. Aim of the phase is to focus on how the distribution grid and its entities interact with the transmission grid through substation equipment, and look at increased integration based on the demands of protection logic found at the interface between transmission and distribution [6]. The benefits of upgrading substation communications with the distribution grid entities must be determined, thereby providing a complete model for smart distribution grid operation from the transmission grid interconnection to the pro-sumer.

3. Assessment

The proposed testbed enables the researchers to provide novel, secure, resilient and dependable methods for the distribution-side smart grid. The testbed framework focuses on ICT systems, software and protocols to achieve efficient and secure operation, and includes an analysis and countermeasures to attacks. The power infrastructure be modelled but largely assumed to be an existing infrastructure; where necessary, the limited augmentation of lines, generation capacity and electrical system components in the power system should be taken into account, and recommendations made. Specifically, during the development of the testbed, the following steps should be carried out:

- A technical guide on dependable control and coordination of **a smart pro-sumer household**, including secure protocols for data interchange, ICT systems and home grid integration

- A technical guide on dependable control and coordination of **neighborhood grids**, including secure protocols for data interchange, ICT systems and distribution grid integration
- A technical guide on dependable operation of **smart distribution grids from substation to households**, including secure protocols for data interchange, ICT systems and distribution/transmission grid interconnection.

According to our assessment, a testbed constructed based on the above-mentioned criteria provides realistic results for smart grid applications versus the existing testbed testing either ICT or power grid sides.

On the other hands, Figure 3. shows that the applications running on these three power grid areas require remarkably different latencies. While home grid and neighborhood grid require relatively higher and flexible latency values, transmission grid requires strict latency values, which is not easy to provide with on the shelf products [1-2]. Moreover, Table 1 denotes while transmission grid requires high reliability and security, home and neighborhood grids require high privacy and medium reliability and security [3,4].

To properly model such a complex system with different and dynamic latency, reliability and security requirements, we consider that the proposed hardware integrated and cyber-physical smart grid testbed is necessary and a must for safety implementation of future smart grid applications. The proposed model is built by the authors' large experiences on this field, which helps researchers build such a testbed near future.

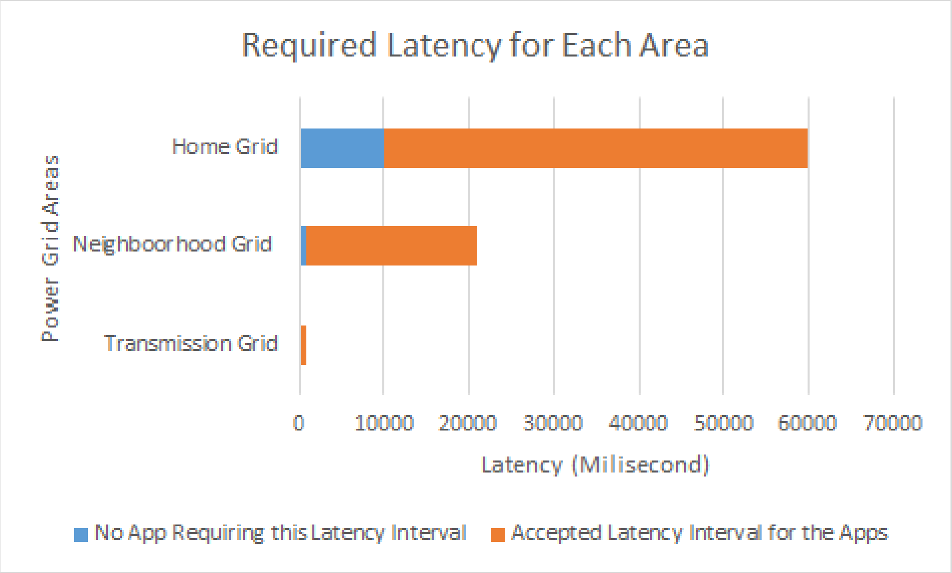

Figure 3. Latency Requirements of Different Power Grid Area Applications

Table 1. Security, Privacy and Reliability Requirements Comparison of Power Grid Areas

	Reliability	**Security**	**Privacy**
Transmission Grid	99,5	High	Low
Neighboorhood Grid	99	Medium	Medium
Home Grid	98	Medium	High

4. Conclusion

Implementing a cyber-physical application, particularly for critical infrastructures such as the Smart Grid, requires a testbed combining both IT infrastructure and the physical infrastructure in order to properly assess the effect of the both failures of cyber and physical components. Wireless networks, in particular in the access network, will be the prominent commination media for SG devices. Modelling wireless media via simulation tools do not give correct results for time-sensitive applications of SG. Therefore, developing such a testbed is of great importance when considering the future of power distribution grids will base on IT infrastructure. However, developing such a complex testbed is not a trivial issue. In this work, we propose a cyber-physical testbed framework with development phases and probable research topics that can be conducted on. Our assessment also shows the requirements of such testbed. For future work, we plan to implement a small-scale such a test bed and discuss possible issues about getting correct results for both IT and power sides.

Acknowledgement

Thanks to my colleagues giving feedback about the paper and the topic.

Author's Contributions

All authors have contributed equally to this work.

Statements of Conflicts of Interest

There is no conflict of interest among the authors.

Statement of Research and Publication Ethics

The author declares that this study complies with Research and Publication Ethics.

References

[1] Fang X., Misra S., Xue G., Yang D. 2012. Smart grid-the new and improved power grid: A survey. IEEE communications surveys & tutorials, 14 (4): 944-980.
[2] Gungor V.C., Sahin D., Koçak T., Ergut S., Buccella C., Cecati C., Hancke G.P. 2013. A Survey on smart grid potential applications and communication requirements. IEEE Transactions on Industrial Informatics, 9 (1): 28-42.
[3] Oldak M., Kilbourne B. 2010. Communications requirements comments of utilities telecom council. Department of Energy, Washington, DC, USA.
[4] Cintuglu M.H., Mohammed O.A., Akkaya K., Uluagac A.S. 2017. A survey on smart grid cyber-physical system testbeds. IEEE Communications Surveys Tutorials, 19 (1): 446-464.
[5] Demir K., Germanus D., Suri N. 2015. Robust qos-aware communication in the smart distribution grid. Peer-to-Peer Networking and Applications, 10 (1): 193-207.
[6] Wang W., Lu Z. 2013. Cyber security in the smart grid: Survey and challenges. Computer Networks, 57 (5): 1344-1371.
[7] Hahn A., Ashok A., Sridhar S., Govindarasu M. 2013 Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid. IEEE Transactions on Smart Grid, 4 (2): 847-855.
[8] https://www.iotone.com/term/cyber-physical-systems-cps/t145 (Accessed: 07.11.2019).