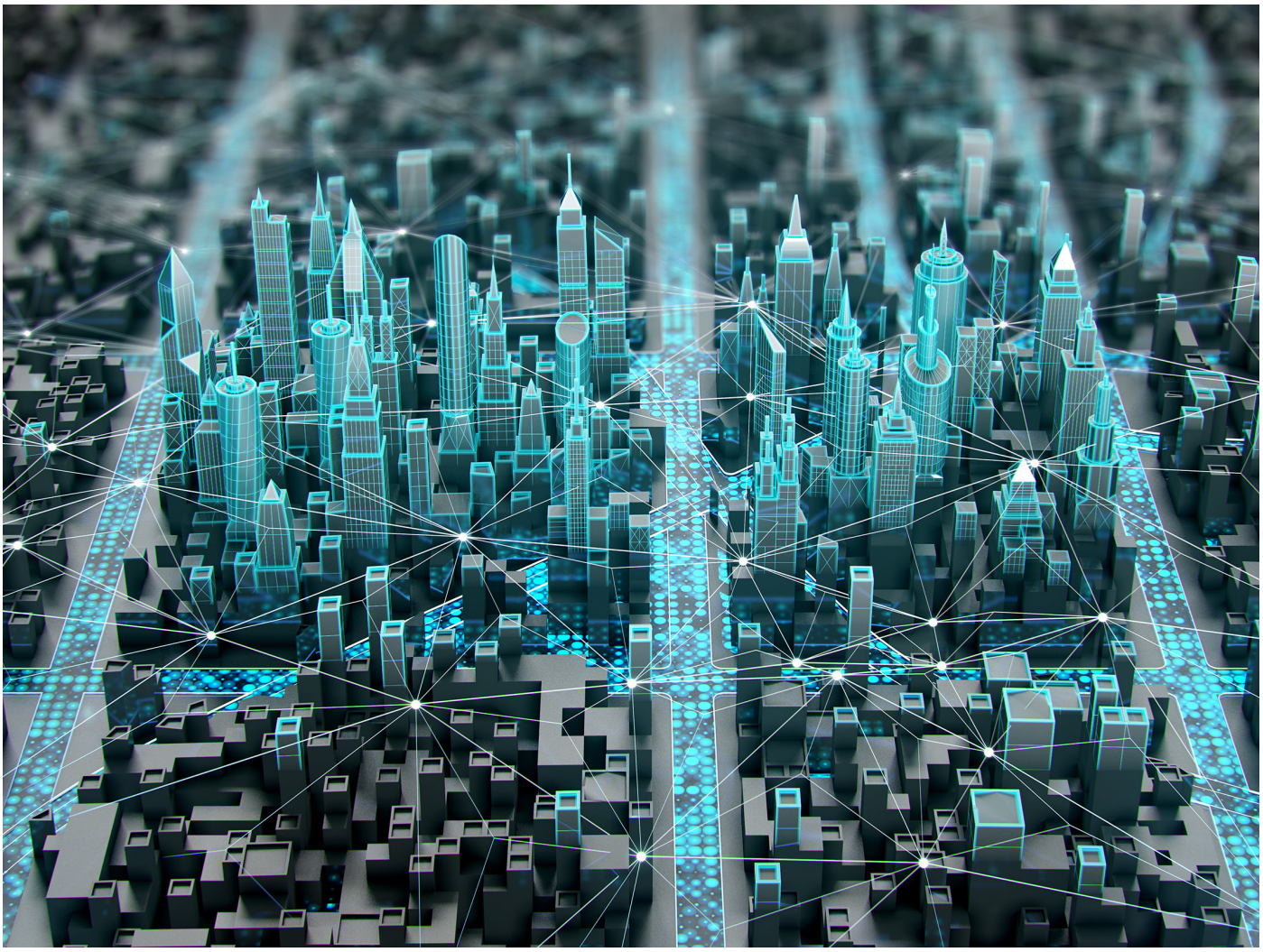
EPRI

5G ARCHITECTURE

Evolution and Roadmap for the Utility Industry



December 2021

Introduction

Utilities and other critical infrastructure industries need secure, high-bandwidth connectivity for reliable and resilient grid operations.

These industries may be unaware of new options in system architecture that can provide more flexibility and reduced costs for their next-generation networks. This white paper will describe these new architecture options and the value they could represent, with a focus on 5G networks.

The call to action is for EPRI and the industry to collaboratively create a roadmap for applying these technologies to serve the industry use cases, address gaps in security and technical capability, and optimize the benefits of the 5G functionality and architecture.

Industry Needs for Private Networks

Utilities are driven to consider construction of private broadband wireless networks in order to better meet reliability and resiliency requirements and to support grid modernization programs. Compared to public networks, private networks can provide benefits in terms of operational visibility, quality of service, coverage area, and upgrade cycle. Beyond the industry needs for ubiquitous, secure, and high-bandwidth connectivity, other drivers are moving the industry towards the adoption of next generation wireless networking standards. The most relevant standards come from two standards development organizations (SDOs). In the case of Wi-Fi, the SDO driving the changes and that certifies conformance to the standards is the Wi-Fi Alliance (WFA). In the case of mobile cellular networks, the SDO is the 3rd Generation Partnership Project (3GPP) (For further information on standards see the *Telecom Standards Guidebook* 3002020378).

Digital transformations often increase data volumes and velocities as required for video streaming to support digital workers or real-time analytics with distributed computing at the grid edge. 5G and NextGen Wireless Local Area Network (WLAN) can support use cases with increased bandwidth needs for increased data volumes and velocities when LTE (a 4G cellular standards) is not enough (see EPRI report 3002022297). Digital worker use cases also require high-bandwidth connectivity for technologies that include augmented reality (AR), virtual reality (VR) and XR? As many carriers charge by data traffic, high bandwidth applications are costly in terms of OpEx and drive utilities to invest in private networks. In the generation realm, the plant cannot operate without access to work management systems on the IT network.

Here are some scenarios impacting different aspects of grid operations.

Broadband Connectivity in the Generation Plant

The goal of nuclear power is to produce safe, reliable, and affordable electricity for its customers. To do so, utilities continuously investigate new ways to optimize efficiency and productivity using modern technologies. Wireless networks are the backbone of in-plant modernization efforts as plants adopt wireless technologies to drive more automated equipment monitoring and support the digital workforce. Up to this point, conventional Wi-Fi technologies (as designated by IEEE 802.11a, b, g, and n) are most common in plants however these networks have proven to be costly with limitations. As an alternative, EPRI has investigated and demonstrated the ability to bring in cellular networks using distributed antenna systems (DAS) (see EPRI report 3002009128). Use of cellular networks for in plant wireless has opened the door to new applications derived from the consumer market. Although there are proven ways to address cyber security concerns through functional isolation (see EPRI report 3002008206) with a direct connection to a carrier, there is still reluctance to fully adopt cellular for in plant applications. It is anticipated that a private 5G network can alleviate some of those concerns.

The primary use cases for nuclear in plant wireless networks predominantly relates to one of two main categories: equipment monitoring and a continuously connected digital worker.

Equipment monitoring may include triaxial vibration, acoustic,

Table of Contents

This white paper was prepared by EPRI.

temperature, pressure, voltage/current, oil quality, and other sensors used to monitor component health. Currently these are offered with Wi-Fi connectivity but can also include Bluetooth or cellular options with or without routers that ultimately push data to company servers. Over the last few years this has also included other wireless protocol options that takes advantage of the unlicensed 900 MHz and 433 MHz frequency bands.

For the digital workers, there are a variety of uses cases and devices available. For example, many utilities have converted to electronic work packages where tablet devices are used instead of paperwork packages to perform field work. Cell phone usage in the plant is also trending up as LAN lines become outdated and replaced. Utilities are beginning to adopt wireless dosimetry for real time monitoring and alerts to ensure workers in radiological environments stay out of harm. And lastly there is a growing interest in augmented and virtual reality applications as a means to provide remote support to field workers troubleshooting equipment. Most devices supporting the digital worker have the ability to communicate via Wi-Fi or cellular.

Fossil and renewable power are in the midst of an energy transition. The generation sector in the United States and across the world has committed to an energy transformation from high carbon-intensive power generation to less carbon-intensive power generation. Most utilities in the United States have publicly announced carbon emission goals for the future. With these goals comes plans for decreased carbon emissions. As gigawatts of carbon-intensive electricity capacity come off of the grid in the coming decades, they will need to be replaced by low carbon resources. Many technologies in the asset mix being considered for replacements are traditional and advanced utility-scale renewable plants. Wind and solar generation tend to be remotely located, unmanned stations that are expected to have additional control and monitoring capability beyond what is available today. As this capability expands and utilities make remotely located renewable technologies a greater portion of their asset mix, they will require robust communication networks. As networks are developed, private or hybrid (private and commercial) 5G will need to be considered. 5G communications can help to facilitate automated plant-to-plant, machine-to-machine, secure remote access, or plant-to-control room communications where it may be difficult to install, maintain, or operate traditional wired networks.

In addition, secure communications will become increasingly important as more automation and remote access requirements are needed. As an energy transformation is occurring, at the same time, a workforce transformation is occurring. Workers from traditional generation assets are learning new skills and taking on new responsibilities in other utility business units. As new unmanned remote assets are built and brought online, there is more of a need to ensure that secure two-way communications exist to facilitate growing needs for remote access into plant control systems. Vendors and integrators are losing talented employees like utilities and will not be able to physically travel to remote sites as easily as they have done in the past. In addition, new digital technologies being installed at plants for monitoring and control will increasingly need to have secure communication pathways to communicate with other digital systems offsite. These help to ensure in-plant process health, grid stability, real-time control and dispatch, and cyber security monitoring and response.

One of the major issues that cyber security defenders are addressing is non-repudiation and identity management. Currently, when personnel need to establish remote access to a site, they must manually authenticate through operators in the control room using multi-factor authentication tokens over the phone. Some utilities have more automated methods, but no additional security measures in place to ensure that the actual person trying to remote into the system is who they say they are. One way of improving identity management and non-repudiation is to implement a zero-trust environment. Zero-trust is the concept of authenticating every device or person on the network to every device or person outside of the network. It in fact, doesn't "trust" any devices until they are specifically authenticated each time. Part of a zero-trust architecture includes segmentation and micro segmentation. 5G technologies may be useful when implementing a zero-trust architecture at a plant. The United States Department of Defense (DoD) recently published their *Zero-Trust Reference Architecture* that can be used by utilities as a guide and starting point to implement a zero-trust environment. The DoD document provides architecture best practices and points to implementation standards for the different infrastructure equipment, devices, and swim lanes. When incorporating 5G as part of an overall zero-trust environment, the DoD references may provide additional insight to ensure its ability to provide additional capability.

Broadband Connectivity in the Field

The field area network (FAN) is an essential layer of many utilities' smart grid communications infrastructure. The FAN concept enables a ubiquitous, high-performance, secure, reliable network providing "last mile" backhaul service for distribution supervisory control and data acquisition (SCADA) and advanced metering infrastructure (AMI) systems. It also enables network access services for advanced distribution management and automation, distributed energy resources, and any future smart grid applications requiring connectivity from within and beyond the distribution substation. A partial list of utility field device use cases includes:

- Distribution Automation
- Underground Network Devices
- T&D Substation SCADA (Serial and Ethernet)
- Transmission Line Switches
- Gas Measurement, Distribution, and Storage
- Water SCADA
- Generation – Hydro Monitoring – Fo and Water Level
- Voltage Monitoring and Adjustment
- Load Curtailment
- Distributed Generation, DER
- FLISR – Teaming Reclosers
- Protection – Mirrored Bits
- Cap Bank Controller
- PMU Data
- AMI Backhaul
- C&I Metering
- Residential Metering
- Firmware Updates

In addition, there exists a growing number of security and situational awareness use cases. Video streaming is bandwidth intensive and avoiding those costs on commercial cellular can represent significant cost savings. Legacy wireless technologies are challenged in dealing with video because of limited bandwidth and often manage the available capacity through QoS policies so that more critical applications are not impacted by video transmissions. The 5G technology does not have bandwidth constraints and accommodates streaming video without requiring any special handling.

The Wireless Network Ecosystem

The wireless network ecosystem can be divided into the following categories: cellular network operators (CNOs) also known as "carriers", infrastructure providers, user equipment (UE) vendors, and system integrators.

Carriers may be nationwide or regional and they own and operate networks. In the US the main carriers are AT&T, Verizon, and T-Mobile. Typically, carriers have a direct business relationship with the majority of the end users. Carriers may also have a wholesale relationship with resellers that package and provide the service retail to end users.

Infrastructure providers manufacture Radio Access Network (RAN) and core network equipment. The RAN mainly consists of radio frequency (RF) base station equipment, which is the network side of the air-link with the UE. Core network equipment are specialized servers and routers that interconnect the individual base station sites of the RAN with each other, as well as provide the interconnection with public internet and telecommunications networks. The core network equipment also provides the carriers with the operations, administration, maintenance, and provisioning (OAM&P) functionalities. Finally, infrastructure providers also produce and maintain the software that enables both RAN and Core components.

UE vendors are the manufacturers and suppliers that produce the handsets, modems, and other terminal equipment that is purchased and employed by the users to connect with the carrier networks.

System integrators work in different industry verticals (such as government, transportation, health care, utilities, and others) to bridge the gap between the standard service offerings of the carriers and develop special solutions tailored to the needs of a particular enterprise.

Business Models of Outsourcing and Sharing

In some cases, commercial cellular carriers will provide in-building network expansion. Examples are airports and stadiums. If there is a business opportunity, the operators will be interested in considering it.

One of the downsides to commercial cellular carriers (in-plant or in the field) is the desire to avoid ongoing operating expense

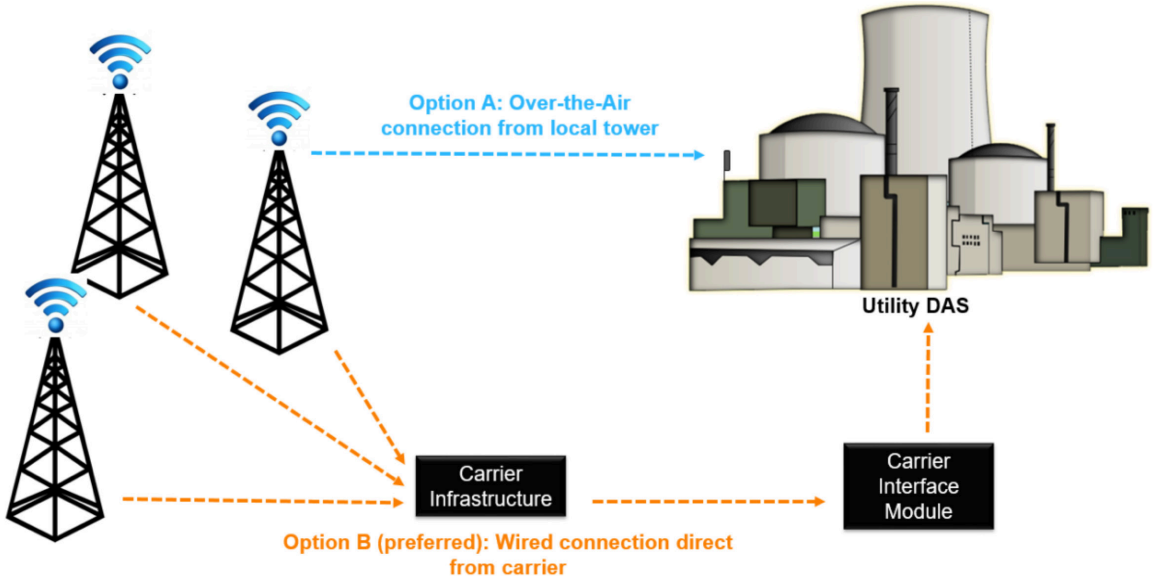
or OpEx charges. Due to regulatory policies based on rate of return on investment, utilities prefer capital expense or CapEx procurements and investments such as in-plant Wi-Fi and Private LTE in the field.

The procurement line is blurred as some private 5G networks may choose to move their core to a cloud service which would involve ongoing costs and may be construed as OpEx line items. However, every component of a private network has a software component which requires ongoing licenses and updates.

In-plant Network Technologies

Power generation facilities are often located in rural areas with minimal coverage and due to the robust nature of these plants, signal propagation thru dense concrete and miles of metallic piping can create RF challenges. It is for this reason that signal propagation in-plant is best accomplished with a Distributed Antenna System (DAS). There are three methods to get signal to the DAS. The simplest, fastest, and most cost-effective method is to use an over the air connection from the nearest cell tower with a donor antenna. This would require a rebroadcast agreement with the carrier which will typically take 3–6 months. Although this connection method makes for a great demonstration of cellular in-plant, in the few cases this has been used by utilities it has created reliability issues due to the increased traffic on a potentially dated rural tower. Also, some sites may be many miles from local towers therefore the signal that is getting rebroadcasted may be weak to begin with. The other two connection options to feed a DAS signal involve creating a direct connection with a cellular carrier. There are two methods to accomplish this connection. One method makes use of a small cell "hub' or aggregation point. This connection would likely have a dedicated fiber connection to the carrier switch and baseband. This connection method is common in stadiums, airports, and other high traffic areas. Some power generation facilities have small cells on site. Those that do not have them would have to talk with the carrier and the carrier would agree if they see value. The other direct connection option installs a full baseband unit and radio unit(s) in the plant. This option requires a dedicated fiber connection between the carrier switch, carrier base band unit, and carrier radio(s). These two connection methods are preferred for utilities and are the most reliable and higher performing options due to higher throughput speeds and higher bandwidth. The downside of these two direct connection methods is they may take years to implement. It is not uncommon for the process of approval and planning with the carrier to take 1–3 years depending on the carrier and the priority of the customer. Therefore, the other options may need to be considered (such as using an over the air connection in the interim) until a direct connection is established.

The emergence of citizens Broadband radio service (CBRS) for in-plant private networks has become a new option for in-plant wireless. The advantage with this configuration is that utilities could benefit from a secure private network and capitalize on the available spectrum in the 3.5 GHz band. However, studies



show that sub gigahertz frequency bands tend to propagate better in-plant therefore from a hardware perspective, there could be little advantage.

Open RAN – Enabling New Options for System Architecture and Integration

The architecture of LTE and 5G is evolving in response to several trends:

1. Desire for improved interoperability within the network
2. Improved modularity of the RAN components
3. Trends toward "softwarization" and cloud computing

The RAN, as noted above, is comprised of the fixed cellular network infrastructure such as base stations and the supporting components. The 3GPP name for a cellular base station is "enhanced Node B" or eNB. Open RAN is the architectural concept of open (meaning documented and standardized as opposed to proprietary) interfaces between the functional elements of an 5G/LTE system. O-RAN is a specific instance of this architecture. It is the name of the Open RAN architecture defined by the O-RAN Alliance, which is a specification group. The O-RAN Alliance was spun out of the Telecom Infrastructure Project initiated by Facebook.

To understand the benefits of Open RAN, consider the "classic" LTE architecture as shown in Figure 1. The Radio Access Network or RAN consists of the towers and cell sites (e Node B) that form the fixed infrastructure. The LTE Core consists of several logical components that are typically located at a data center. The RAN connects to the core by a Wide Area Network often referred to as the Backhaul network. This network can be transported over private fiber, leased fiber, or point to point microwave links. There is a preference for fiber due to the inherent capacity limitations with microwave radio technology.

Motivations for Functional Splits

One architectural enhancement that is widely deployed (independent of Open RAN) is to split the base station (eNB) functionality between separate physical units: The Baseband Unit (BBU) and the Remote Radio Head (RRH), as shown in Figure 2. This split can save cost by replacing a coaxial feedline running up the tower to the antennas with a fiber optic cable and a DC power supply cable. A standard called Common Public Radio Interface or CPRI defines the protocol interconnecting the BBU and the RRH over the fiber. The BBU is sometimes referred to as the Radio Equipment Control (REC) and the RRH is sometimes referred to as the Radio Equipment (RE). A benefit of the split is that the RF signal only travels a short distance from the RRH unit at the top of the tower to the antennas, lowering signal losses. A potential downside is higher costs when tower climbers are needed to service the RRH if it fails.

The BBU consists of computer hardware—typically built around software defined radio (SDR) and a conventional (white-box) computing processor. Split Base Station BBUs were initially designed to control the three antenna sectors of a classic tower site macro-cell installation—3 RRUs connected to one BBU. As computing capability continues to increase, it becomes feasible (and desirable) for a BBU to control more than three radios across multiple RRH units. This leads to the Cloud RAN architecture where RRHs on towers are connected by a wider area fiber network to a higher capacity

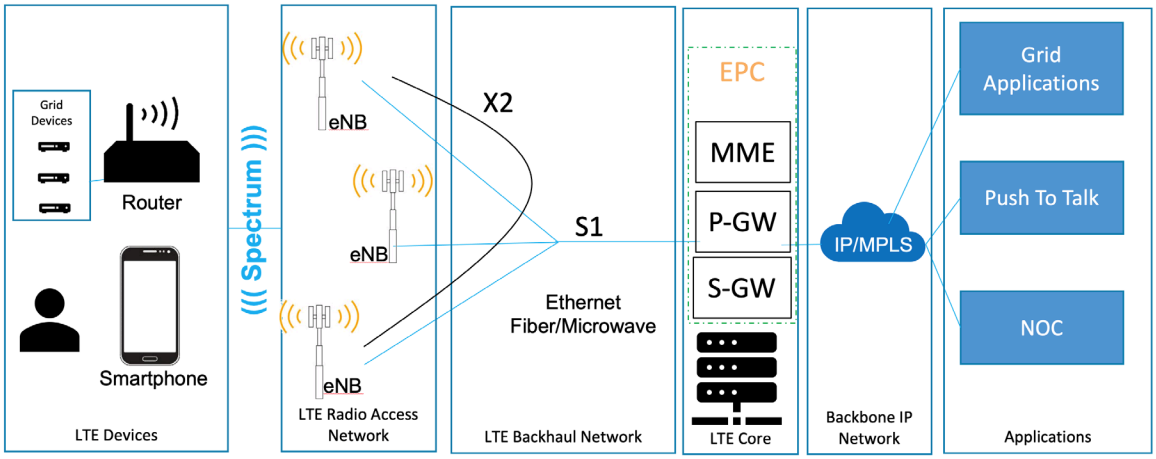


Figure 1. Classic LTE Architecture

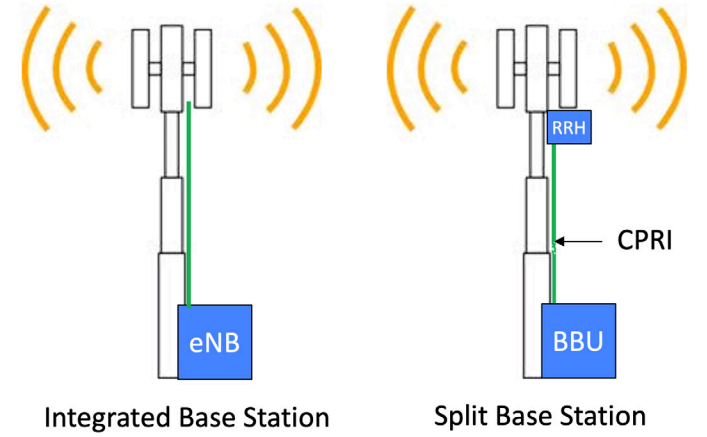


Figure 2. Split LTE Base Station (eNB)

BBU at a centralized location. The fiber optic link connecting the RRHs and the BBUs is called Fronthaul, in contrast to Backhaul, which connects the eNB (whether a single unit, or split RRHs and BBU) to the Core. Due to the tight timing constraints of the split architecture, there are distance limits for Fronthaul due to the propagation speed of light in fiber. Depending on implementation details and vendor choices, the maximum distance of Fronthaul is typically limited to 10s of km. Therefore, a single Cloud RAN BBU instance cannot serve a large city or utility service territory alone.

Open RAN takes the virtualization and segmentation of functionality further within the RAN. Note that the traditional backhaul is already standardized by the 3GPP as the S1 interface, or NG interface in the case of a 5G core, so is not included on the Open RAN.

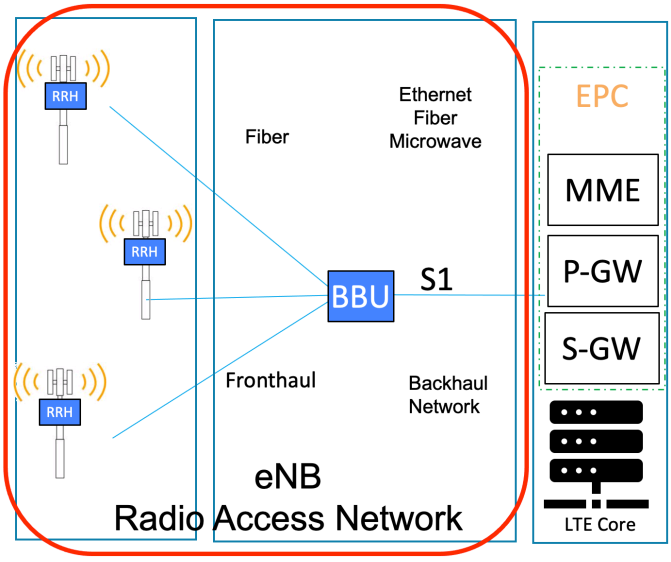


Figure 3. The Radio Access Network (RAN) in the LTE Architecture

5G Functional Splits

The LTE architecture is transformed to the 5G architecture using the 5G nomenclature in Figure 4, highlighting the scope of O-RAN. With the adoption of 5G terminology, as described in the 3GPP disaggregation approach defined in TS 38.801, the BBU is further divided into the Centralized Unit (CU) handling non-real-time functions, and the Distributed Unit (DU) with real-time functionality, and thus a requirement to be closer to the radio hardware. This provides more flexibility in network deployment and allows easier virtualization of the CU functionality on commodity hardware or cloud computing platforms.

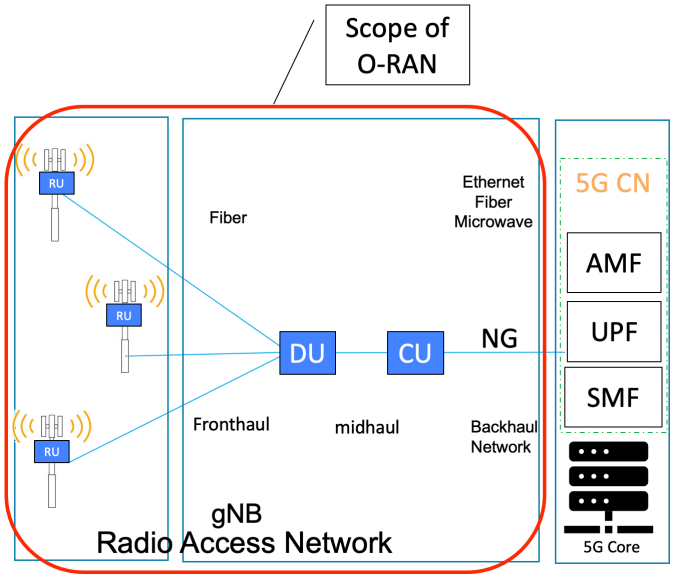


Figure 4. The Radio Access Network (RAN) in the 5G Architecture

5G Terminology for the RAN and 5G Core is:

- 5G CN — 5G Core Network
- AMF — Access and Mobility Function
- UPF — User Plane Function
- SMF — Session Management Function
- CU — Centralized Unit
- DU — Distributed Unit
- RU — Radio Unit

The scope of O-RAN is highlighted because it enables further granularity (splitting of the embedded functions within the RU, DU, and CU defined by the 3GPP). This allows more flexibility to support the wide variety of utility network requirements and use cases. This is especially true of networks containing both 4G and 5G elements. O-RAN defines standard, interoperable interfaces between the RU, DU, and CU. The specifications allow some of the lower layers of functionality to be moved between these functional units as requirements dictate. This allows network designers to balance cost and performance – for example, a lower system cost might be achieved by moving functionality from DU into the CU (using commodity hardware), but it could limit performance. Higher performance can be obtained by pushing functionality to the edge (DU) at the cost of more complex and capable DUs.

Building from a 5G Core (as will be likely for future designs), O-RAN can enable a mixture of deployment options, including LTE. See Figure 5 below. The functionality of an ng-eNB (which provides an LTE air interface while connecting to a 5G core) can be supported from a DU. In some cases (such as small cell), the DU and CU can be combined into a DRU.

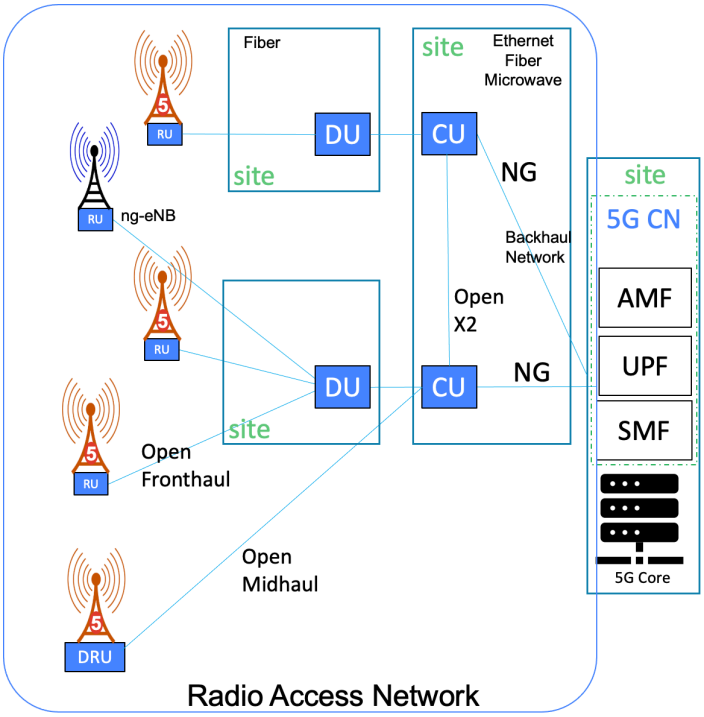


Figure 5. O-RAN Network with 5G Core

Benefits of Open RAN

In conclusion Open RAN (and the O-RAN specification) provide benefits to the utility user on several fronts. First, the opening of previously internal interfaces between network functional blocks enables improved interoperability and implementation choices. A utility deploying a private LTE/5G network is not limited to selecting a single vendor and exclusively using their products. An RU could be sourced from one vendor, a CU from another vendor, and the core could be provided as a cloud service. The second value of O-RAN is the granular selection of functionality provides more options for integrating different types of equipment for different use cases. O-RAN takes the distributed and edge computing definitions from 3GPP and extends it further to allow more flexibility in design and configuration. It also enables the potential for reuse or re-purposing of equipment as network needs change.

The Open RAN architecture enables options where components are virtualized (to save cost). On the other hand, virtualization is not required allowing smaller simpler networks to embrace dedicated hardware. Similarly, Open RAN does not require that the network be decentralized. The advantages of the open interfaces and interoperability can provide benefits with small scale or centralized network configurations.

5G and Cyber Security

The Potential of 5G for Utility OT Cyber Security

Today's cyber security is often "bolted on" rather than "baked in" for utility networks. There are a number of reasons for this status. First, no cyber security standard exists that is akin to an Underwriter Laboratories' global safety certification and product manufacturers may develop products that lack strong authentication and authorization features. Second, there are significant gaps in cyber security awareness on the part of consumers that impact the demand for end-to-end cyber security capabilities in products and services.

Intrinsic cyber security is defined by EPRI as a state where security is fully integrated in the business's mission, processes, technology, and culture. Intrinsic cyber security is embedded in products, processes, and skills, and is the default path for designs, deployments, and operations of simple to complex systems.[1]

1 EPRI's "Preparing for the 2030 Energy System: Why We Need a New Cyber Security Vision" whitepaper describes intrinsic cyber security and its importance to the electricity subsector's roadmap to enhanced cyber security. Product ID 3002020794.

5G platforms have the potential to improve utility OT cyber security postures.

- Virtualization allows for easier distribution of cyber security solutions and can potentially speed response and recovery times as compromised virtual systems may simply need replacement rather than more resource-intensive equipment redeployments.
- 5G platforms, with their increased bandwidth and speeds, create possibilities for utilities to embed distributed on-premises computing and/or cloud computing at grid edges. Edge computing can support a variety of data-intensive utility use cases that leverage AI and prescriptive analytics. Artificial intelligence solutions that handle threat detection can be more effective by performing pre-computing tasks before sending data on to other capabilities.
- 5G platforms can help support robust authentication and authorization capabilities to help enable zero-trust environments and architectures.
- 5G, especially at the edge and within a plant may be used to develop specific segments, LANs, or sub-LAN to help enable deception technologies and decoy networks.
- 5G offers significant flexibility in data transmission speeds. The faster data speeds of 5G can help enable accurate representations of networks, devices, and security systems by integrating real-time data and enabling new technologies like digital twins. These technologies may also be able to be used as used "hot standbys" for production OT equipment that have been attacked and compromised by cyber means.
- 5G networks reduce the reliance on proprietary hardware and software, commercial off-the-shelf (COTS) hardware can perform the same functions at a lower price point. Often, proprietary equipment and hardware rely on "security through obscurity" to try to stay under the security radar. However, with COTS equipment, security capability, features, and functions are more likely to have been integrated into the product in a development stage and can provide a cyber defender with the information and functionality needed to truly cyber harden the devices. With the additional advantage of being common COTS devices, they are functional and flexible. They typically support numerous applications, protocols, functions, and configurations, include a virtualized environment. This adds more complexity to a network design but can help to standardize configurations and maintenance across the fleet.
- Therefore, utilities with large numbers of DER devices may have IoT use cases for network slices that support monitor/control requirements for load management.

Cyber Security Considerations and Cautions

5G platforms offer considerable promise for utility networks. However, there are important questions that need to be answered and risks that require thoughtful mitigation.

- It will be critically important that the resources that design and implement device security—from utility owned grid components to end user IoT—correctly deploy devices to 5G standards. 5G technologies place increasing reliance on virtualization, network segmentation in the form of network slicing, and SDN. Skills competency will not be focused solely on OT domain expertise. There will be needs for skills more commonly associated with cloud computing, data centers, and IT environments along with wireless telecom and mobile device knowledge.
- Cyber security in networks that blend 4G and 5G technologies is only as good as the least secure technology. 5G technologies in an existing 4G network will not infuse the entire network with 5G cyber security capabilities. Network migrations must assess these risks and address vulnerabilities in both private and leased network scenarios. An overall review of the network, communication pathways and an understanding of which attack surfaces exist will allow cyber defenders to make the necessary mitigations to legacy equipment to ensure that the entire network is secure.
- 5G platforms offer new opportunities for utilities to embed distributed on-premises computing and/or cloud computing at grid edges to support edge computing. That will trigger security architecture changes to how utilities secure the grid edge and data at rest and in transit.
- The proliferation of grid-connected, end user IoT devices introduce new risks for utilities. Intrinsic cyber security baked into IoT devices could be an important mitigation to these risks. Without it, the burden will fall to properly skilled resources to correctly deploy devices to 5G cyber security protocols defined by utilities.
- Existing cyber security solutions that monitor traffic may not be able to adjust to the increase in speed and the added volume of traffic enabled by 5G platforms, either creating incomplete monitoring coverage or latency on the network as security devices need to slow traffic for a complete analysis. The increased analysis could also create a lot of new cyber security data that will be sent to Security Information and Event Monitoring (SIEM) tools.

These tools have the potential of creating additional reports and alerts that could inundate a human cyber defender, especially as the tools are learning how to baseline and tune the additional traffic.

- SDN adds new flexibility and scalability to network management, but also adds new risk. SDN replaces hardware-based network management functions with software that will connect with OT systems through a series of application program interfaces (APIs) that may be new in existing utility security architectures. Utilities leasing 5G networks should consider written descriptions, service level guarantees, and audit capabilities to ensure that network management APIs are fully secured by their service providers.
- Like all wireless communication, 5G still has the ability of being jammed. Depending on the function and data that the 5G network is serving, jamming can be detrimental to operations. It has been shown that persons with motivation, intent, and capability to jam wireless signals can be successful over a long distance with varying impact. In addition, because the signals and communications are being transmitted wirelessly, anyone with the proper equipment is able to capture and monitor the communications. If the communications are not encrypted, a cyber threat actor can inject malformed packets or unauthorized commands in line with effect.
- Some legacy OT communications networks and protocols cannot support encryption.

Hybrid Networks of 5G and WLAN

The 5G ecosystem and the Wi-Fi ecosystem can meet the requirements for high throughput wireless connectivity across a range of utility facilities and use cases. 5G offers the promise of interoperability and roaming between private and commercial networks. A device that works in-plant on a private 5G network may also be able to work externally on a commercial 5G network.

Both private 5G and Wi-Fi offer the advantage of private ownership of the infrastructure, and the ability to avoid ongoing subscription costs.

Wi-Fi 6 operates in unlicensed spectrum. In many in-plant environments, this is not a concern due to the location and isolation of the site. For urban and enterprise, the shared nature of unlicensed spectrum can result in unpredictable performance. The availability of 160 MHz channels enables the very high throughput that compares favorably to the best offered by 5G.

Modernization of the WLAN is a timely matter for many plants and utility sites. In many cases, the installed networks are based on 802.11n, which dates back to 2006. Wi-Fi has always ensured backwards compatibility, so these older networks continue to function with new devices. However, two generations have been released since then, and equally important, the Wi-Fi security standards have advanced to WPA3 in the past two years.

The leading option for Private 5G is CBRS (Citizens Broadband Radio Service) spectrum, which is shared spectrum controlled by a Spectrum Access Service (SAS). The SAS allocates spectrum and specifies allowable RF power based on avoiding interference with incumbents and other users. Depending on conditions, spectrum may be allocated as a 10 or 20 MHz channel. CBRS availability may be limited in urban areas but is widely available at the rural sites where many plants are located.

Commercial 5G services are offered in three types of frequency bands. Some operators offer 5G in low bands (under 1 GHz). These bands offer smaller channel size and throughput that is only slightly above LTE. The low bands offer the best coverage, so operators can highlight their nationwide 5G coverage based on these bands.

Table 1. Comparison of Wireless Technologies

Technology	Performance	Range	Cost Model
Private 5G (CBRS Spectrum)	100–200 Mbps UL and DL	100–500 m depending on allowed power and environment	CapEx plus small OpEx for SAS subscription
Commercial 5G (Mid-band spectrum)	~ 1 Gbps DL 100–200 Mbps UL	1 –5 km depending on site and environment	OpEx (subscription)
Commercial 5G (millimeter wave spectrum)	1–2 Gbps DL 200–500 Mbps UL	~ 100 m handheld mobile Typically, 1 km (sometimes up to 10 km) fixed wireless access Typically line of sight only	OpEx (subscription)
Wi-Fi 6	~ 1 Gbps UL and DL	~ 100 m – including indoor with obstructions	CapEx

The highest throughput is available from millimeter wave bands (24–72 GHz). These bands allow wide channels and multi-gigabit throughput. The downsize is the short range and line of sight propagation. These networks are commercially deployed only in densely populated areas. The millimeter wave 5G bands are all licensed, so they are not available for private network deployment.

Mid-band commercial spectrum is often referred to as sub-6 GHz but has the most significant amount allocated around 2.5 GHz. This spectrum offers high throughput with a longer range. It is being built out in the USA but will be primarily limited to urban areas. It offers the best model for bringing in external commercial 5G networks into a plant with a DAS.

An important characteristic of 5G commercial networks is the bias toward downlink performance. Downlink rate is important for consumers downloading content, so commercial networks optimize that metric. Utility use cases are often symmetrical or even uplink biased. The symmetrical performance of private 5G in CBRS and Wi-Fi 6 may be beneficial in this regard.

The best solution for a specific utility use case will depend on the situation, environment, and preferred cost models. Mixed and hybrid networks are also possible. This is quite practical since every 5G equipped device also supports Wi-Fi. The architecture and deployment of hybrid networks involving private Wi-Fi and commercial 5G introduce challenges and opportunities for enhancing cyber security.

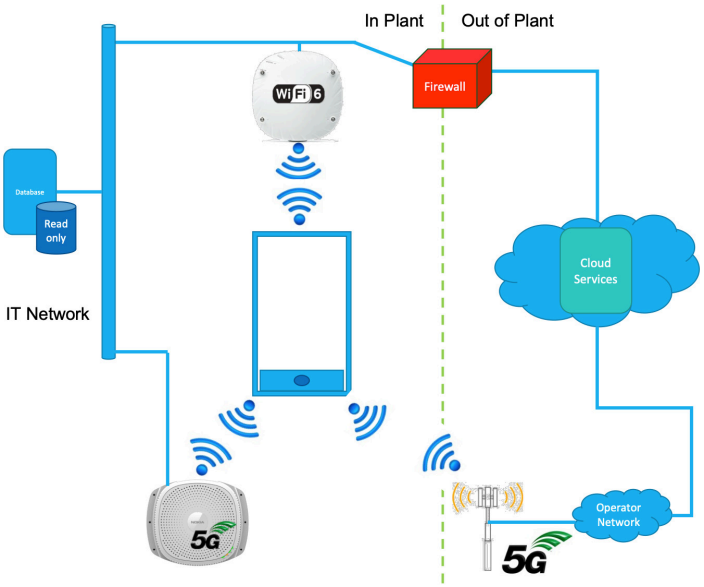


Figure 6. Example Hybrid 5G/Wi-Fi In Plant Network

Next Steps for EPRI Research

EPRI research in these areas is ongoing. The Information and Communications Technology program 161 continues to explore the application of private and public LTE for the grid and map the evolution and opportunities of 5G. The Cyber Security programs 183 and 209 continue to explore approaches to identify, contain, and mitigate cyber threats.

Current EPRI Projects

- The LTE and 5G Security project explores the security of these cellular standards, identifying threats and mitigations for both private and commercial networks.
- The Next Generation Wireless LAN supplemental project focuses on advanced connectivity using 5G and WLAN technology across the range of utility use cases, including In Plant, In Substation, and In Enterprise.

Future Opportunities for EPRI Research

- Develop an industry roadmap for next generation connectivity, leveraging where the broader wireless industry is going, (E.G. Toward a more distributed user plane, more functional partitioning, standards-based partitioning, and zero trust architecture.
- Investigate mutual interdependencies around precision timing. 5G/LTE networks and other utilities OT systems for in-plant, precision timing is needed for monitoring.
- Further study is needed to quantify the ROI for various private/public/hybrid models.

How utilities can leverage EPRI experience in evolution of communications and cyber security roadmaps:

- Vendors, regulators, SDOs, Utilities, DOE, and other agencies with an interest in 5G. A roadmap could be constructed by meetings of stakeholders.
- Address lack of knowledge of the growing internal interdependencies between digital systems deployed as part of utilities digital transformations. This includes precision timing, but much more. Timing, connectivity, management of data, how to deal with 5G as a new architecture.

The evolution of wireless technologies towards 5G brings opportunities and challenges for utilities. There is a need for ongoing research how to best ensure these new network platforms deliver additional reliability, resilience, and security for critical grid systems.

This challenge is exacerbated by moving systems to cloud services, which increases dependence on external telecom services and connectivity. The 5G architecture offers improvements in flexibility in the context of the internal and site networks, while providing a platform for enhanced cyber security capabilities.

EPRI RESOURCES

Tim Godfrey, *Program Manager*
650.855.8584, tgodfrey@epri.com

Jay Herman, *Principal Technical Leader*
913.626.8255, jherman@epri.com

Christine Hertzog, *Principal Project Manager*
650.314.8111, chertzog@epri.com

Nicholas Camilli, *Principal Project Manager*
704.595.2594, ncamilli@epri.com

Jason Hollern, *Program Manager*
704.595.2579, jhollern@epri.com

Information and Communication Technology (P161)

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY ITS TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE, DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY EPRI.

THE ELECTRIC POWER RESEARCH INSTITUTE (EPRI) PREPARED THIS REPORT.

Note

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

About EPRI

Founded in 1972, EPRI is the world's preeminent independent, non-profit energy research and development organization, with offices around the world. EPRI's trusted experts collaborate with more than 450 companies in 45 countries, driving innovation to ensure the public has clean, safe, reliable, affordable, and equitable access to electricity across the globe. Together, we are shaping the future of energy.

3002023219 December 2021

EPRI
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com