Communications for the Future Electric Grid: Systems and Implications

Peter Fuhr, Ph.D.[1], Sterling Rooke, Ph.D.[2], Elizabeth Piersall[3]

[1]Distinguished Scientist, Oak Ridge National Laboratory, Oak Ridge, TN 37831 USA
[2]Research Professor, Electrical Engineering & Computer Science Dept., University of Tennessee, Knoxville, Knoxville, TN 37996 USA
[3]Graduate Student, Bredesen Center, University of Tennessee, Knoxville, Knoxville, TN 37996 USA

Abstract – *As the operation of the electric grid continues to become more automated, the associated increase in sensors and systems places increasing demands for fast-response, cybersecure communications. This paper presents a review of advances underway in communications and networking technologies that may be implemented to meet these future electric grid requirements.*

Key Words: *electric grid, automation systems, communications, networking*

1. INTRODUCTION

A forecast of the grid-related communications in the 2040 timeframe is fairly easy because the communications needs expressed in envisioning the operation of the future grid (FG) provide insight. Over the past decade, many studies have identified the need for advancements in and implementation of sensing devices and systems that can lead to significant improvements in grid operational visualization. The associated increase in the measurements' values can then serve as the underpinning for a wave of advanced analytics to decipher and predict grid operations on a temporal and geographical scale not currently available.

Advancements in grid control systems are predicated on the measurement improvements, which rely on a stable, secure, efficient communications fabric upon which the information rides. The following passage, excerpted from The Future of The Electric Grid [1], highlights such needs:

> *New communications infrastructures and architectures will support power system operations in the future. Many methods of data transmittal are used for various communication tasks on the power system today; radio, microwave, power line carrier, and fiber optics are some of the more common media. To accommodate the high bandwidth, latency, and reliability needs of future software applications, fiber optics likely will become more prominent.*

An article in a 2007 issue of *The Economist* entitled, "When Everything Connects" [2] predicted the coming era of machine-to-machine devices that use a hybrid (wired, wireless, optical) communication fabric.

Almost a decade later, industrial wireless standards organizations were establishing a basis for network integration in which a central network management system could control sensors via an Internet Protocol (IP-)–addressable reconfigurable gateway device. Such a common system management scheme, ISA-100, is exemplified in Fig 1.

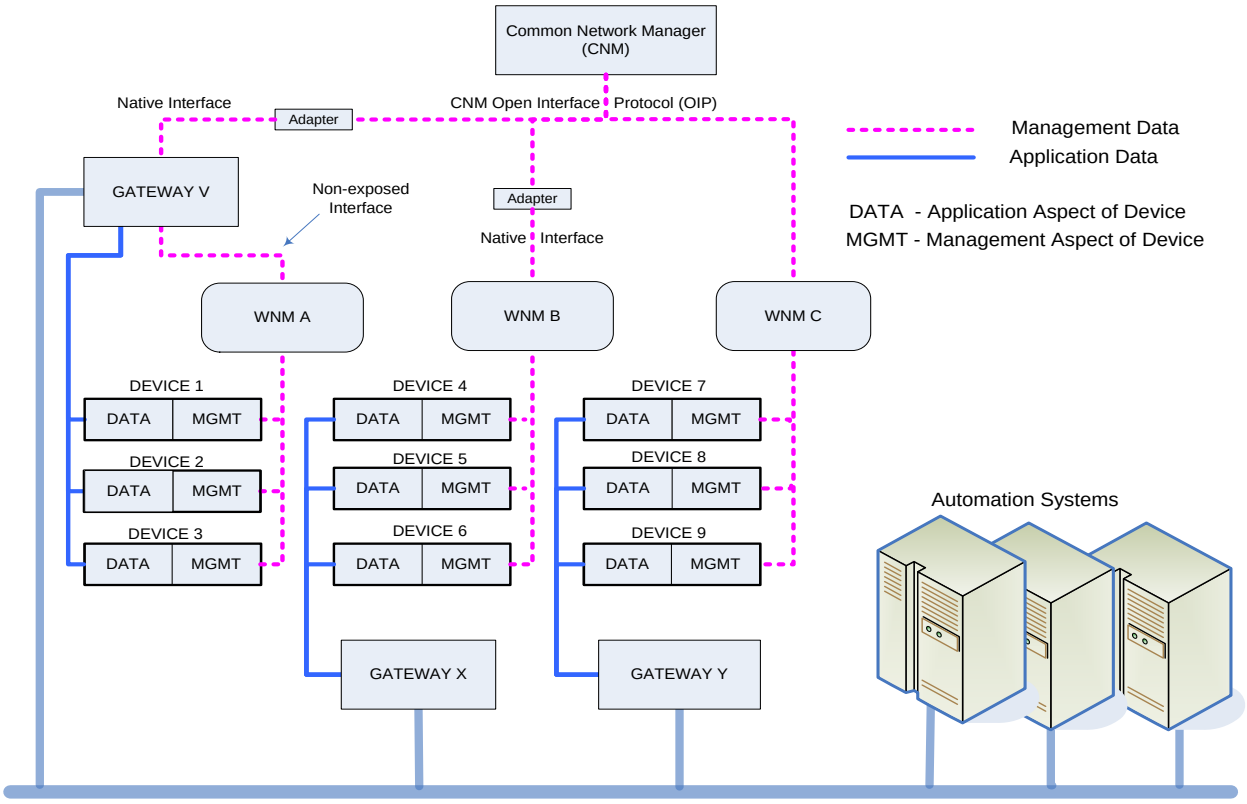

Fig. 1: Network topology supporting a common network management system for industrial and utility settings (Source: Common Network Management Concepts and Terminology Technical Report (International Society of Automation Standard 100.11a [ISA-dTR100.20.1]), June 2015)

2. FIRST BACKWARD, THEN FORWARD

To look forward in FG communications, reviewing previous work is useful—not only in terms of communications four sensors and controls, but also for incorporating the needs for efficient overall utility operation. Nelson-Shira [3] described the advancements presented and discussed at the 18th Annual Critical Communications World event held in Amsterdam, Netherlands, in 2016. At that time, the major advancement in public safety and utility personnel communications systems used at utilities was the migration from Terrestrial Trunked Radio (TETRA) [4] to 4G long-term evolution. The article had a specific point, perhaps aimed at TETRA vendors:

> *A recurring theme [at the conference] was that TETRA is not dead and should be around for at least 10 – 15 years.*

Utility communications have a much broader realm than simply the transport of measurements from advanced sensors to a control system. A 2010 paper describing the envisioned smart-grid communication network design [5] presented a view of the grid elements, components, and applications—along with information transfer requirements—in a sequence of diagrams, presented in Figs. 2 and 3.

Coupled with the network topology and communications requirements are the companion latency requirements for a variety of central smart-grid applications, as shown in Fig. 4.

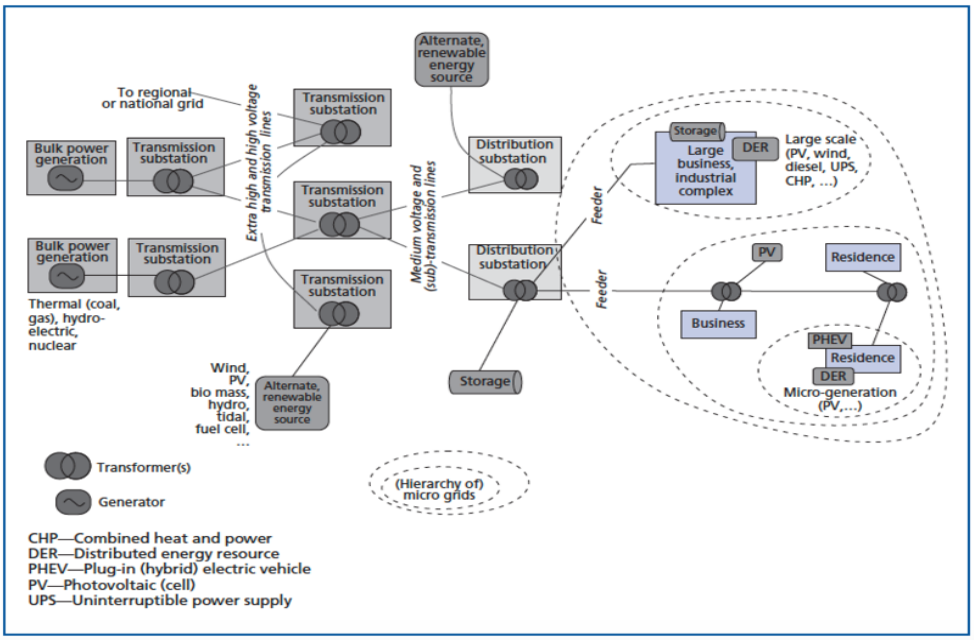

Fig. 2: Generation, transmission, and distribution elements composing the smart grid (circa 2010)[5]

Application	Scope HS or P2P	Data Rate/ Data Volume (at Endpoint)	(One Way) Latency Allowance	Reliability	Security
Smart metering	HS	Low/v. low	High	Medium	High
Inter-site rapid response (e.g., teleprotection)	P2P	High/low	Very low	Very high	Very high
SCADA	P2P, HS	Medium/low	Low	High	High
Operations data	HS	Medium/low	Low	High	High
Distribution automation	HS, P2P	Low/low	Low	High	High
Distributed energy management and control (including ADR, storage, PEV, PHEV)	HS, P2P	Medium/low	Low	High	High
Video surveillance	HS	High/medium	Medium	High	High
Mobile workforce (push-to-X)	HS	Low/low	Low	High	High
Enterprise (corporate) data	HS	Medium/low	Medium	Medium	Medium
Enterprise (corporate) voice	P2P	Low/v. low	Low	High	Medium
Micro grid management (between EMSs)	HS, P2P	High/low	Low	High	High

ADR—Automated demand response
EMS—Energy management system
HS—Hub-spoke
P2P—Peer-to-peer
P(H)EV—Plug-in (hybrid) electric vehicle
SCADA—Supervisory control and data acquisition

Fig. 3: The communications requirements for the logical application elements comprising the smart grid (circa 2010) are presented along with recommended network topologies[5]

Application (only a few example applications considered)	Application setting		Latency allowance (assumed, unverified)	Comments
Teleprotection	All	In the order of decreasing priority ↓	8 ms, 10 ms	For 60 Hz and 50 Hz, respectively
Phase measurement unit	Class A data service		16 ms	60 messages per second stipulated for Class A data service in [14]
Push-to-talk signaling	Incident-related		100 ms	
Smart meter	Connect to many meters in a short time		200 ms	Example: ADR within 1 minute for up to 300 meters connected over a shared medium
SCADA data: poll response			200 ms	See [8].
VoIP bearer			175–200 ms	Includes P2P and all PTT
VoIP signaling			200 ms	Includes non-incident-related PTT
Phase measurement unit	Class C data service		500 ms	Post event (latency value assumed). See [14].
On demand SCADA			1 second	See [8].
Smart meter	Periodic meter reading		≥ 1 second	Say, once an hour or lower frequency of reading

ADR—Automated demand response
P2P—Peer-to-peer
PTT—Push-to-talk
SCADA—Supervisory control and data acquisition
VoIP—Voice over IP

Fig. 4: Smart grid application latency requirements[5]

These figures provide targets for communications operations and performance that are still valid in 2020—10 years after being reported. The authors envision that latency and bandwidth requirements will certainly change to support the FG circa 2040. This statement is supported by a 2016 review of future utility communications needs [6] as shown in the following excerpt:

Utility telecommunications growth will come from increasing geographic coverage of the monitoring networks and speed of response, rather than increasing data rates. Commercial and domestic requirements are moving toward 30 Mbps and possibly 100 Mbps, but many utility requirements can be met with 2.4 kbps per site, which could potentially increase to 10 Mbps. Telecom signal latency and asymmetry requirements in the electricity industry are linked to voltage levels, requiring latencies as low as 6 milliseconds (ms) with associated asymmetry of less than 300 ms if protection systems are to function correctly. These requirements emerge from the need to compare in-cycle values across an electricity network in real time where the duration of a half cycle is 10 ms to maintain stability and identify faults.

Similarly, a 2016 ExxonMobil and Lockheed Industry Day meeting focused on the potential use of aerospace control system design for advanced automation systems such as industrial control systems or large-scale supervisory control and data acquisition (SCADA) and presented a historical view of control systems development. Additionally, as shown in Fig. 5, predictions were made as to the development of open-source control-system applications through 2020. This figure, when combined with the communications system requirements presented in the prior figures, illustrates how the control-system applications dictate the communications performance.

3. WIRELESS COMMUNICATIONS FOR INDUSTRIAL AND UTILITY COMMUNICATIONS

Channel congestion in wireless systems is a continual issue. Novel schemes have been developed that result in collision-free communications even in dense deployments. An example specified in IEEE Standard 802.15.4 enhanced through the industrial wireless specification ISA100.11a is illustrated in Fig. 6, in which channel- and temporal-based hopping sequences are used.

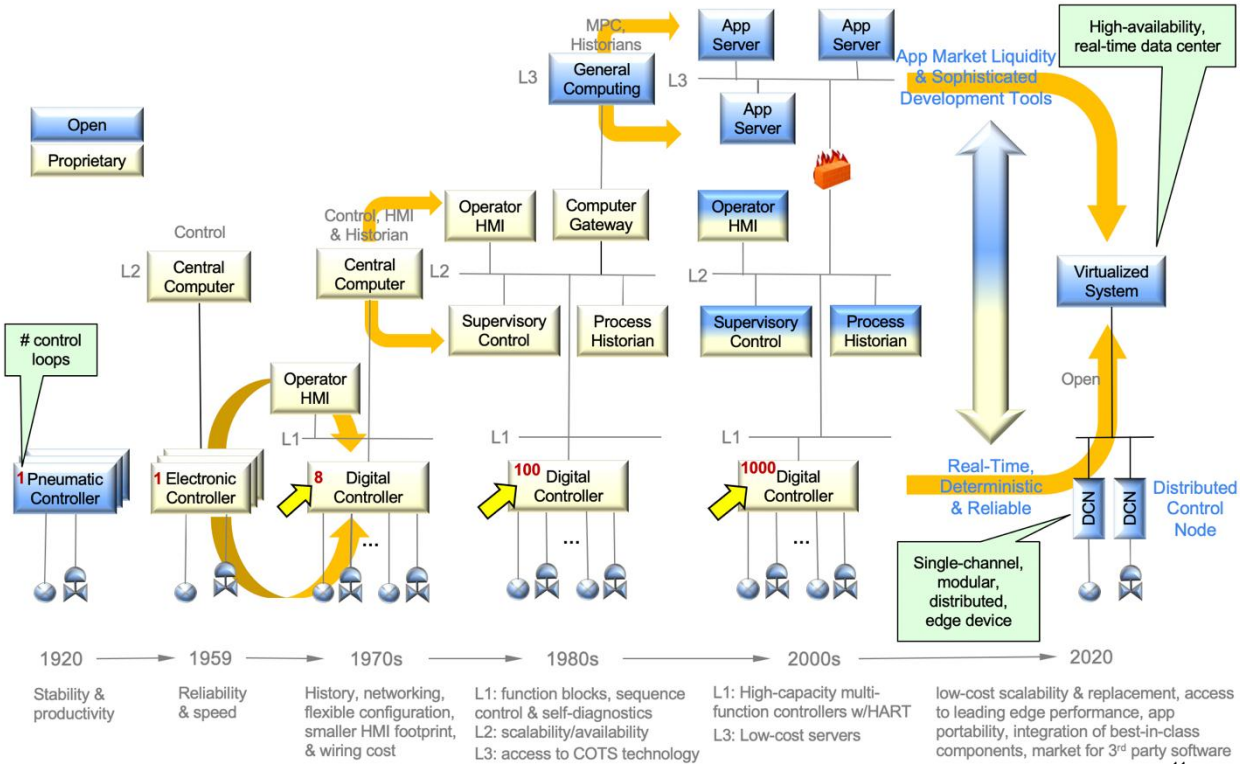

Fig. 5: Timeline of control system advancements in terms of sophistication of operation as well as the increasing role of open-source versus proprietary-system developments (Source: ExxonMobil, 2016)

Spatial diversity of wireless sensors adds a third dimension of freedom to address the possible wireless communications channel congestion, which, when coupled with a scheduling pattern, results in hundreds of devices being essentially collocated. The time-frequency schedule in Fig. 6 is followed by wireless sensors to which the scheduling pattern shown in Fig. 7 is applied, which significantly reduces the cochannel interference (channel congestion) issues.

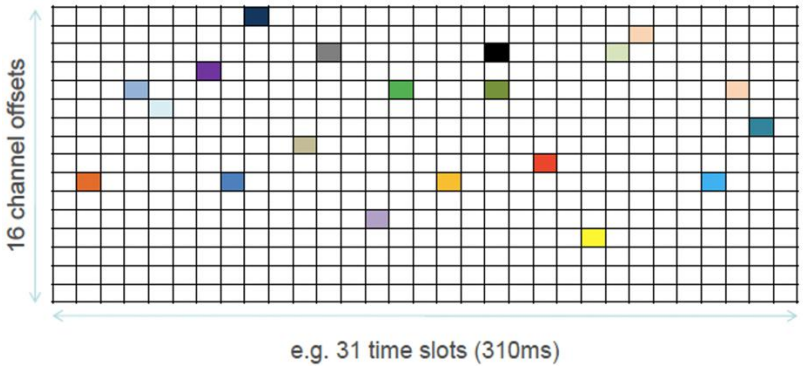

Fig. 6: Collision-free machine-to-machine wireless communications in an industrial setting exercising two degrees of freedom: time and frequency hopping

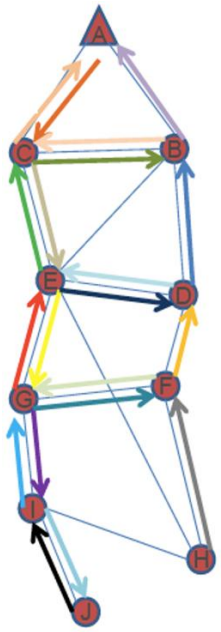

Fig. 7: An operational schedule tailored to mitigate radio frequency/channel congestion of overlapping wireless sensors

The mitigation strategy illustrated in Figs. 6 and 7—enacted through ISA100.11a—suggests advances in network-centric operation with reconfigurable topologies. This technique, a companion of software-defined networking, illustrates how academic research in communications and networking can be adopted by major automation companies, standardized, and then made available to utilities. The increasing presence of Internet-of-Things (IoT)—and its companion, the somewhat more robust Industrial IoT (IIoT)—devices in utility and industrial settings will potentially lead to more performance demands on a utility's communications infrastructure, particularly when the predicted billions of IoT/IIoT devices are deployed.

4. TOPOLOGIES

The Purdue Enterprise Reference Architecture (Purdue Model) was developed more than 20 years ago. With a goal of defining a reference architecture for SCADA/industrial control systems, it became standardized as ANSI/ISA-95. An illustration of ISA-95 in Fig. 8 shows how a company's operational technology (OT) system intersects and interacts with the information technology (IT) design, as well as corporate/enterprise systems. The design, representative of devices, systems, and operations in that time frame, has been modified many times, frequently based on placing firewalls and segmentation boundaries to address various cybersecurity issues that have developed.

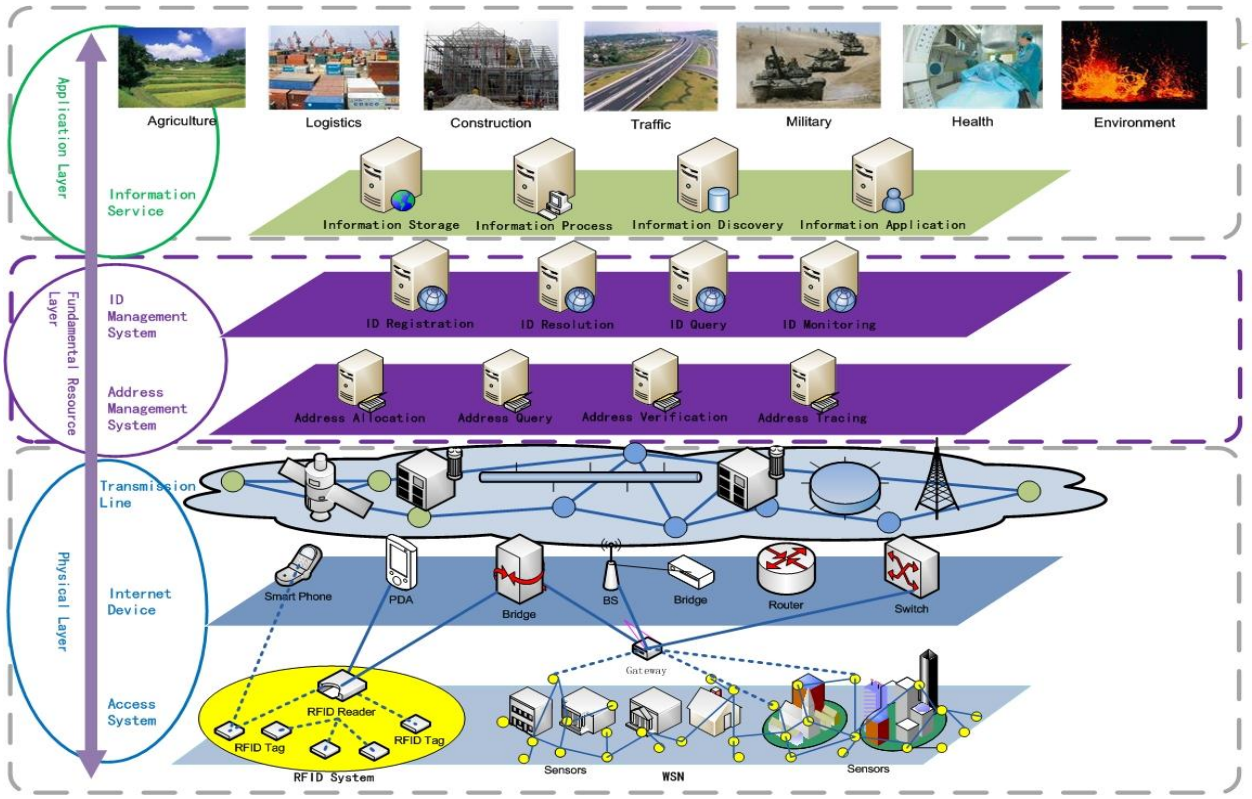

Fig. 8: Layered structure allows for network operation with IoT devices following a model used for application programming interfaces in software system development

5. ENVISIONED ADVANCEMENTS

Although implementations of the ISA-95 model architecture at utilities and industrial complexes abound, the increasing introduction of IP-addressable devices—frequently coupled with wireless access—has led to significant distortions to strictly follow ISA-95 rules. Specifically, an IP-centric architecture leads to a flattening topology in which logical and physical network segmentation is replaced by IT-managed virtual local area networks, thereby sharing infrastructure resources.

Named-data-networking addressing is the next anticipated advancement for circa 2040 communications to have significant implications for automation and the FG. Looking back over the past 20 years, the continued migration from OT networks to IT networks, transporting measurements, commands, and control information in an industrial/utility setting has been predicated on IT support of the overall operations. A major driver for this shift from an OT-centric to IT-centric network and support has been the the Transmission Control Protocol (TCP)/IP stack. Research in and around 2020 presents connectivity to the utility network or the Internet as being easy by having the connected device have an Ethernet driver and hooking up the TCP/IP stack. This has allowed dissimilar network types in remote locations to communicate with each other. As a protocol stack, TCP/IP is efficient at moving data while also being robust and readily scalable. TCP/IP enables any properly configured node to communicate with any other node by using a point-to-point communication channel with IP addresses as identifiers for the source and destination. The network then transports the data bits. Additional flexibility arises from being able to either name the locations to ship the bits to or name the bits themselves. Today's TCP/IP protocol architecture relies on naming the locations.

Unsurprisingly, this design was guided by the communication model used by a circuit-switched telephone network location-centric design. Phone numbers became IP addresses and circuit-switching was replaced by packet-switching with datagram delivery. However, the point-to-point location-based model stayed the same.[1] IP addressing relies on a number of devices (e.g., routers, domain name system servers) and operations for information to flow from one IP address to another. As witnessed through numerous cyberattacks, these routing devices are foundational to the IP-to-IP information transport and, as such, are targets for utility and industrial system operation disruption. Although mitigation strategies such as rotating IP addresses in a pseudo-random manner—the moving target defense—are in initial use, the fundamentals of IP-based messaging remain.

An alternative addressing scheme, named data networking (NDN), is receiving considerable research attention [7]. NDN relies on the use of an identifier or a name instead of an IP address. Therefore, IP address allocation or domain name system services are no longer needed to translate names that are used by applications to addresses or by IP for delivery. From a security standpoint, IP pushes packets to the destination address whereas NDN retrieves data by names. For example, consider a case in which a request for information has been sent using NDN. With NDN, when the user receives the traffic/information back, the first question that arises is, "Has the user asked for this data?" If the user has not asked for the data, then it is unsolicited. This system prevents distributed denial of service attacks because the system simply ignores the incoming data.

6. SUMMARY

The type of synthetic system described may be combined with other communications advances, such as transport using a fiber-optic quantum network. Although this network requires an exchange of devices and systems that support NDN, it provides a means of addressing the seemingly ever-increasing cost and complexity of cybersecurity systems used by utilities and industries. Meanwhile, wireless and IoT/IIoT devices will prevail with worldwide harmonization of spectrum being driven by end users and vendors.

The final point in this prediction of FG communications circa 2040 involves the operations and responsibilities for maintaining the network. A current trend is to have the utility's IT department assume maintainance of the overall communciations network. This maintenance includes inside-the-substation communications—traditionally the realm of OT.

Cybersecurity is causing a change to this situation. Many utilities currently require the IT department to receive "permission" from the cybersecurity technology (CT) department before deploying and reconfiguring system elements (including installing new or replacement sensors and systems). This predicts the FG situation in which OT specifies a device to be installed in, for example, a substation. The request goes to IT for addressing and configurations information and to be incorporated. IT then sends the request to CT for verification of compliance with the utility's cybersecurity rules, meaning that CT will have overall responsibility for an OT device—a significant change from 2020.

[1] There are obvious variants to this point-to-point model, including the User Datagram Protocol over IP.

7. REFERENCES

1. http://energy.mit.edu/research/future-electric-grid/.

2.https://www.economist.com/leaders/2007/04/26/when-everything-connects

3. P. A. Nelson-Shira, "CCW: A Glimpse into the Future of Critical Communications," Radio Resource Intl., Quarter 3, 2016, RRImag.com.

4. Terrestrial Trunked Radio, a European standard for public service communications, https://en.wikipedia.org/wiki/Terrestrial_Trunked_Radio.

5. K. C. Budka, J. G. Deshpande, T. L. Doumi, M. Madden, and T. Mew, "Communication Network Architecture and Design Principles for Smart Grids," Bell Labs Tech. J. 15(2), 2010, pp. 205–228.

6. A. Grilli, "Utilities Quest for Dedicated Spectrum" Radio Resource Intl., Quarter 3, 2016, RRImag.com.

7. https://named-data.net/consortium/.