IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 13, 2016, accepted January 17, 2016, date of publication February 18, 2016, date of current version March 17, 2016.

Digital Object Identifier 10.1109/ACCESS.2016.2531279

Resilience and Security: A Qualitative Survey of Urban Smart Grid Architectures

PETER EDER-NEUHAUSER, TANJA ZSEBY, (Member, IEEE), AND JOACHIM FABINI
Communication Networks Group, Institute of Telecommunications, TU Wien, Vienna 1040, Austria

Corresponding author: P. Eder-Neuhauser (peter.eder-neuhauser@nt.tuwien.ac.at)

This work was supported by the TU Wien University Library through its Open Access Funding Program and the research projects URBEM and SIMULTAN.

ABSTRACT Smart grids require information and communication technology (ICT) in order to control dynamics in the power grid. However, adding ICT creates additional entry points in vulnerable hard- and software, increasing the attack surface, and provides distribution paths that can be used by malware for attacks. This paper provides a qualitative evaluation of smart grid architectures for urban environments, comparing four topology types based on six quality indicators: resource control, security, resilience, quality of service, compatibility, and cost. The impact of each power grid topology on the applicability of ICT components in communication topologies is also considered. We summarize the benefits and drawbacks of each topology with a focus on the implementation of decentralized and self-organizing structures.

INDEX TERMS Information and communication technology, malware, network topology, power grids, self-organizing networks, smart grids.

I. INTRODUCTION

Smart grids utilize ICT to increase efficiency and reliability in the management of dynamic power consumption and generation. Although ICT allows for new capabilities, it also increases the attack surface of the smart grid that must be addressed in order to ensure the security of future energy networks. Khan et. al. [1] and Yu et. al [2] provide a comprehensive survey of technologies, applications, case studies, architectures, and security issues.

This paper provides a qualitative evaluation of four ICT topologies based on existing smart grid reference architectures such as SGAM [3], NIST [4], and BSI [5], [6] among others. These topologies supplement the existing power transmission and distribution hierarchy. We analyze the benefits and drawbacks of each ICT topology in an urban context using six quality indicators: *resource-control, security, resilience, quality of service (QoS), compatibility* and *cost*. The four ICT topologies discussed in the paper are the fully centralized approach, a fully decentralized approach, an autonomous cells structure and mesh networks. These have been derived from the existing reference architectures with a view to ensuring feasible quality of service while increasing resilience and architecture based security. We aim to overcome some of the issues of fully centralized and decentralized approaches by adopting the best of both worlds.

The remainder of the paper is structured as follows: Section II discusses the state of the art of the power grid (energy domain) as well as of communication architectures (ICT domain). In Section III, we present a threat model that emphasizes the need for security in critical infrastructures, discuss basic vulnerabilities and explain the attack surface. Section IV considers propagation vectors based on real world incidents, while Section V looks towards future developments in the energy domain such as microgrids and decentralized generation. In Section VI, we propose four ICT topologies based on the reference architectures from Section II-B. Benefits and drawbacks are weighed in Section VII with respect to resilience and security aspects. Section VIII concludes the paper. The main contributions of this paper include qualitative comparisons and concrete proposals for smart grid topologies with regard to architectural vulnerability and security.

II. STATE OF THE ART

The following section provides an overview of power and ICT infrastructures in todays grids (Fig. 1). Supervisory Control and Data Acquisition (SCADA) systems are present in the power transmission grid that includes the Ultra-High-Voltage (UHV) and High-Voltage (HV) levels. The power distribution grid including Medium-Voltage (MV) and Low-Voltage (LV) levels does not yet contain ICT. However, smart devices can be found on the Home Appliance (HA) level. Wang *et al.* [7] and Crane *et al.* [8] argue that diversity in a system can increase resilience by reacting to

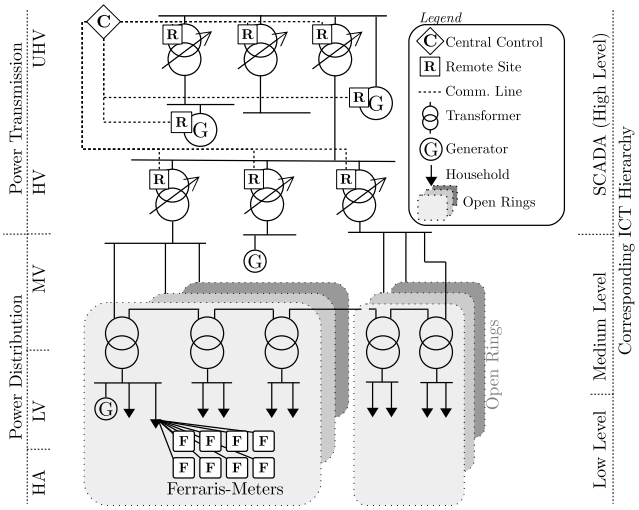

FIGURE 1. The power grid today.

environmental change through functional compensation; diversity of architectural styles and communication methods is thus essential for resilient smart grids.

A. THE POWER GRID TODAY (ENERGY DOMAIN)

The European *power transmission grid* is a synchronous power grid that spans 34 countries and is organized by the European Network of Transmission System Operators for Electricity (ENTSO-E), a network of numerous transmission grid operators (TSO) [9], [10]. The power grid was built using a centralized approach; generation units at the transmission grid level and consumption subsumed within distribution grids, which are located subjacent to high-voltage substations that supply them. Kerber and Witzmann [11] argue that most urban distribution grids are organized in open rings, allowing alternative reconnection routes to circumvent faulted parts. In recent years numerous decentralized renewable energy generators have been installed at the *power distribution* level, following the policies on clean energy such as the German "Energiewende" [12]. These small generators have the potential to push fossil power generation at power transmission level, out of the market, leading to a decrease in rotating masses (generators) in the transmission grid. However, often unpredictable decentralized generation could result in voltage fluctuations. Fossil generation thus serves as an emergency reserve in case renewables fall short. In view of the rising number of decentralized installations, grid operators increasingly require that renewables also take part in grid stability. An environment as dynamic as this demands active control mechanisms, which in turn require communication systems for management [13].

According to Christiner [14], with the paradigm change in the energy sector, intraday energy exchange and utility intervention continue to increase. Today, the power distribution grids operate increasingly at the limits of their capacity due to increasing bidirectional power flows. The possibilities of decentralized generation, controllable loads and power storage provide flexibility for grid operators but also require ICT.

B. COMMUNICATION IN POWER INFRASTRUCTURES (ICT DOMAIN)

ICT is already present in the power transmission grid, which is organized in a centralized hierarchical structure under the control of the TSO. Utilities are usually blind below the MV transformer, that connects the transmission grid to the distribution grid. According to Igure et al. [15] legacy SCADA systems experience an increasing number of attacks, but were developed with a view toward delivering a high level of performance and meeting network constraints, without taking security concerns into account. Furthermore, their research shows that almost 70% of the incidents were *attacks* originating outside the network.

Several reference architectures for smart grids have been proposed so far. SGAM [3] offers a holistic approach that encompasses multiple dimensions ranging from the physical components all the way to the business level. The BSI [5], [6] establishes a protection profile for a smart-meter gateway for network segregation and data handling. NIST [4] outlines a generic model for security strategies and a centralized architecture with meta-level requirements. Ilo [16] divides the power grid into many microgrids with each its own control strategy, in order to minimize the amount of communication. ENISA [17] offers security recommendations, outlines risks, and challenges, and provides a knowledge inventory. SG^2 (Smart Grid Security Guidance) [18] uses a threat and risk analysis to explore the impacts of and countermeasures against attacks. Key results include a threat catalog and proposals for countermeasures and effective encryption and authentication measures. Further, they find that, while embedded security is immature, reducing the attack surface may help prevent attacks. The results were combined into a holistic model that can be extended to future ICT functionalities. Khan et. al. [1] provide a comprehensive survey of applicable technologies, architectures and security considerations with detailed methods described under the references [131], [132], and [193]. Akhtar and Rehmani [19] survey wireless sensor networks and their power supply with regard to renewable resources, storage technologies, and wireless power transfer.

C. WIDE AREA MONITORING SYSTEMS (WAMS)

The North American Synchro-Phasor Initiative (NASPI) [20] and Kanabar et. al. [21] present recent advancements using Phasor Measurement Units (PMUs) as a base technology for monitoring the power grid. The measurements help achieve situational awareness and serve as input for control functions. Most WAMS are organized in hierarchical architectures with a control center. According to Zhang et. al [10], WAMS manage the data exchange among control centers and state estimators, which apply statistical methods to make decisions based on the collected data. As dynamic renewable and

distributed energy sources become more widespread, monitoring functions utilizing WAMS become increasingly important.

D. ADVANCED METERING INFRASTRUCTURE (AMI)

According to Dan and Bo [22], AMI collect data on power consumption and transmit them to the utility company. This approach allows for automated billing and enhanced observability in the power distribution grid. Technologies used to achieve smart metering include power line communication (PLC), dedicated wire, and public mobile carrier or wireless networks. Bou-Harp et. al. [23], Yan et. al. [24] and Khan et. al. [1] list technologies such as Zigbee, WiMAX, Wifi and GSM as possible means of supporting smart metering. As mentioned earlier, the BSI [5], [6] defines security considerations for AMI that use a gateway connecting smart meters, Wide Area Networks (WAN) and home appliances.

III. THREAT MODEL

The European Commission has declared energy and ICT alongside water, food, medical and emergency services, public order, finances and transportation to be *critical infrastructures* [25]. According to the National Critical Infrastructure Protection Strategy (KRITIS) [26] of the German Federal Ministry of the Interior, society is vulnerable to a number of threats, including not only natural events, technical and human error, but also terrorism and war. This study considers resilience in smart grids as a means to reduce the impact of technical failure and natural events. According to NIST [4], future smart grids require security measures on the basis of architectural design, among other means against an array, of typical adversaries for information systems, which according to NIST includes nation states, hackers, terrorists, organized crime, non-organized crime, industrial competitors, and disgruntled or negligent employees.

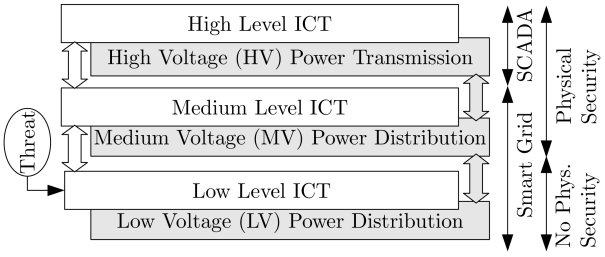

FIGURE 2. Sample threat to smart grid ICT.

Threats such as nation states, organized crime and disgruntled employees will remain even with high security measures in place, as they can infect critical nodes on higher levels of the hierarchy. However, decentralized systems and strict policies may help to prevent incidents arising from such threats. The main entry points are assumed to be located at the lower ICT levels which have no physical security measures in place and are publicly accessible (Fig. 2). If such devices are connected in a mesh network, malware may propagate quickly even to other networks such as water- or gas-grids (Fig. 3). We assume that smart grid communication uses secure protocols for integrity, authentication, and encryption. However, new security vulnerabilities in soft- and hardware arise every day and can be exploited by attackers to compromise systems. Therefore, system architecture should be designed to prevent or slow the spread of attacks.

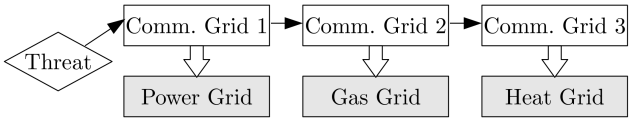

FIGURE 3. Incident propagation.

Future smart grids should deploy ICT on a large scale, mainly on the power distribution level. Figure 2 depicts a threat to low-level ICT. Devices at this level are installed in public places, were physical access cannot be effectively restricted. Such devices can thus be targeted by adversaries with limited skill and resources and should not be considered trustworthy. ICT devices installed at the medium voltage level, which can be locked inside a transformer room, can be considered more secure. Nevertheless, ICT must impede malware propagation by implementing vertical and horizontal security:

- *Vertical security:* Measures against infections of higher layers in the hierarchy (e.g., smart meter to control center)
- *Horizontal security:* Containing the spread of malware between entities on the same level (e.g., meter to meter)

IV. INCIDENT PROPAGATION AND CASCADING EFFECTS

This section discusses incidents that are considered as attack vectors on smart grids when triggered intentionally.

Christiner [14] describes the propagation of a broadcast message from the control system of a gas grid into the power grid SCADA due to a misconfiguration. The message proliferated, as in a denial-of-service attack. The SCADA system was unusable until the broadcast had faded out. During this incident, the grid operators were unable to monitor or control the power transmission grid. However, no blackouts occurred thanks to the manual control of TSO employees. This real world example shows that incidents in one infrastructure can indeed spread to other infrastructures. However, in future smart grids the number of nodes will be much higher rendering manual override much more difficult.

Figure 3 shows an incident propagating across different networks that control otherwise separate grids.

Another example involves a cascade of overloaded power lines, which resulted in the division of the European power transmission grid into three islands each with a different frequency. Enough reserve generation was available to maintain the stability of each island and to resynchronize; however, this example shows that incidents can propagate across an entire continent [27].

Recovering from incidents poses another problem. Since few black-start-capable power stations are available, ENTSO-E [30] has developed extensive restoration guidelines for the power grid. When rebuilding a collapsed power grid, its components must first be re-energized and non-self-sufficient power plants can only be connected after a stable grid is operational. Bruno et. al. [31] explains the lengthy process of restarting a collapsed power grid. Klick et. al. [28] present further research on vulnerable industrial controllers. According to Burke and Fahey [29], cyber attacks on power grid controls already occur more frequently today, unbeknownst to the public.

V. FUTURE APPROACHES IN THE ENERGY DOMAIN

One option open to future power grids is to upgrade open rings to microgrids that balance and trade energy with neighbors under ICT management. In a decentralized future, many distribution grids would remain connected to the transmission grid but should be able to run autonomously in case of a blackout. In line with the suggestions of Ilo [16], microgrids would be able to balance consumption and generation within their boundaries. Additional demand would be communicated to neighbors and the TSOs. During times of insufficient local generation, power would be requested from alternative sources. Otherwise, consumers would have to be dropped in favor of grid stability, priority being given to critical consumers such as water supply or public authorities. In case of a Europe-wide blackout, many microgrids could run autonomously for a period, helping restore a stable power grid. Decentralized generation might actually expedite restoration in this case. However, because regulations render urban areas intrinsically incapable of sufficient generation, and consumption density is higher compared to rural areas, wide ranging blackouts would be expected should the transmission grid fail. Still, water supply and emergency services could be covered with a small amount of generation and support recovery when reconnected.

In contrast to the historically centralized power grid, a fully decentralized approach would have no generation at the power transmission level, which would be used exclusively for balancing. The APG report [14] shows that some legacy power plants must remain in service in order to maintain a minimum amount of rotating masses. This means that decentralized power generation must increasingly participate in grid stability. According to Farhangi [32], the future power system is likely to settle somewhere between a fully centralized and a fully decentralized system such that distributed sources cover most generation with a small base load covered by bulk generation.

VI. FUTURE APPROACHES IN THE ICT DOMAIN

The following sections discuss possible ICT topologies based on the reference architectures in Section II-B. Fig. 4 and Table 1 present a comparison of the ICT topologies according to power grid hierarchy type. They will be explained in detail in the following sections. The centralized, cell and mesh

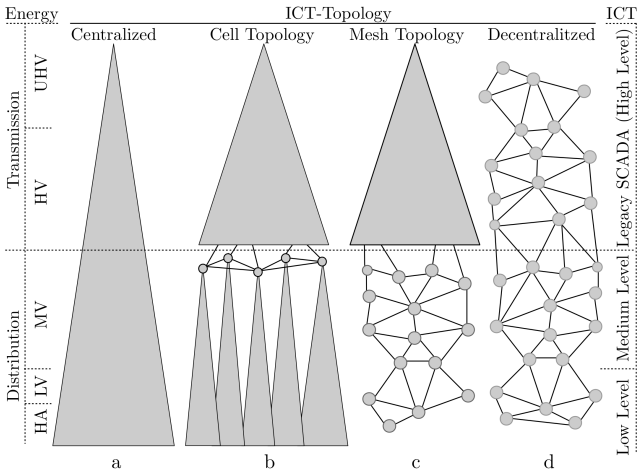

FIGURE 4. Comparison of topologies.

TABLE 1. Control mode comparison at all hierarchy levels.

	Power Grid Hierarchy Level			
	HV	MV	LV	HA
	ICT Hierarchy Level			
Control mode	High	Medium	Low	
a. Centralized	central	central	central	central
b. Cell Topology	central	mesh	central	central
c. Mesh Topology	central	mesh	mesh	mesh
d. Decentralized	mesh	mesh	mesh	mesh

topologies (Fig. 4-a, b, c) differ at the power distribution level. All topologies assume that legacy SCADA systems remain in service at the power transmission level except for the fully decentralized approach (Fig. 4-d), which requires an upgrading of the legacy approach to mesh capability.

Silva [33] concludes that centralized star topologies over distributed mesh networks are beneficial as regards coverage, capacity, reliability and cost. However, mesh networks transfer data hop-by-hop, which entails redundant paths resulting in increased protocol overhead and latencies. While star topologies are best for scenarios without security threats, mesh-based resilience becomes a valuable feature if ICT systems are threatened with failure due to misconfiguration or attacks. Khan et. al. [1] provide a survey of technologies for smart metering that can be used for smart grid communications, including Power Line Communication (PLC), dedicated wires, public mobile carriers or wireless networks. Cognitive radio in particular can be optimized through the utilization of many spectra [1].

Six indicators are used to compare the topologies in the following sections:

- *Resource Control:* How well is the topology suited to achieve situational awareness of the processes in the power grid? How effective is it in managing data, self organization and optimizing resources?
- *Security:* How well is the topology suited to prevent attacks and malware propagation inside networks and across neighboring networks?

- *Resilience:* How well is the topology suited to mitigate failures of or attacks on ICT components?
- *Quality of Service:* How does the topology influence communication quality in terms of protocol overhead and latency?
- *Compatibility:* How well is a topology suited to interface with legacy systems? Will an upgrade be necessary?
- *Cost:* What are the estimated financial (qualitative) implications for upgrading different topology styles?

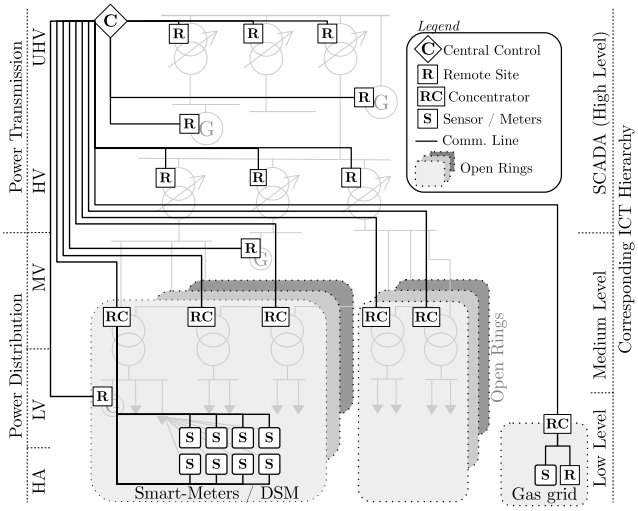

FIGURE 5. Smart grid with a centralized topology.

A. CENTRALIZED TOPOLOGIES

Fully centralized architectures (Fig. 4-a and 5) concentrate and collect all data in a single control center. There may also be middle boxes that only collect and distribute data without deciding on actions. When decisions are made in the control center, all commands are propagated downwards across all levels allowing for situational awareness and the optimization of resources. However, as shown by ENISA [17], Kammerstetter et. al. [34], Kupzog [35], Shin et. al. [36] and Van de Vyver et. al. [37], a centralized topology causes unacceptable latencies in data transmission, low flexibility, low resilience, and congestion situations, and has a single point of failure. For the remaining figures electrical parts are illustrated in gray and ICT in black.

Although redundant structures can mitigate errors in a single control center, planned attacks are not easily overcome by a backup system. *Architecture-based security* must be considered in the design, construction and deployment, rather than being retrofitted. A vulnerability at such a high level can lead to catastrophic failures. Yet a fully centralized architecture can provide some level of protection against malware. In central topologies, malware cannot spread horizontally, as nodes are connected only to higher levels. An attack may propagate vertically, but higher layers are usually better protected (e.g. through firewalls or virtual networks and physically secured buildings). Furthermore, the heterogeneity of components on different levels of the hierarchy may foster resilience. Worth mentioning in this context is the potential threat resulting from the reuse of hardware, software, and design in various products from a single vendor. Primarily aimed at cost reduction, identical software or hardware at different levels of the hierarchy can allow for malware propagation across hierarchy levels.

Centralized ICT is practicable in some nodes within the power transmission grid. However, the nodes to be managed multiply when households with smart devices and distributed generation are taken into consideration. It would not be feasible to control these via the legacy approach. The central control node would thus become even more critical than it is today, and the cost of managing a power grid would be concentrated at the higher ICT levels, which could be less costly than it would be to protect many nodes in a distributed network.

In summary, the *benefits* of centralized topologies are:

- *Resource Control:* Central data collection and control allow overall situational awareness that can be used toward resource optimization.
- *Security:* Physical access is controllable at the medium ICT layer, and direct horizontal propagation is impossible because of the hierarchical structure.
- *Compatibility:* Legacy SCADA can be integrated directly.
- *Cost:* Higher layers with a smaller overall number of devices require expensive upgrades, while lower layers can function without local intelligence.

The *drawbacks* of centralized topologies are:

- *Resilience:* Low level systems depend on expensive high level systems. Redundancy increases resilience against failure but not necessarily against attacks.
- *QoS:* Excessive communication demands and long distances cause latency between nodes.
- *Security:* Malware may spread vertically undetected because there is no local control unit for analysis on the lower level. However, central control is usually better protected than are distributed units.

B. CELL TOPOLOGY

This section discusses a topology with designated cells in the ICT domain that match the electrical microgrid (Figures 4-b and 6). These cells are controlled by a decentralized agent called a cell controller as in the proposal from Kupzog [35] but with additional competences for security and resilience. This cell controller is located above the MV transformer, acting as a master node, data hub and center for local intelligence, providing additional security functions.

The transmission grid remains under the control of the legacy SCADA system, which connects to the cell controller via dedicated uplinks. These uplinks provide information to SCADA systems in the interest of achieving situational awareness, but cannot be used to send control signals in either direction. Each cell acts autonomously, independent of SCADA control, and may also exchange information with

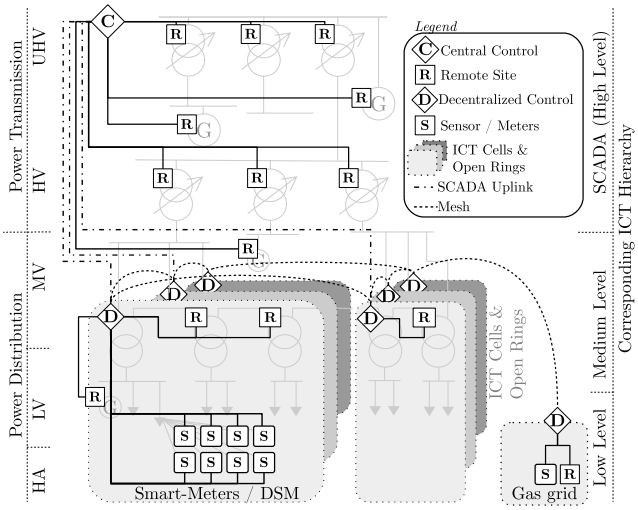

FIGURE 6. Smart grid in cell topology.

its neighbors on the same hierarchy level. Thus, SCADA manages the power transmission grid, while decentralized cell controllers manage their subjacent local grids. Each cell consists of several MV transformers that are clustered under and controlled by one cell controller. The slave nodes collect and concentrate data for delivery to the cell controller. Smart metering and other services such as demand side management are controlled by the cell controller, which can act as a virtual power plant. For security reasons services should not circumvent the cell controller, as they converge data from lower levels and aggregate it for SCADA, other WAN entities and neighboring cells.

The cell controller's functions resemble those of the BSI gateways specified in [5]. These act as firewalls, segregate networks, and prevent communication among smart meters. They are usually located inside locked buildings and thus are physically more secure than are smart meters. Local control and containment makes the spreading of malware to higher layers or to other grids unlikely. As physical security is difficult to accomplish for low-level ICT devices such as smart meters, certain threats persist meaning that medium level ICT such as cell controllers have to deal with compromised nodes.

Customer data or control signals are sent to recipients external to the cell controller only in aggregated form. Cell controllers establish a mesh network with other cell controllers in order to add resilience in case of a high level failure. Because they represent intermediate local control entities, cell controllers must be well protected against malware infections. Anomaly detection should be employed locally so that the cell controller can preventatively warn neighbor cells and restrict communication. Only necessary data should be communicated to other cells or SCADA systems. Communication via the Internet should only take place through the cell controller. Measurement inputs are divided into *critical values* for stability such as voltage (3 phase), current (3 phase and direction), frequency and phase angle, and *non-critical values* for market signals concerning demand-side management: ΔP, ΔQ, smart meter data, etc. Critical values have priority for grid stability. As in the traffic light concept in [38], certain data is prioritized.

Shin *et al.* [36] argue that the most cost-effective approach to implementing smart grids is to utilize middleware in commercial communication infrastructures (e.g. GSM networks or Internet cable). However, running control commands over shared networks opens the smart grid up to new attack vectors. We argue that security concerns require that higher-level communication (e.g. with SCADA or between cell controllers) should use dedicated networks. Shared networks may be used on the lower levels where physical security is impossible to achieve. Cell controllers must be able to provide security functions such as anomaly detection or firewall functionality, which represent the greatest cost factor in this topology type.

In summary, the *benefits* of the cell topology are:

- *Resource Control:* Situational awareness can be established and resources optimized more easily than in fully decentralized or meshed environments due to the cell's hierarchical structure.
- *Security:* Physically secured cell controllers can control malware propagation. Restricting communications among cells and to SCADA systems provides additional security.
- *QoS:* Local cell control minimizes data exchange and solves congestion issues.
- *Resilience:* Cells are resilient to failures on high levels. Meshing cell controllers adds resilience, where the failure of one node does not endanger other cells.
- *Compatibility:* SCADA can be integrated into cells.

The *drawbacks* of cells are:

- *Resource Control:* It is more difficult to establish situational awareness and optimize resources than in fully centralized environments. If the electrical topology changes due to faults, the renegotiation of ICT control is more complex because many cells are involved.
- *Cost:* The highest costs occur at the cell controller level, which have to operate as autonomous entities with numerous functions. Higher layers need not implement extensive security as in Section VI-A.

C. MESH TOPOLOGY

The mesh topology (Fig. 4-c and 7) differs from the cell topology in that all devices are meshed into a dynamic cluster at the distribution level that may form links across different types of grids (e.g. electricity, water or gas). Cell controllers are located on top of MV-transformers and organize local control as explained in Section VI-B.

In this topology the legacy SCADA system controlling the power transmission grid remains unchanged, and communication at the power distribution level occurs via a mesh network with local control units. These decentralized control units are under the control of the DSO and provide communication uplinks to higher levels. Meshed devices can form

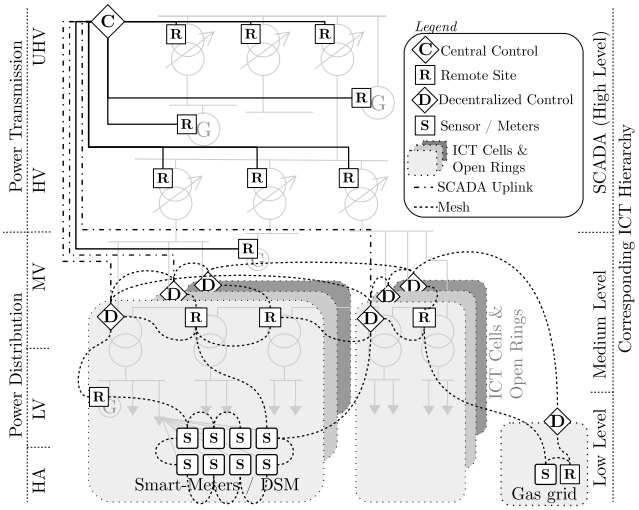

FIGURE 7. Smart grid in mesh topology.

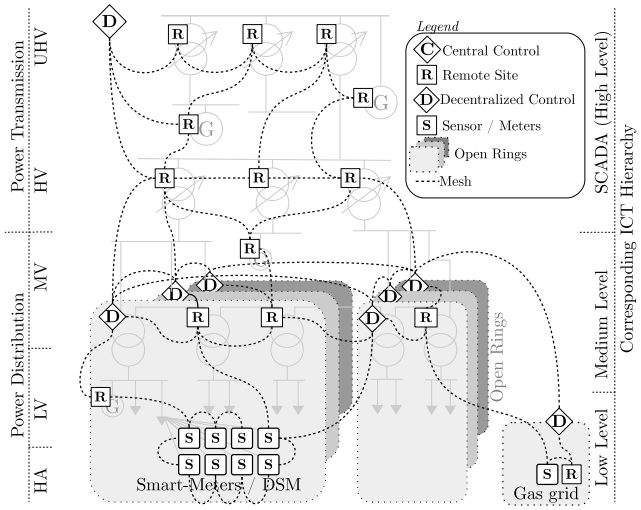

FIGURE 8. Smart grid with a decentralized topology.

a mesh network outside their electrical grid, circumventing the control of the DSO. As put forward by Christiner [14] and mentioned in Section IV, broadcast messages can propagate across vast distances and cause problems for other grid providers. A future smart grid must be able to mitigate misconfiguration, as such incidents pose a realistic threat in attack scenarios.

Mesh structures are inherently more resilient to failure than are centralized structures but harbor the risk that malware could propagate quickly across different networks. Devices could be restricted to a geographical location on protocol level, but this would diminish the network's resilience. Further, Targon [39] argues that mesh networks are less costly to implement than standard centralized topologies only under certain conditions. Because every mesh node requires its own security system, it can be assumed, in accordance with ENISA [17], that mesh networks are generally more expensive than centralized topologies.

In summary the *benefits* of mesh topologies are:

- *Resilience:* The effects of electrical failures or attacks on specific nodes can be mitigated by using alternative nodes and communication links.
- *QoS:* The high number of available communication links reduces the probability of congestion, while limiting the propagation scope reduces latencies.

The *drawbacks* of mesh topologies are:

- *Resource Control:* It is more difficult to establish situational awareness and optimize resources because of the dispersion of the collection process. Furthermore, the logical topology may differ from the electrical topology, causing problems for control functions.
- *Security:* The high number of communication links supports malware propagation and its spread to other infrastructure grids. Data is sent hop-by-hop through other nodes that may not be trustworthy.
- *QoS:* Mesh networks can overcome local bottlenecks through load balancing. Routing decisions and multi-hop routing can lead to additional overhead . Some routing protocols may influence latency.
- *Compatibility:* Legacy SCADA cannot easily be integrated via uplink into local nodes.
- *Cost:* The highest costs occur at the decentralized controller level, but security has to be implemented across all nodes in the mesh.

D. DECENTRALIZED TOPOLOGIES

A fully decentralized architecture (Fig. 4-d and 8) leads to higher resilience and reduced data congestion thanks to alternative paths, but is more vulnerable to malware propagation, which may spread faster and even infect systems outside the power grid where similar hardware or software is in use. As mentioned in Section VI-C, Targon [39] and ENISA [17] argue that mesh networks are often more expensive in terms of capital expenditure, especially taking into account the cost of security functions for every node.

In summary, the *benefits* of decentralized topologies are:

- *Resilience:* Local intelligence mitigates the effects of high level failure and is robust against local failures and attacks.
- *QoS:* Local data management minimizes latencies. Local control minimizes data exchange, and alternative paths prevent congestion.

The *drawbacks* of decentralized topologies are:

- *Resource Control:* Situational awareness and resource optimization are difficult to achieve, since data is collected locally and must be exchanged with other nodes.
- *Security:* High connectivity between nodes and identical hard- and software facilitate the spread of malware through similar vulnerabilities.
- *Compatibility:* Extensive retrofitting becomes necessary if mesh is implemented on the higher layers.
- *Cost:* Economically unviable costs accumulate at the high levels of ICT, which must be upgraded to a mesh network.

TABLE 2. Mapping of topologies to reference architectures.

Topologies in figure 4	SGAM [3]	BSI [5]	ILO [16]	NIST [4]	ENISA [17]
a. Centralized	yes	yes	no	yes	yes
b. Cell Design	yes	yes	yes	yes	yes
c. Mesh Design	no	no	option	no	yes
d. Decentralized	no	no	no	no	option

VII. COMPARISON SUMMARY

This section provides a qualitative comparison of the ICT topologies described in Section VI. Table 2 shows the applicability of the ICT topologies discussed for the proposed reference architectures described in Section II-B. While centralized and cell topologies can be supported by most models, mesh and decentralized topologies are not compatible with all reference architectures. The ENSIA model seems to be able to support the widest range of topologies. The quality indicators introduced in Section VI are discussed and compared in Table 3.

TABLE 3. Comparison of topologies over all hierarchy levels.

		ICT Hierarchy Level			
		High	Medium	Low Level	
Centralized	Resource Control	high	high	high	high
	Security	strong	strong	strong	strong
	Resilience	low	low	low	low
	Quality of Service	low	low	low	low
	Compatibility	high	high	high	high
	Cost	high	medium	low	low
Cell Topology	Resource Control	high	medium	high	high
	Security	strong	medium	strong	strong
	Resilience	low	high	low	low
	Quality of Service	low	high	low	low
	Compatibility	high	medium	medium	medium
	Cost	low	high	low	low
Mesh Topology	Resource Control	high	medium	low	low
	Security	strong	medium	weak	weak
	Resilience	low	high	high	high
	Quality of Service	low	high	high	high
	Compatibility	high	medium	low	low
	Cost	low	high	medium	medium
Decentralized	Resource Control	medium	medium	low	low
	Security	weak	weak	weak	weak
	Resilience	high	high	high	high
	Quality of Service	high	high	high	high
	Compatibility	low	low	low	low
	Cost	high	medium	medium	medium

The main drawback of fully *centralized topologies* (Section VI-A, Fig. 4-a) is the potential for communication bottlenecks between low-level ICT and high-level SCADA. Furthermore, a central control location is an easy target for attackers, even if redundancies are implemented. However, legacy SCADA systems may persist as they are, considering their low cost.

In the *cell topology* (Section VI-B, Fig. 4-b), cells operate autonomously. A local cell controller manages energy consumption and communication as a master node. Strict policies prevent malware from spreading vertically beyond the cell-controller. Horizontal propagation is contained by limiting communications outside the cell. Each cell is a small hierarchical structure subjacent to the MV transformer (and below the medium ICT level) with its controller as the convergence entity. Many cells are connected via a mesh network at the medium ICT level for added resilience against failures in low- and high-level ICT systems.

The *mesh topology* (Section VI-C, Fig. 4-c) connects all devices at the low and medium ICT level into one mesh network. This approach provides better resilience against equipment failure, but at the cost of decreased containment capabilities. Further, SCADA systems cannot be integrated directly except via dedicated gateways. Those would be similar to the cell controllers, but would not restrict the formation of a mesh network across parts of the electrical grid not directly connected. Even independent grids such as water or gas grids could participate in the mesh network.

TABLE 4. Comparison of quality indicators.

+ Benefit - Drawback	Centralized	Cell Design	Mesh Design	Decentralized
Resource Control:				
Situational awareness for top level decisions	++	+	-	- -
Situational awareness for resource optimization	++	+	-	- -
ICT topology matches electrical topology	+	++	-	-
Topology re-negotiation after failure	++	-	-	-
Complex data collection	-	++	+	-
Security:				
Horizontal security against malware propagation	++	++	- -	- -
Vertical security against malware propagation	+	+	-	- -
Physical security against direct access	+	+	- -	- -
Data security through local data management	+	+	-	-
Resilience:				
Resilience against failure	+	++	++	++
Resilience against attacks	- -	+	+	+
Local intelligence	- -	++	++	++
ICT and electrical cells form microgrids	- -	++	-	-
Complexity of control over nodes	+	-	+	+
Self-organization	-	+	+	++
Quality of Service:				
Low latency	- -	++	++	++
Low congestion	- -	+	++	++
Compatibility:				
SCADA can be integrated into the topology	++	+	-	- -
Cost:				
Low cost upgrade feasible	+	-	-	- -

A fully *decentralized topology* (Section VI-D, Fig. 4-d) has its main drawback in malware containment. Malware may quickly spread to other grids and across hierarchies. Moreover, today's power transmission grids are controlled exclusively by centralized SCADA systems. Upgrading all of these existing systems for mesh network capability is likely not economically viable.

Table 3 provides a summary of the quality indicators in the ICT topologies across all hierarchy levels, providing an estimation of the impact on different levels of the hierarchy. Table 4 compares the quality indicators in detail for the four ICT topologies. It shows the benefits and drawbacks of each topology as discussed in Sections VI-A through VI-D.

VIII. CONCLUSION

This study provides a qualitative evaluation of smart grid ICT topologies for urban environments. It presents benefits

and drawbacks of centralized, decentralized, and two hybrid topologies based on quality indicators including resource control, security, resilience, quality of service, compatibility and cost. Although we find that centralized and decentralized topologies have benefits in some respects, hybrid topologies are found to be able to overcome shortcomings in both cases.

The cell topology provides the most benefits for future smart grids through the placement of sensitive nodes in physically secure locations and the hierarchical structure from the building level to the cell controller. To implement this topology, electrical open rings would have to be upgraded to microgrids with corresponding communication nodes. This allows for situational awareness and control over the substations and their subjacent low-voltage (LV) grids, adding resilience during and after a failure. The mesh network between the local cell controllers yields benefits for congestion management and resilience. However, local security measures and physical security in the cell controllers must account for the containment of malware and spreading.

Finally, utility companies may prefer to purchase key-ready systems in order to decrease costs, but the reuse of hardware and software in these systems may replicate security vulnerabilities across hierarchy levels. Compartmentalization within the ICT architecture can prevent propagation of malware, while penetration testing can help to discover vulnerabilities.

REFERENCES

[1] A. A. Khan, M. H. Rehmani, and M. Reisslein, "Cognitive radio for smart grids: Survey of architectures, spectrum sensing mechanisms, and networking protocols," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 860–898, Oct. 2016.

[2] R. Yu, Y. Zhang, S. Gjessing, C. Yuen, S. Xie, and M. Guizani, "Cognitive radio based hierarchical communications infrastructure for smart grid," *IEEE Netw.*, vol. 25, no. 5, pp. 6–14, Sep./Oct. 2011.

[3] CEN-CENELEC-ETSI Smart Grid Coordination Group, "Smart grid information security—Reference architecture," CEN-CENELEC, Bruxelles, Belgium, Tech. Rep. SG-CG/M490/H, Dec. 2014.

[4] *Guidelines for Smart Grid Cyber Security*, document NISTIR 7628, National Institute of Standards and Technology, Aug. 2010.

[5] Federal Office for Information Security (BSI), "Certification Report BSI-CC-PP-0077-2013: BSI protection profile," Federal Office Inf. Secur., Germany, Tech. Rep. BSI-CC-PP-0077-2013, 2013, p. 28.

[6] Federal Office for Information Security (BSI), "Certification Report BSI-CC-PP-0077-V2-2015: BSI protection profile," Federal Office Inf. Secur., Germany, Tech. Rep. BSI-CC-PP-0077-V2-2015, Jan. 2015, p. 28.

[7] L. Wang, M. Zhang, S. Jajodia, A. Singhal, and M. Albanese, "Modeling network diversity for evaluating the robustness of networks against zero-day attacks," in *Computer Security* (Lecture Notes in Computer Science), vol. 8713, M. Kutyłowski and J. Vaidya, Eds. Switzerland: Springer International Publishing, Sep. 2014, pp. 494–511.

[8] S. Crane, A. Homescu, S. Brunthaler, P. Larsen, and M. Franz, "Thwarting cache side-channel attacks through dynamic software diversity," in *Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, Feb. 2015, pp. 1–14.

[9] (Jul. 2015). *ENTSO-E Member Companies*. [Online]. Available: www.entsoe.eu/about-entso-e/inside-entso-e/member-companies

[10] X.-P. Zhang, C. Rehtanz, X. Bai, Z. Wu, and U. Hager, "Towards European smart grids," in *Proc. IEEE Power Energy Soc. General Meeting*, Jul. 2011, pp. 1–5.

[11] G. Kerber and R. Witzmann, "Statistische Analyse von NS-Verteilungsnetzen und Modellierung von Referenznetzen," *ew Fachthema Netze*, vol. 6, pp. 22–26, 2008.

[12] Heinrich Böll Foundation. (Aug. 2015). *Energy Transition: The German Energiewende*. [Online]. Available: http://energytransition.de/

[13] B. Droste-Franke, B. Paal, C. Rehtanz, D. U. Sauer, J.-P. Schneider, and M. Schreurs, *Balancing Renewable Electricity: Energy Storage, Demand Side Management, and Network Extension From an Interdisciplinary Perspective*, vol. 40. Germany: Springer, Jan. 2012.

[14] G. Christiner, "Die Rolle der APG für die Stromversorgungssicherheit—Nationale und internationale Herausforderungen," E-Control, Austria, Tech. Rep. 20903, May 2013, p. 13.

[15] V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in SCADA networks," *Comput. Secur.*, vol. 25, no. 7, pp. 498–506, Oct. 2006.

[16] A. Ilo, "The energy supply chain net," *Energy Power Eng.*, vol. 5, no. 5, pp. 384–390, Jun. 2013.

[17] ENISA, "Smart grid security—Recommendations for Europe and member states," European Union Agency Netw. Inf. Secur., European Union, Tech. Rep. 2012-07-01, Jul. 2012, p. 69.

[18] L. Langer and M. Kammerstetter, "SG2—Smart grid security guidance," Austrian Inst. Technol., Seibersdorf, Austria, Tech. Rep. SG2_Poster_SGW2014, Oct. 2014.

[19] F. Akhtar and M. H. Rehmani, "Energy replenishment using renewable and traditional energy resources for sustainable wireless sensor networks: A review," *Renew. Sustain. Energy Rev.*, vol. 45, pp. 769–784, May 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1364032115001094

[20] North American Synchro Phasor Initiative. (Mar. 2015). *NASPI Homepage*. [Online]. Available: https://www.naspi.org/

[21] M. Kanabar, M. G. Adamiak, and J. Rodrigues, "Optimizing wide area measurement system architectures with advancements in phasor data concentrators (PDCs)," in *Proc. IEEE Power Energy Soc. General Meeting (PES)*, Jul. 2013, pp. 1–5.

[22] L. Dan and H. Bo, "Advanced metering standard infrastructure for smart grid," in *Proc. China Int. Conf. Electricity Distrib. (CICED)*, Sep. 2012, pp. 1–4.

[23] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, "Communication security for smart grid distribution networks," *IEEE Commun. Mag.*, vol. 51, no. 1, pp. 42–49, Jan. 2013.

[24] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 5–20, Feb. 2013.

[25] European Commission, "Green paper on a European programme for critical infrastructure protection," Commiss. Eur. Communities, European Union, Tech. Rep. COM(2005) 576 final, Nov. 2005, p. 26.

[26] Federal Ministry of the Interior, "National strategy for critical infrastructure protection (cip strategy)," Federal Ministry Interior, Germany, Tech. Rep. 34423, Jul. 2009, p. 18.

[27] Union for the Co-Ordination of Transmission of Electricity, "Final report on system disturbance on 4 November 2006," UTCE, Belgium, Tech. Rep. 20070130, Nov. 2006, p. 85.

[28] J. Klick, S. Lau, D. Marzin, J.-O. Malchow, and V. Roth, "Internet-facing PLCs as a network backdoor," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Sep. 2015, pp. 524–532.

[29] G. Burke and J. Fahey. (Dec. 2015). *AP Investigation: US Power Grid Vulnerable to Foreign Hacks*. [Online]. Available: http://bigstory.ap.org/article/c8d531ec05e0403a90e9d3ec0b8f83c2/ap-investigation-us-power-grid-vulnerable-foreign-hacks

[30] ENTSO-E, "Network code on emergency and restoration (ER): Emergency Restoration," Eur. Netw. Transmiss. Syst. Oper., Belgium, Tech. Rep. 150325_ENTSO-E_NC ER, May 2015, p. 42.

[31] C. Bruno, L. Guidi, A. Lorite-Espejo, and D. Pestonesi, "Assessing a potential cyberattack on the Italian electric system," *IEEE Security Privacy*, vol. 13, no. 5, pp. 42–51, Sep./Oct. 2015.

[32] H. Farhangi, "The path of the smart grid," *IEEE Power Energy Mag.*, vol. 8, no. 1, pp. 18–28, Jan./Feb. 2010.

[33] J. Silva, "Understanding wireless topologies for smart grid applications," in *Implementing Interoperability: Advancing Smart Grid Standards, Architecture and Community*, vol. 5. USA: Grid-Interop Forum, Dec. 2011, p. 70.

[34] M. Kammerstetter, L. Langer, F. Skopik, and W. Kastner, "Architecture-driven smart grid security management," in *Proc. 2nd ACM Workshop Inf. Hiding Multimedia Secur. (IH&MMSec)*, Jun. 2014, pp. 153–158.

[35] F. Kupzog, "self-controlled exploitation of energy cost saving potentials by implementing distributed demand side management," in *Proc. IEEE Int. Conf. Ind. Inform.*, Aug. 2006, pp. 375–380.
[36] D.-H. Shin, S. He, and J. Zhang, "Robust and cost-effective architecture design for smart grid communications: A multi-stage middleware deployment approach," in *Proc. IEEE INFOCOM*, Apr./May 2014, pp. 2822–2830.
[37] J. Van de Vyver, G. Deconinck, and R. Belmans, "The need for a distributed algorithm for control of the electrical power infrastructure," in *Proc. IEEE Int. Symp. Comput. Intell. Meas. Syst. Appl. (CIMSA)*, Jul. 2003, pp. 211–215.
[38] BDEW, German Association of Energy and Water Industries, "Smart grids traffic light concept," BDEW, German Associat. Energy Water Ind., Germany, Tech. Rep., Mar. 2014, p. 14
[39] V. Targon, "A cost analysis of wireless mesh networks," in *Proc. 12th Int. Symp. Modeling Optim. Mobile, Ad Hoc, Wireless Netw. (WiOpt)*, May 2014, pp. 349–356.

PETER EDER-NEUHAUSER received the MSc degree in energy engineering from the University of Applied Sciences Technikum Wien. He is currently pursuing the Ph.D. degree within the interdisciplinary URBEM PhD-kolleg with the Technische Universität Wien (TU Wien). He is working on smart grid security with a focus on system resilience and malware containment in smart grid ICT.

TANJA ZSEBY received the Dipl.-Ing. degree in electrical engineering and the Dr.Ing. degree from the Technical University of Berlin, Germany. She was a Scientist and the Head of the Network Research Group with the Fraunhofer Institute for Open Communication Systems, Berlin, and a Visiting Scientist with the University of California at San Diego. She is a Professor of Communication Networks with the TU Wien.

JOACHIM FABINI received the Dipl.-Ing. degree in computer sciences and the Dr.Techn. degree in electrical engineering from the TU Wien. After five years of research and development with Ericsson Austria, he joined the Institute of Telecommunications, TU Wien, in 2003. He is a Senior Scientist with the Communication Networks Group with research focus on active measurement methodologies.