Pacific Northwest
NATIONAL LABORATORY

PNNL-39046

Reliability of Digital Communications in Nuclear Facilities and Operations

May 2026

Johnathan Cree
Jarrett Zeliff
Elena Peterson

Prepared for the U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Under Contract DE-AC05-76RL01830
Interagency Agreement: A2307-031-089-048662
Task Order Number: 31310024S0079

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from
the Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062
www.osti.gov
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov

PNNL-39046

Reliability of Digital Communications in Nuclear Facilities and Operations

May 2026

Johnathan Cree
Jarrett Zeliff
Elena Peterson

Prepared for the U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Under Contract DE-AC05-76RL01830
Interagency Agreement: A2307-031-089-048662

Pacific Northwest National Laboratory
Richland, Washington 99354

Executive Summary

This report evaluates methods for assessing the reliability of wired and wireless digital communication networks to inform future application-specific evaluations for nuclear facilities. It does not determine that wireless communications are acceptable for any particular nuclear facility application, and it does not recommend replacing wired communications with wireless communications for safety-related or important-to-safety functions. Rather, the report provides information and methodology that may inform future reliability evaluations where wired or wireless communication alternatives are considered. Communication reliability is important to operational safety, security, monitoring, and other facility functions, but the applicable key performance indicators and reliability expectations are application dependent. The framework is technology-agnostic and provides a hierarchy of network types with different reliability requirements. The authors consider both existing plants and advanced reactors, including small modular reactors.

Methodology

This report integrates reliability metrics across various layers, including physical connections, application-level metrics, such as latency, throughput, and accessibility. It emphasizes the importance of cybersecurity and how confidentiality, integrity, and availability can affect a safety basis. Environmental, infrastructural, and mobility considerations specific to wireless devices were also analyzed. The methodology advocates for a performance-based approach that leverages consensus standards (e.g., International Electrotechnical Commission [IEC], Institute of Electrical and Electronics Engineers [IEEE]) to create adaptable frameworks for analysis of network reliability.

Key Findings

1. **Wireless Technologies Evaluation**: This report categorizes wireless technologies based on taxonomy, including physical signal types (e.g., Light Fidelity [Li-Fi], Radio Frequency Identification [RFID], Near Field Communications (NFC), Low Earth Orbit [LEO] satellites), range (near-field to wide-area networks), and directionality. It highlights advantages, limitations, and evaluation considerations for technologies that may be considered in nuclear facility environments.

2. **Wired vs. Wireless Performance Comparisons**: Wired communication is generally more deterministic in safety-critical scenarios. Wireless solutions may offer flexibility, reduced infrastructure needs, and accessibility benefits, particularly for remote nuclear facilities and small modular reactors; however, whether those benefits are appropriate for a particular application depends on application-specific reliability, environmental, cybersecurity, and safety evaluations.

3. **Reliability Challenges**: Factors such as signal interference, handoffs, and environmental impacts can complicate analysis of wireless communication reliability for nuclear facility applications compared to wired analysis. These challenges do not support a generic determination that wireless is acceptable or unacceptable; instead, they reinforce the need for application-specific evaluation. To address these challenges, key performance indicators are proposed for holistic network evaluations, along with simulation, emulation, and field testing.

Implications for Nuclear Facilities

This report concludes with insights for evaluating wired and wireless communication networks for nuclear facilities. It discusses fault-tolerant and deterministic networking technologies, as well as probabilistic methods that may inform reliability evaluations, where appropriate. The report also emphasizes adherence to exclusion zones and the development of alternative safety controls through site-based assessments, simulations, hardware testing, or a combination of controls to evaluate and mitigate potential interactions between wireless networks and existing systems.

Acronyms and Abbreviations

BLE	Bluetooth low energy
FSO	free space optical
IEC	international electrotechnical commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
KPI	key performance indicators
LEO	Low Earth Orbit
Li-Fi	Light Fidelity
MTU	maximum transmission unit
NAN	neighborhood area networking
NASA	National Aeronautics and Space Administration
NPP	nuclear power plant
PRA	probabilistic risk assessment
QoS	quality of service
RAW	Reliable and Available Wireless
RF	radio frequency
RFI	radio frequency interference
SMR	small modular reactor
UHR	ultra-high reliability
URLLC	ultra-reliable low latency communication
WLAN	wireless local area network
WNAN	wireless neighbor area network
WPAN	wireless personal area network
WWAN	wireless wire area network

Contents

Figures

Tables

1.0 Introduction

This report discusses wireless communication technologies as part of a reliability-evaluation framework for digital communications that may support or interface with a range of nuclear facility functions. References to safety-related, important-to-safety, security, monitoring, and non-safety applications are intended to make the discussion relevant to the different reliability expectations associated with those functions; they are not a determination that wireless communication is acceptable for those applications, nor a recommendation to use wireless communications in safety-related or important-to-safety systems. In some circumstances, wireless technologies may offer flexibility, adaptability, broad-area connectivity, reduced infrastructure needs, or mobility benefits. Potential examples include adding or extending monitoring equipment, supporting temporary communications during network recovery, or providing connectivity where wired infrastructure is impractical. Whether any such application is appropriate would require an application-specific evaluation of reliability, environmental conditions, cybersecurity, physical security, potential effects on other systems, and applicable regulatory or safety considerations.

The major difference between wired and wireless communications is that wired communications utilize a well-defined medium (e.g., twisted copper wire or fiber cable) to transmit the signals. Wireless communications, on the other hand, utilize physical matter (e.g., air, water vapor, sheetrock, and concrete) that exists in the space between the transmitter and receiver to transmit the signals. As such, because wired communications use a more controlled transmission medium, they are generally easier to assess in a general case. The difference does not preclude evaluation of wireless technologies, but it underscores the need for a methodology to assess the reliability of a wireless network and compare it with a wired counterpart for the specific application under consideration.

1.1 Purpose

The purpose of this effort is to develop a methodology for evaluating wired and wireless communication reliability for potential nuclear facility applications. This includes a well-defined method to compare wireless to wired communications from a safety and reliability perspective without making a generic determination that wireless communications are suitable for any particular application. This evaluation method needs to:

- be technology agnostic supporting any wireless medium, (e.g., radiofrequencies [RFs], light, sound, magnetic induction, etc.) and allow for comparative assessments with wired mediums (e.g., copper, fiber, etc.)
- be able to assess the technology's use across multiple missions such as safety, security, reactor monitoring and/or control, building/equipment maintenance, etc.
- support multiple facility types, current fleet vs. small modular reactors (SMRs) vs. advanced reactors.

In order to meet the three criteria stated above, this effort's goal is to leverage consensus standards and develop performance-based metrics to provide a methodology that can be adapted to specific applications.

1.2 Application of Data Links in Nuclear Power Plants

Data links in nuclear power plants (NPPs) can be categorized into two major categories (1) local network links connecting equipment at a facility, and (2) backhaul-type connections between facilities and/or between a site and a central location.

The local network link is comparable to the network in our homes and provides the connectivity between equipment, sensors, people, etc. For wireless networks, such as Wi-Fi and cellular, providing network access to a broad set of devices the infrastructure, (i.e., cabling) is substantially reduced. These types of networks are called last-hop or last-mile networks, as the wireless network provides the last part of the network connection. Using last-hop wireless networks in facilities with multiple networks can have significant benefits by reducing the amount of cabling to be installed and maintained. For example, in a typical facility business systems will be on a different network than safety systems and security systems will have another network as well. All these networks increase the cost and complexity of deploying and maintaining wired networks in a facility and a set of wireless networks can significantly decrease the cost while providing additional capabilities.

Backhaul networks connect facilities such as SMRs in remote locations to a central monitoring/control station and/or provide connectivity between two sites. Wireless has transformed connectivity options over the last 5 years provided by service providers in rural areas, making it possible to connect to high-speed internet almost anywhere in the world. These service provider-based solutions include cellular, Low Earth Orbit Satellite (e.g., Starlink (Starlink 2026), Project Kuiper (Kuiper 2026)), and other wireless service providers. Alternatively, if connecting two sites that are relatively close, less than 25 km to each other, point-to-point wireless backhaul networks can provide solutions using RF or light based such as Taara (Taara Connect 2026). The point-to-point solutions can be set up in hours to days without having to dig trenches between two sites.

1.3 Importance of Communication Reliability in Nuclear Power Plants

Communication reliability for use in nuclear facilities encompasses several factors, ensuring that the communication between the devices on the network is consistent, accurate, and dependable. Reliability of a communication network is measured using the ratio of successfully transferred data to total data transferred. Successfully transferred data are data sent by an application that arrives unaltered and intact at the intended destination and within the required time period. Total data transferred encompasses all data sent by an application regardless of whether it was received. Reliability of digital communication systems can be broken down into the components defined in Section 1.4. Additionally, the larger system which the communication infrastructure is part of should behave predictably and consistently in various conditions, ensuring that communication does not lead to unpredictable states or behaviors. This involves handling variations in network conditions gracefully and maintaining a stable communication state.

Nuclear power plant communication reliability is crucial and varies based on system type: safety-related, important to safety, and non-safety-related systems. For example, business systems have a lower reliability necessary to meet functional requirements than a safety critical system such as reactor control. Even though when a business system is down it can be inconvenient for its users, the reactor can still function and produce power safely. However, if

the communications for the reactor control were to go down and the controllers were to lose the ability to monitor and control safety critical systems, then ideally the reactor safety systems would respond appropriately with automated shutdown functions to prevent an accident. Therefore, it is important to be able to assess the reliability of sub-systems to be able to compare alternative solutions. This comparison can be completed using performance-based metrics to determine whether a solution can meet the reliability requirements necessary for a given system. The outcome of this comparison with regards to reliability can be used to determine the impact to the reliability of the system as a whole.

1.4 Defining Communication Reliability

Reliability is a multifaceted term which has been split into different attributes and defined by the International Electrotechnical Commission (IEC), Internet Engineering Task Force (IETF), and National Aeronautics and Space Administration (NASA). The IEC defines an umbrella term which is called dependability. Dependability includes attributes such as "*reliability, maintainability, and supportability and the resulting availability and in some cases, attributes such as resilience, recoverability, durability, integrity, safety, security, trustworthiness are included in or overlap with dependability*" (IEC 192-01-22 2026).

Even though IETF RFC 4949 uses the attributes of availability, reliability and survivability, RFC 2729 provides a taxonomy of communication requirements with a subsection focused on a taxonomy of communication reliability and related aspects. The most recent work for reliability at the IETF is a working group for Deterministic Networking (detnet) with one of their focuses being high reliability for both wired and wireless networks. Previously there was a separate wireless working group named Reliable and Available Wireless (RAW) at IETF, which released a draft architecture, Reliable and Available Wireless Architecture/Framework, in February 2025 (IETF 2025) and is now being folded back into the Deterministic Networking working group. The RAW draft references the NASA reliability definition, which is defined in NASA-STD-8729.1A—2017-06-13 (National Aeronautics and Space Administration 2017) and categorizes the concept of reliability into three attributes: reliability, maintainability, and availability.

It will be necessary to properly apply these definitions of the concept of reliability appropriately when assessing and comparing the reliability of wired and wireless networks. The IEC's definition of reliability as well as NASA's can be applied broadly to the use of an operational system whereas the IETF's definition of the concept of reliability focuses specifically on network requirements.

As such, in this document the IEC's definition of dependability will be utilized as an umbrella term and the IEC's definitions for reliability, maintainability, supportability and availability will be used when determining the reliability of a system/sub-system. IETF's definitions for reliability, availability and survivability will be utilized when assessing the reliability of a network link.

1.5 Monitoring vs. Control

IEC defines a control system as *"system constituted by a controlled system and its controlling system, in closed-loop control completed by the measuring element and the reference-variable generating element"* (IEC 351-49-06 2026). As such, the monitoring system by itself is not necessarily a control system. It is only part of a control system if the measurements it takes are part of a closed-loop control and used by the controlling element to make decisions.

Monitoring systems can be used for a range of purposes:

- maintenance and predictive maintenance
- internal or external monitoring as an auditing function
- off-line optimization of systems where a human is making the decisions on what to implement based on the data gathered
- feedback to an automated function of the control system and as such are part of the larger control system (in this case it would be considered part of a control system)

2.0 Wireless Technologies Overview

Wireless communication technologies can be categorized into taxonomies using different properties of the technology. Three common properties that are used include (1) type of physical signal (e.g., RF, light, sound, magnetic induction, etc.) (Section 2.1.1), (2) range or network coverage (Section 2.1.2), and (3) directionality (Section 2.1.3).

2.1.1 Taxonomy Based on Physical Signal

The type of physical signal used has a major effect on how well it works in a given environment. For example, light requires line-of-sight and is easily blocked by materials, RFs travel well through air but not water whereas sound travels well through water. While RF is the most abundantly used in commercial applications, other technologies may have niche benefits to specific applications.

2.1.2 Taxonomy Based on Range

Range is a common taxonomy when categorizing RF communication network solutions as shown in Figure 1. It is important to note that in these taxonomies it is common to leave out point-to-point RF solutions which are covered in the next section. Near Field Communications, (NFC), and Radio Frequency Identification (RFID), are proximity-based solutions with a general range of less than 10 m. Wireless personal area networks (WPANs) have a range of up to 100 m and include technologies such as Bluetooth®, whereas wireless local area networks (WLANs) include the different generations of Wi-Fi technologies with ranges up to 1 km. Wireless neighbor area networks (WNANs) provide coverage up to 10 km and include site-based, neighborhood networking technologies which include Zigbee neighborhood area networking (NAN) as well as small cell private cellular networks and wireless wide area networks (WWANs) provide ranges up to 100 km and include macro-cellular technologies as long as low-power wide-area network (LPWAN) solutions such as long-range WAN (LoRaWAN) and SigFox.

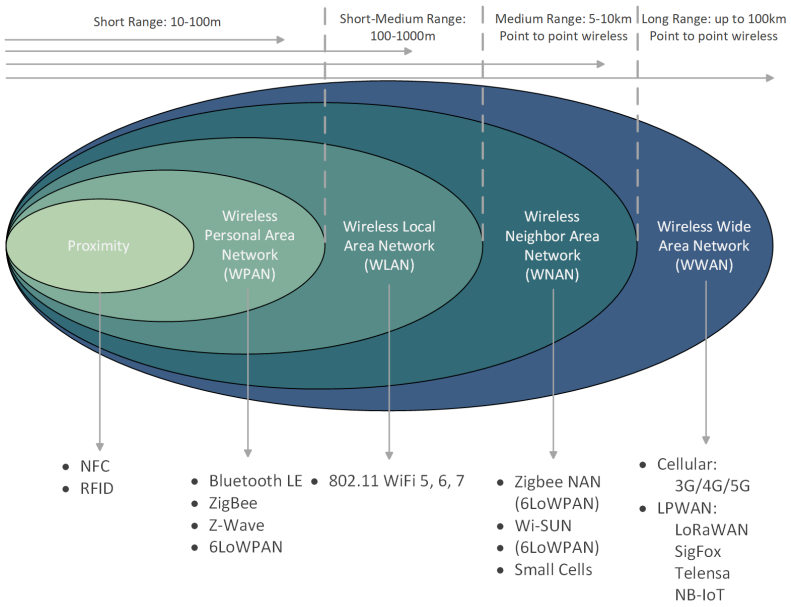

Figure 1. Ranged-based Taxonomy for Radiofrequency Communication Networks

2.1.3 Taxonomy Based on Directionality

Directionality is an important component of wireless communication technologies, as shown in Figure 2. Most consumer devices are omni-directional, meaning that their antennas can transmit and receive signals from any direction. Omni-directional devices provide the ease of use necessary for the general consumers to pick up a device and use it without knowledge of the location of the transmitters. Devices with directional antennas can be paired with omni-directional devices to build a network such as in the cellular network where directional antennas are used on cell towers and user-devices have omni-directional antennas. Directional antennas can also be considered highly directional, creating a tight beam between two devices, which is seen in point-to-point wireless devices. Some technologies such as light-based communications favor directionality where a sound on the other hand reflects so easily that even directional solutions become essentially omni-directional.

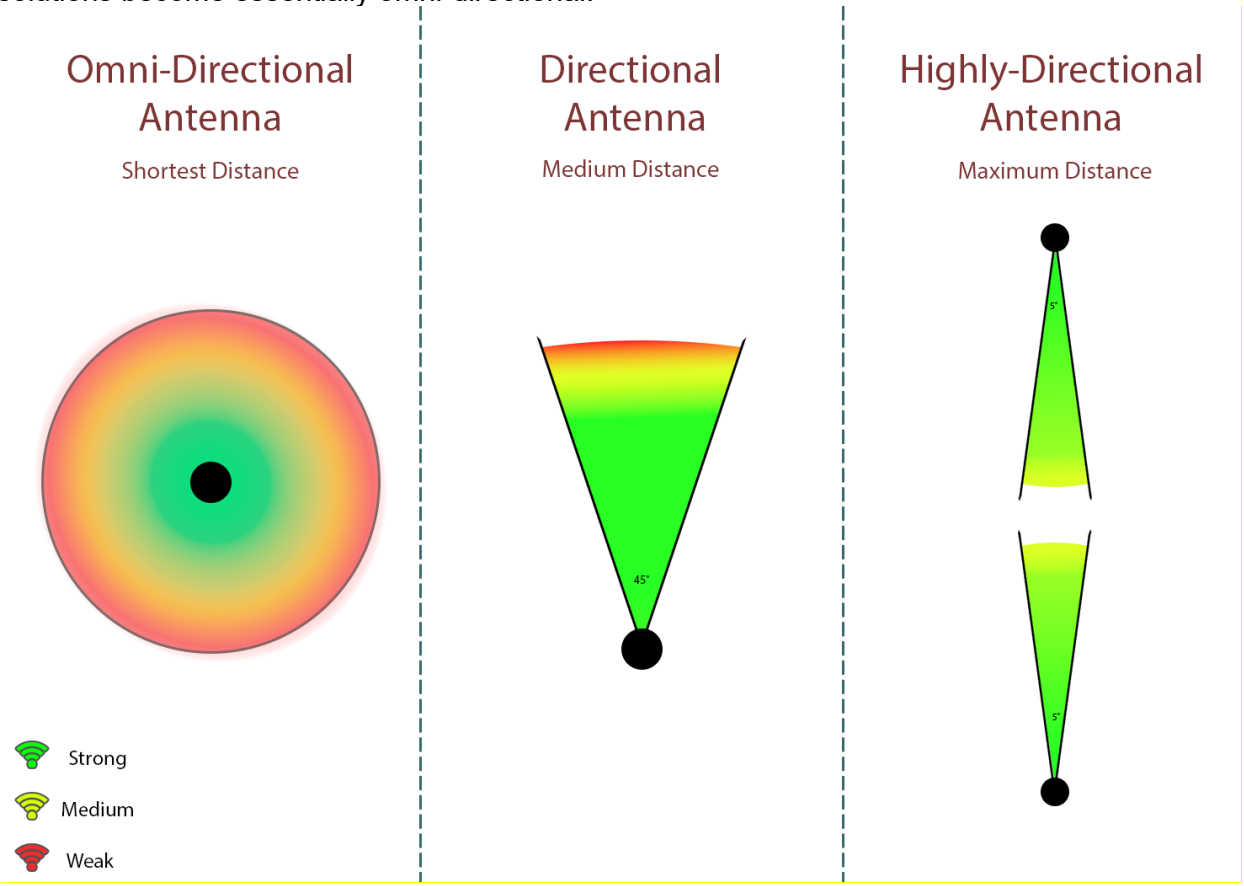

Figure 2. Antenna Type Taxonomy

2.1.4 Common Wireless Technologies

Below is a list of commonly used wireless technologies that provide a wide range of capabilities. This list is not inclusive of all wireless technologies that may be useful in nuclear facilities.

- Wi-Fi 802.11: Wi-Fi is a widely used wireless networking technology based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards. It provides high-speed internet and local network connectivity over short to medium distances. Commonly used within homes, offices, and public spaces.

- Bluetooth®: Bluetooth is a short-range, peer-to-peer (P2P), wireless technology designed to connect and exchange data between devices. Often used in headphones, speakers, smartphones, and fitness trackers. Bluetooth operates on the 2.4 GHz frequency band and is ideal for WPANs.
- Zigbee: Zigbee is a low-power, low-data-rate wireless communication protocol specifically designed for Internet of Things (IoT) devices. This technology is well suited for smart home devices and industrial automation and makes use of mesh networks to extend its range.
- Z-Wave: Z-Wave is a wireless communication protocol primarily used in smart home automation. Operating in the sub-1 GHz band to avoid interference with Wi-Fi and Bluetooth, it enables smart devices like locks, lights, and thermostats to communicate in a mesh network. Z-Wave boasts long battery life and easy interoperability, with a focus on secure and encrypted connections for residential and commercial applications.
- 6LoWPAN: 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) is a networking protocol that enables resource-constrained devices to use internet protocols such as IPv6. Allowing devices to connect over low-bandwidth, low-power networks. Designed for constrained environments, 6LoWPAN facilitates efficient communication in applications ranging from home automation to industrial monitoring.
- LoRaWAN: LoRaWAN (Long Range Wide Area Network) is a protocol optimized for battery-powered devices that require long-range communication with minimal energy consumption. Operating in sub-1 GHz frequency bands, LoRaWAN enables communication over distances of up to several kilometers, making it ideal for applications like agricultural monitoring, smart cities, and industrial IoT. Its low data rate sacrifices speed for battery longevity and is best suited to devices that transmit small packets of data intermittently.
- Cellular 4G, 5G: Cellular communication technologies such as 4G and 5G enable seamless wireless voice, video, and data transmission over large geographic areas. While 4G provides high bandwidth for mobile broadband, 5G introduces ultra-low latency and high-speed connectivity. Cellular networks serve diverse applications ranging from smartphones to autonomous vehicles and are supported by robust global infrastructure.
- Satellite LEO: Low-Earth Orbit (LEO) satellites provide global wireless connectivity for remote and underserved regions. Positioned closer to Earth than traditional geostationary satellites, LEO systems (such as Starlink) offer lower latency and faster speeds, making them ideal for internet services, and disaster recovery. They are especially critical for maritime, aviation, and other scenarios where terrestrial networks are unavailable.
- Li-Fi: Li-Fi (Light Fidelity) is a wireless communication technology that uses visible or infrared light to transmit data at high speeds. It operates as an alternative to radio frequencies and can be integrated into LED lighting systems for dual functionality. Li-Fi is well-suited for RF-sensitive environments such as hospitals and airplanes, offering fast, localized, and interference-free communication.
- Point-to-Point: Point-to-point wireless communication establishes a direct connection between two fixed locations. It is often used to extend networks in remote areas or link buildings and towers where physical cables are impractical. Point-to-point systems are known for their high bandwidth, reliability, and low latency but require precise line-of-sight alignment.
- Free space optical: Free Space Optical (FSO) communication uses focused beams of light, such as lasers, to transmit data wirelessly through the air. It provides high-speed secure communication over medium-to-long distances as long as there is a clear line of sight. FSO is

an effective alternative to fiber-optic cables in urban or challenging terrains, though environmental factors like fog and dust can impact performance.

- RFID: RFID uses electromagnetic fields to automatically identify and track objects via tags embedded with electronically stored information. These tags communicate with RFID readers to enable inventory management, access control, and supply chain tracking. RFID operates across frequency bands (low, high, ultra-high) based on the desired range and data transfer requirements, offering versatility in commercial and industrial settings.
- NFC: NFC is a short-range wireless technology that enables secure communication between two devices held within a few centimeters of each other. Commonly used for contactless payments (e.g., Google Pay, Apple Pay), secure door access, and device pairing, NFC operates on the same frequency as RFID but focuses on very close proximity for added security and ease of use. Its simplicity and versatility make it ideal for many consumer applications.
- BLE: Bluetooth® Low Energy is a variant of Bluetooth designed specifically for power efficiency and extended device battery life. BLE supports IoT applications such as smart lighting, wearable health monitors, fitness trackers, and other low-power devices that require intermittent data transmission. While its range and bandwidth are lower than standard Bluetooth, BLE's optimization for minimizing power consumption makes it ideal for battery powered devices in connected ecosystems.

2.1.5 Characteristics of Wireless Communications

Wireless communications can be characterized in many ways. Common properties to compare multiple solutions include throughput, reliability, latency, mobility, number of connected devices, and energy consumption. With current technologies it is possible to increase these different attributes with compromises. For example, increasing the range of wireless signals either increases power consumption or, if it is already running at maximum power, reduces the throughput. Increasing reliability may decrease throughput and increase latency. Generally, marketing materials provide the best case scenarios—maximum throughput, minimum latency, maximum range. However, it is unlikely that all these properties can be achieved simultaneously. Furthermore, each technology differs and the effect on the range of one technology by increasing power, may not provide a similar benefit to another technology.

Similar attributes can be used when comparing wired and wireless communications. Tradeoffs among these attributes can also be found in wired networks. For example, as shown in Table 1 for ethernet cabling, wired communications have maximum ranges for each type with a tradeoff between maximum range, reliability and throughput. The longer the cable, the lower the signal-to-noise ratio, which can increase the bit error rate, which is described later in Section 3.0.

Due to the configurability of these technologies and their tradeoffs, comparing wired and wireless technologies requires prior consideration of both technology and configuration. Comparing the as-marketed values will not provide a sufficient comparison as they are not likely achievable.

Table 1. Ethernet Cable Maximum Distance vs. Type vs. Data Rate

Category	Max. Data Rate	Bandwidth	Max. Distance	Usage
Category 1	1 Mbps	0.4 MHz	-	Telephone and modem lines
Category 2	4 Mbps	4 MHz	-	LocalTalk & Telephone
Category 3	10 Mbps	16 MHz	100 m (328 ft.)	10BaseT Ethernet
Category 4	16 Mbps	20 MHz	100 m (328 ft.)	Token Ring
Category 5	100 Mbps	100 MHz	100 m (328 ft.)	100BaseT Ethernet
Category 5e	1 Gbps	100 MHz	100 m (328 ft.)	100BaseT Ethernet, residential homes
Category 6	1 Gbps	250 MHz	100 m (328 ft.) 10Gb at 37 m (121 ft.)	Gigabit Ethernet, commercial buildings
Category 6a	10 Gbps	500 MHz	100 m (328 ft.)	Gigabit Ethernet in data centers and commercial buildings
Category 7	10 Gbps	600 MHz	100 m (328 ft.)	10 Gbps Core Infrastructure
Category 7a	10 Gbps	1,000 MHz	100 m (328 ft.) 40 Gb at 50 m (164 ft.)	10 Gbps Core Infrastructure
Category 8	25 Gbps (Cat8.1) 40 Gbps (Cat8.2)	2,000 MHz	30 m (98 ft.)	25 Gbps/40 Gbps Core Infrastructure

Source: Eaton 2026. "Ethernet Cables Explained." Accessed January 20, 2026. https://tripplite.eaton.com/products/ethernet-cable-types.

3.0 Reliability Metrics for Wired and Wireless Digital Communication

Modern wireless communications are working towards a focus on reliability such that the benefits of wireless can be brought to applications that traditionally require wired networks. For example, the 5th Generation mobile cellular broadband network (5G) added support for Ultra-Reliable Low Latency Communications (URLLC) with a goal of latency as low as 1 ms and 99.999% reliability. The future Wi-Fi 8 protocol, 802.11bn (Galati-Giordano et al. 2024), has a focus on Ultra-High Reliability (UHR) to support applications that have strict reliability requirements. IEEE 802.15.4 standards (IEEE 2016) have also been working on providing high reliability and deterministic communications for wireless technologies with advanced features such as time-slotted channel hopping.

Assessing the reliability of communications between a single link in either wired or wireless systems relies on communication properties, as described in Section 2.1.5, that are affected by:

- synchronization and timing—wireless links where the devices are synchronized can provide coordination on when to send/receive and decrease the probability of contention/interference
- location of devices—two devices that are out of range of each other may not know of each other and transmitted signals can cause problems for devices that are in an overlapping area
- latency—the amount of time it takes the message to traverse the transmission medium
- signal-to-noise ratios—how much signal makes it from the transmitter to receiver compared to the amount of noise/interference that is received at the receiver
- a combination of the above.

When viewing a wired or wireless network as a whole, instead of a collection of individual links, it is important to account for higher level networking concepts such as:

- network flows and routes
- redundancies in network paths
- fault tolerance of the network
- quality of service needs of multiple applications
- functional patterns for each device on the network and how to manage resource allocation
- packet ordering as messages can be split into multiple packets and arrive out of order based on the different paths each packet can utilize.

It is important to note that both wired and wireless networks can be affected by and cause unintentional effects on other systems. From a technological point-of-view the major difference between the wired and wireless communications is that wired communication uses a well-defined medium (e.g., wire, a trace on a circuit board or fiber cable) to transmit the signals and the shielding on the cable reduces the exposure of those signals to the outside environment. Wireless, on the other hand, uses physical matter (e.g., air, water vapor, sheetrock, concrete, etc.) that exists in the space between the transmitter and receiver to transmit the signals.

IETF RFC 2729 provides an extensive Taxonomy of Communication Requirements. While this taxonomy was meant specifically for large-scale multicast applications, by generalizing RFC

2729 as needed, it provides a great overview of communication requirements necessary to assess the reliability of any application. This makes it a great reference for a starting point for comparing wired and wireless reliability.

Ongoing IETF work on Deterministic Networking (detnet) (IETF 2026) , including prior Reliable and Available Wireless work, is relevant because it addresses bounded reordering, latency, loss, packet delay variation (jitter), and high reliability for wired and wireless networks.

3.1 Reliability Metrics for Wired and Wireless Link

Reliability of a communication link can be measured using error rates such as bit-error-rate or packet-error-rate. Bit-error-rate, a measure of the number of bit errors relative to the number of bits sent with bits being the smallest unit of data represented by a 0 or a 1. Packet-error-rate is a similar measure that instead measures the number of erroneous packets received relative to the number of packets sent. A data packet is a package of data that is used to transport data across the network, it typically includes sender/receiver address and some way to check and validate that the packet was received correctly. If the packet was not received correctly and the errors cannot be fixed on the receiver's end, then the packet must be retransmitted. As such, the bit-error-rate has a direct correlation to the packet-error-rate which in turn can require retransmitting packets reducing available bandwidth and potentially causing additional bit-errors.

While bit-error-rate and packet-error-rates are good measurement tools to determine the stability of a network link, they are primarily measurements that are affected by underlying causes which can make them difficult to consistently measure and predict the outcomes, especially in dynamic networks that change over time. As such, it is likely better to compare the reliability of two networks using the underlying characteristics of the network including: signal-to-noise, latency, timing/synchronization, and location of devices.

Signal-to-noise is the amount of signal received by a receiver compared to the noise of the environment. Noise may be from interference or background noise. This concept correlates well with sound and how it is easier to hear someone speaking in a quiet room than a loud room when the speaker is speaking at the same volume. The higher the received signal compared to the noise results in a lower the bit-error-rate/packet-error-rate as the receiver can clearly hear the message.

Latency is the amount of time it takes for the message to go from the sender to the receiver. Usually this is measured in round-trip-latency which includes processing time and the amount of time it takes for the initial receiver to respond. Latency has a direct influence on the amount of data that can be transmitted because links with lower round-trip-latency can respond and start the next transfer faster. Latency can also directly affect reliability as it can affect message length and the chance to be impacted by interference, e.g., speed of light vs. speed of sound.

Timing/synchronization of devices and messages can affect the bit-error-rate through contention/interference. If devices transmit at the same time using the same underlying medium, then the messages can cause contention by having two or more messages collide. This collision can cause one or more of these messages to have lower signal-to-noise ratios and thus higher bit-error-rate, reducing overall reliability. However, if devices mitigate the timing issues through some type of synchronization, the devices can minimize the chance that multiple devices transmit at the same time helping address potential link reliability issues caused by contention.

The timing/synchronization issues are influenced by the location of the devices.

- In wireless networks this is as simple as if two or more devices are located far enough away from each other that they cannot directly affect each other's transmission then these devices can transmit at the same time and timing/synchronization is not required shown in Figure 3. If the devices are located within transmission distance from each then synchronization can help mitigate timing issues.
- In a wired network synchronization is critical for devices that share the same cable. In a network architecture where each pair of devices have a single cable run between them with separate cables for transmission and reception then the devices can freely transmit as needed. If devices share the same transmission cable with one or more device(s) then timing matters and synchronization can mitigate timing issues.

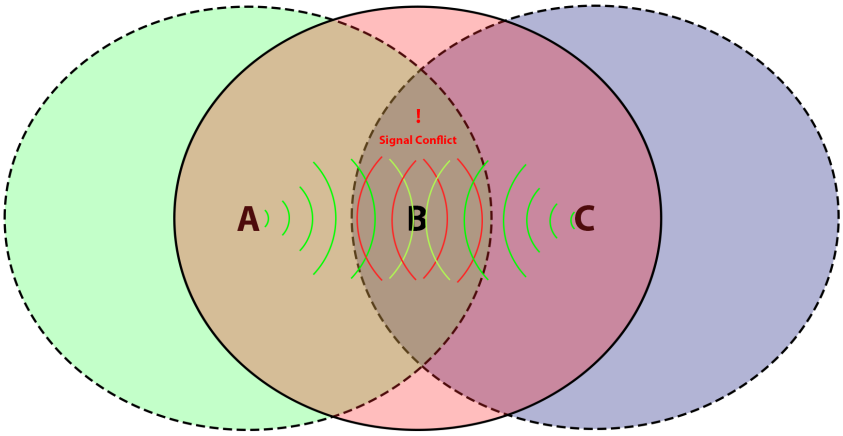

Figure 3. Two separate signals outside of each other's range can cause conflicts on the receiver's end

3.1.1 Environmental Considerations (Wireless)

As wireless links use the open space to send signals, the environmental conditions may have an impact on the signal-to-noise ratios and thus affect the bit/packet error rates. As such, reliability of the communication link must take into consideration the range of ideal and non-ideal environmental conditions that the network will be exposed to and mitigate risks appropriately. Environmental considerations must be made to ensure that all possible conditions are accounted for with respect to the underlying communication technology and any systems communication technology may have an adverse effect on. Examples of these include but are not limited to:

- wireless systems that use light, smoke, or other aerosols that can cause degradation of the signal between transmitter and receiver.
- precipitation, such as rain or snow attenuating a wireless signal through either RF or light.
- a "noisy" (sound, RF, light, magnetic, etc.) environment, where there are unintended irradiators such as power transformers that are creating noise, other equipment in the environment that use the same frequencies, or something intentionally jamming the environment.
- space weather and electromagnetic pulse effects, particularly where satellite, long-range wireless backhaul, or other exposed communication paths are considered.

- wireless signals from a network causing incorrect sensor measurements within a facility. This must also consider the materials in an environment as reflections of wireless signals can create additive interference in locations causing higher signal strengths at specific locations.
- radiation environments can affect digital electronics and communication equipment by causing single-event upsets or other errors in memory, processors, or transmitted/received data. These effects are not unique to wireless systems, but may need to be considered for communication equipment located in radiation environments.

3.1.2 Infrastructure Aging Considerations

Reliability of each link depends on the age and deterioration of the equipment/infrastructure. Communication network components degrade over time (e.g., fiber cables deform or sustain rodent damage, the copper in ethernet connections corrodes, and cable shielding cracks or blisters). Seismic events, vibration, and other mechanical stresses can also loosen connectors, damage terminations, or cause complete or intermittent loss of connection. All these issues can cause degradation in the signal-to-noise that is received on the other side of the link and introduce errors on that link. They may also cause a link to completely go down. The rate at which the infrastructure degrades is determined by the environment it is exposed to (e.g., thermal, radiation, humidity, debris and physical stress extremes) as well as maintenance such as wire/fiber splicing. In some cases, reducing reliance on long cable runs or equipment exposed to harsh environments may reduce certain aging-related failure mechanisms; however, any wireless alternative would need to be evaluated for its own environmental and reliability vulnerabilities.

3.2 Reliability of end-to-end connections

An end-to-end connection is the connection between the initial sender and the final receiver which may include multiple network hops across different wired/wireless networks. Take for example, the network shown in Figure 4, there are five computers (A–E) connected to three routers (1–3) which are connected to a server. An end-to-end connection between terminal A and the server passes through all three routers. In this scenario, bit/packet errors could be introduced on each of the four links through which the data has to traverse as described above or a router may be overloaded and decide to drop a packet based on the available throughput it can handle and how much data is being processed by all devices sending data through that router. Even in this simple example measuring the reliability of the end-to-end connection can be extremely complex. In the real-world terminal A would likely have multiple paths to be able to send data to the server, and the data from A may be split up and traverse multiple paths to be reassembled at the server in the proper form. As such, the reliability of the end-to-end connection is not just a function of the reliability of each link, it includes additional factors such as:

- network flows and routes
- redundancies in network paths
- fault tolerance of the network
- quality of service (QoS) needs of multiple applications
- functional patterns of life for each device on the network and how to manage resource allocation
- packet ordering as messages can be split into multiple packets and arrive out of order based on the different paths each packet can utilize

- protocols that are used by equipment in the network.

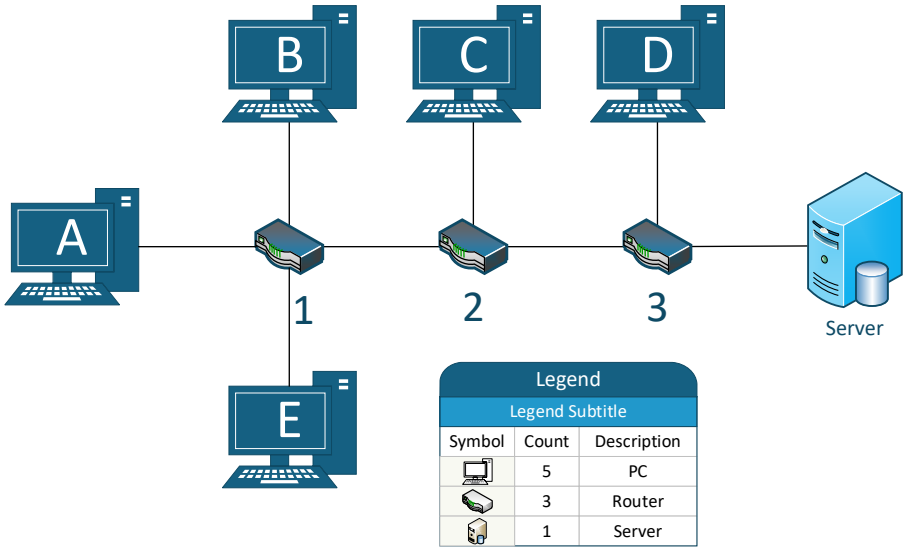

Figure 4. Example Network

There are solutions and protocols designed to enhance the end-to-end reliability of a wired and wireless network. These solutions provide functionality for load balancing and redundant messaging, as well as the ability to prioritize certain network traffic over other traffic. For example, there may be an application that requires low latency, and these algorithms can be designed to minimize the latency of one application and in doing so the latency for a different application may increase that is not as sensitive to latency (e.g., low latency video conferencing vs. email).

Further, applications can also have methods to enhance the end-to-end reliability of a network link. A simple example to explain this is when a streaming video reduces its quality during times of network congestion. This type of application can increase the reliability of the overall network at the expense of additional complexity when assessing the overall network reliability as these applications create highly dynamic traffic patterns that react and adjust to current conditions.

3.3 Reliability of the Application

Viewing reliability from the perspective of the application introduces a number of other considerations. Questions such as:

- Does the application have access to the network resources it needs?
- How do cybersecurity controls impact the reliability analysis of the network?
- Are the network components physically secure, if not how does the physical security of a component impact the overall reliability of the network?

The following sections cover the application layer components to assess when determining whether the underlying reliability of a wired or wireless link impacts the overall application.

3.3.1 Accessibility, Latency and Throughput

Accessibility, latency, and application throughput are related measures of a communication network's QoS. The reliability of an application is dependent on the network's ability to meet the QoS requirements for that application and the capability of the network to provide the necessary access and uptime requirements within the throughput and latency needs. Priority schemes and deterministic networking controls should be evaluated carefully because prioritizing one application can improve determinism for that application while reducing available margin for other applications sharing the network.

Accessibility is the ability to access the network when and where it is needed. This can be a specific location or an area of coverage that allows for mobility of the connected devices. The reliability of a network's accessibility is dependent on the other network traffic and signals using the same communication medium. To mitigate accessibility risks, redundancy can be built into the network to ensure that there are multiple methods to connect a device.

As noted earlier, latency is the amount of time it takes to send a packet from a source to a destination. Some applications have strict latency requirements (e.g., voice/video calls) and others do not (e.g., email). When there are latency requirements the application's reliability is dependent on the network meeting these requirements. Many industrial automation applications require latencies which are too low for humans to perceive. Latency can be affected by the following: underlying technology, physical distance between source and destination, routing path, and network congestion. Mitigating reliability risks regarding latency can be performed through QoS prioritization and/or deterministic networking.

Application throughput is the amount of data that is sent and received by an application. Network throughput is the maximum data that a network can process at a given time. When determining the required throughput of a network it is important to consider the throughput required by all applications that will utilize that network. Applications that have throughput requirements can utilize QoS prioritization to mitigate reliability risks.

3.3.2 Confidentiality, Integrity, and Availability

The confidentiality, integrity, and availability are the triad that form cybersecurity. These components are important to safety applications as they guard against unauthorized access to data and systems and data manipulation. Without cybersecurity components in place the safety of a system could be compromised without knowledge.

- Confidentiality: The network should transmit data such that only the authorized recipient(s) can read the messages. It is important to note that information can be gleaned by functional patterns of life such as when and where a specific type of message is sent. Unique identifiers also present confidentiality concerns especially in mobile systems as these identifiers can be used to track mobile systems. In terms of reliability confidentiality is an application specific factor, some applications require confidentiality, others do not.
- Integrity: The integrity of the data packets being sent over the network should not be susceptible to manipulation, spoofing, duplication, etc. The network equipment itself should not be altered in an unauthorized way either by a human or as an autonomous response. Ways to ensure integrity may include blacklisting an authorized device, changing routing in a way to drop packets, etc.

- Availability: The network needs to be available and able to send an authorized message from the source to the destination as specified by the operational needs. Factors for availability include up-time of the network, network redundancy both in backup equipment and in multiple routes for data to take, and the ability for the network to continue to operate when presented with denial-of-service attacks.

3.3.3 Adaptability, Extensibility, and Scalability Considerations

When operations, applications and technology evolve, the underlying network infrastructure needs to adapt to support those changes. Adaptability is the ability for the network to adjust to changes in the environment and requirements. Extensibility is the ability to add new features to the network or extend the network to new locations. Scalability is the ability to increase the network's ability to handle increased demand in terms of throughput, number of connected devices and/or area of coverage. Reliable networks do more than just transmit data without error and within a specified time. Reliable networks need to be able to adapt to changing security and safety policies. They should be able to extend functionality to address future requirements which may include an increased data rate, stricter latency requirements, and/or scalability in area of coverage and number of devices connected.

3.3.4 Physical Security Considerations

The physical security of communication technology plays a crucial role in maintaining its reliability, particularly by preventing unauthorized access that can lead to intentional disruptions or manipulations. Securing communication network equipment is essential to ensure that unauthorized individuals are unable to make alterations to these devices. Physical security measures work synergistically with cybersecurity defenses, providing an additional layer of security by restricting physical access to critical network hardware.

One significant distinction between wired and wireless networks lies in their vulnerability to physical security risks. Wired networks offer enhanced physical security due to the use of cables (e.g., wire or fiber) to transmit signals, making them less susceptible to unauthorized interception or manipulation. However, they still require robust physical safeguards to prevent tampering with the network infrastructure.

In contrast, wireless networks are inherently less physically secure, as signals are transmitted through the air rather than through physical cables. This mode of communication introduces distinct challenges, necessitating specialized controls to mitigate risks such as signal interference, jamming, unauthorized signal collection, signal manipulation, or even safety concerns posed by signal exposure. Effective mitigation strategies for wireless networks include measures such as ensuring sufficient distance between unauthorized users and network equipment, as well as implementing robust shielding mechanisms.

Examples of physical security measures for wireless networks include the establishment of protective boundaries around sensitive areas, the use of shielded environments like containment zones, and leveraging existing physical barriers, such as the walls of buildings. These precautions help ensure that the wireless signal remains secure and does not compromise the integrity or functionality of the network.

3.4 Reliability Metrics Specific to Mobility/Wireless Devices

Wireless communications provide capabilities that wired networks do not. For example, mobility where a wireless device can physically move around without a cable being connected to it. As such, there are specific reliability metrics that need to be accounted for in wireless networks that do not necessarily have a one-to-one correlation in wired networks.

3.4.1 Mobility

Mobility is the ability for a wireless device to move around in a network. This mobility as well as the mobility of the entities around it create a complex and dynamic environment. From a reliability perspective it is important to consider if the wireless network provides acceptable coverage, meeting bandwidth and latency requirements, to all areas that the device will move around when the device relies on wireless connectivity.

3.4.2 Handoff

Handoff is the ability for a network to maintain a device's connection as it transitions from one wireless access point (i.e., the network's wireless connection point) to another wireless access point. Handoffs may involve a break-before-make transfer or simultaneous connection to more than one access point during the transition. Handoffs are what make it possible for a wireless network to consist of more than one radio and provide coverage beyond what a single radio can cover. The reliability of a successful handoff is important for the device to maintain normal communications. Failed handoffs can cause dropped calls on cellular networks and force a device to reconnect to the network. Handoffs, either successful or failed, take time and can introduce additional latency during the handoff, which could have adverse effects on certain applications.

3.4.3 Number of Devices in a Specific Region

The scalability of a network, i.e., the total number of devices in a network, applies both to wired and wireless networks. Further, not all networks are built homogeneously and as such certain locations may support a larger number of devices than others. The big difference and why this is called out specifically here is that for wired networks the limit is physically imposed by the number of cables connecting to that network. Whereas, for wireless networks, the user rarely knows the design limit and can keep adding more wireless devices without fully understanding the impact an additional device has on another device. Congestion of wireless networks can cause challenges from increased latency and reduced bandwidth to not being able to successfully connect to the network. For cellular networks large events can cause significant congestion wherein devices may not be able to connect to the network. It is common for planned events that cellular providers deploy temporary cell sites to manage the additional load. Further, prioritizing critical devices such as those of first responders in the cellular network can mitigate the impacts that the network congestion can create for critical wireless connections.

3.4.4 Environmental Concerns

Environmental concerns for wireless devices from a reliability perspective include the signal-to-noise type of concerns as outlined in Section 3.1.1 as well as impacts the device may have on the environments it will be exposed to. For example, intrinsic safety requirements may apply in environments with flammable or explosive gases. Environmental concerns may also

include seismic events, vibration, and other mechanical stresses that affect device mounting, connectors, antennas, or any cabling associated with the wireless device.

4.0 Simulation/Emulation Capabilities

There are several different wireless simulation/emulation capabilities that can be used to assess the reliability of a wireless network. When choosing a capability, it is important to assess the level of simulation fidelity it provides. Simulation fidelity is the degree to which a simulation replicates the realism of the actual environment as well as the system or situation being simulated. The lowest fidelity level allows users to place wireless devices, and the simulation assumes a given bit-rate-error without being influenced by the wireless signals of other devices interfering with each other. Simulations are executed with minimal realism.

The highest simulation fidelity would be a digital recreation, digital twin, of a facility where the facility and equipment in the facility are modeled with the materials of the real items. A wireless network (with digital equivalents of the antennas) and wireless devices would be placed throughout the digital twin. Any environmental concerns that would be expected (e.g., smoke, fog, etc.) could be added to the simulation. The digital twin would then operate with the expected communication patterns of life as a real facility and put through the various modes of operation with normal and possible off-normal operations. Wireless device failures could be simulated to understand the impacts caused by specific devices going offline.

For example, NS-2 (ns-2 Project 2026), GNS3 (GNS3 2026), NetSim (NetSim 2026), and MATLAB (MATLAB 2026) have the lower fidelity type simulation capabilities when it comes to wireless networks, some of these are top tier for wired networks. This is because these simulators have limited wireless network simulation capabilities and are unable to simulate the wireless signal propagation, environmental effects and interference.

Examples of middle to high fidelity include, NS-3 (Prakash and Abdrabou 2020, ns-3 Project 2026) and OMNeT++ (OMNet++ 2026). These are both open-source network simulators and are constantly being enhanced with new capabilities by the community. The standard capabilities for wireless networks for these have become middle to high fidelity depending on which modules are used. These typically provide wireless physical layer simulation with propagation using path loss models for different environmental effects. Structures and mobility can be simulated using NS-3 (Prakash and Abdrabou 2020, NS-3 Project 2026) with the Buildings model or OMNeT++ (OMNet++ 2026) with the INET framework (Khana et al. 2013).

The most sophisticated and highest fidelity wireless simulators include offerings such as those from Ansys (Ansys 2026), and NVIDIA (NVIDIA 2026) as well as WiSE. These companies offer simulators with capabilities where the physical space is created as a digital twin and the simulation of the signals from the wireless devices interact with the digital world. This is as close as it comes to the real-world simulation, as multiple devices will interact with each other as well as the environment (e.g., smoke, fog, etc. can be added). While these wireless simulators provide some of the most advanced capabilities there are limitations in the assumptions they make. For example, ray-tracing has challenges in simulating the wireless effects on rough surfaces since absorption and reflection of certain materials are different. Specific geometries also create challenges for the simulators as light and RF behave differently (Wang 2024).

Due to the limitations of even the most advanced simulators/emulators it is important to perform real-world testing. Real-world testbeds and onsite testing are the only way to truly understand the behavior of a wireless network in a given environment and should likely be required for applications that involve important to safety and safety-related networks. Simulation is important and a good place to test ideas and gain a better understanding of optimal placement of wireless access points. Simulation-based data can guide real-world testing so the safety of a system can be determined.

5.0 Network Types and Wireless Use Cases

5.1 Nuclear Network Classes

This section provides a high-level overview of different network classes that exist at nuclear facilities.

5.1.1 Non-Safety Network

Non-safety networks are a group of networks that connect computers and people, where the equipment operates on the network and communications sent across the network have limited impact on the immediate safety of the people and facilities. This includes networks such as information technology networks, which are the networks used for business functions of the network. The reliability of these networks has little impact on safety. However, network disruption can create inconveniences. If any of the following components are part of a different system type, then the networks that support them will be included in the other network class. For example, if a phone is used in the event of a safety related off-normal event, the phone's network would be part of the safety network.

Examples include but are not limited to:

- information technology business networks: billing, payroll, human resources, training, asset tracking, shipping/receiving
- email
- phone system for office workers
- internet access
- video teleconferencing

5.1.2 Monitoring/Operational Networks

System monitoring networks are a step above information technology networks when it comes to operational risks. These networks connect devices that provide information back to a central location to track trends and maintenance of facilities. The information gathered by these systems is not automatically acted upon and a human interprets the data before acting. As such, if the network goes down for a period, there must not be an increase in risk to life or operations. Further, these systems pose limited threats to human life and no threat to critical facility operation if they fail.

Examples include but are not limited to:

- networks that connect monitoring equipment, e.g., enabling predictive maintenance with external/secondary sensors or non-critical components
- connectivity for non-critical "secondary" facility operations such as leak detection for a kitchen, bathroom, etc.
- connecting radiation-based exit scans of people where scan results are sent to a central repository for accounting purposes (note that nothing is acted on in real time, wherein if a network is down, then data can be sent when a network is back up or a person can manually go and collect measurements)

- enabling a digital twin for monitoring that is used only to collect data about the environment and which allows a human decision-maker to collect the data necessary to understand operations at a facility.

5.1.3 Security Network

Security and access control networks are the networks that provide communications for equipment and personnel that protect the facility. These include any proximity card readers, electronic locks, camera and sensor systems for security purposes, and potentially voice and messaging between security personnel. These systems and the networks around them provide physical security that monitor the facility and provide access to only authorized individuals and are inherent to providing the safe operation of a facility. These networks must be reliable for the security of the system and as such must indirectly be reliable to secure a site from unauthorized access that could impact the safety of the facility.

5.1.4 Important to Safety Network

Important to safety networks are networks that are not used directly for safety systems but instead provide networking to systems that support or complement safety-related systems and networks. The networks provide communications for structures, systems and components that are not used directly for safety systems and provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the public.

5.1.5 Safety-Related Network

Safety-related networks support communication between systems, structures, components or humans to support procedures and controls that must remain functional during and following design-basis events. The functionality of these systems, procedures and controls ensure safe operations and ensure that key regulatory criteria are met, such as levels of radioactivity release (U.S. Nuclear Regulatory Commission 2021).

5.1.6 Proposed Wireless Communication Use-Cases

Many use-cases for wireless communications have been proposed where wireless communications are envisioned to enable new processes and procedures for the nuclear industry and reduce the lifecycle cost of operating facilities. Examples of proposed use-cases can be found in (Pulgarin et al. 2024), one such use-case proposed is to augment the refueling control system with wireless communications. (Muhlheim et al. 2023) provide a wish list of wireless application in nuclear power plants which include but are not limited to: wireless data retrieval, movable wireless cameras, movable temporary wireless measurements during maintenance, wireless dosimeter system across the plant, movable wireless detectors for radiation, gas or oxygen levels, wireless document retrieval during inspections, and wireless emergency response systems.

To reduce the risk of using wireless communications, it may be possible to limit their use to key time periods or locations, such as using wireless for the connection from suitable digital processing or aggregation equipment associated with sensors in a containment building to a remote monitoring facility, rather than implying direct wireless connection to analog sensor elements. Suitability would depend on the radiation environment, shielding, qualification, and the specific function being supported. Another example includes using an array of heterogeneous sensors to measure the energy produced by a micro-reactor to supply process

heat as opposed to electricity. Here, wireless communications can be used to reduce wiring at the facility and connect suitable digital processing and aggregation equipment, or secondary monitoring devices to a local aggregation point. Wireless communications could also be used to connect a facility located in a remote area (e.g., the Arctic) to a central monitoring station.

Finally, wireless communication can support remote monitoring of small modular reactors (SMRs) in a variety of ways, which can in turn help power communities on small islands and in the Arctic, for example, or in other remote locations such as mining camps, or supply process-heat or power to cargo ships (World Nuclear News 2025, Pacific Forum International 2022, World Nuclear News 2023, World Nuclear News 2025, Natural Resources Canada 2025). The remote location or mobile nature of many of these applications for SMRs presents a challenge for monitoring the SMRs in a scalable way. However, wireless advances such as LEO satellite communications could provide solutions where wired networks cannot when it comes to SMRs.

5.2 Wireless Use Case Topology

5.2.1 "Last Mile" Wireless

Last Mile wireless use cases are where wireless is used to make the final communication link between the network and the end-device. For example, Last Mile networks include cellphone to cell tower or laptop to Wi-Fi Access Point link.

Examples of Last Mile wireless communication use may include:

- use cases where mobility is needed, such as an underwater autonomous vehicle with sensors monitoring storage or spent nuclear fuel.
- places with limited concern for wireless signal propagation due to strong physical security. Examples may include wireless communications in a shielded room—radiation protection, personal radiation detectors, live telemetry of personal radiation detectors throughout the facilities.
- wireless communications used to retrofit new functionality: examples may include containment—facility surrounding the reactor "reactor core, containment," building with negative pressure, spent nuclear fuel cooling, and tower cooling for boiling water reactors.
- wireless communications beyond where wired networks currently exist. Examples may include wireless access outside the fence at the physical boundary, such as, radiation air monitoring outside the facility to track emissions.

5.2.2 Backhaul Wireless

A backhaul network connection provides the connection between a facility and the larger network, e.g., the internet connection at a house provides the backhaul connection for the house.

Examples where backhaul wireless may be useful include:

- mobile or remote SMRs.
- as a secondary or backup network connection. For example, floating nuclear reactors when using a wired backhaul connection can have a reduction in physical security compared to a

wired network connecting it to land. Wireless networks have no cables to cut and could be used to reduce the risk of using the wired network in this type of application.

6.0 Comparison with Wired Data Links

6.1 Communication Reliability

Wired and wireless network links can be compared using common metrics. For example, metrics may include bandwidth, throughput, jitter, packet loss, error rates, bandwidth utilization, one-way latency, round-trip latency, network availability, and retransmission rate. These metrics work well when comparing a single link in a network, agnostic to the application, and agnostic to the technology for wired or wireless communications being used. This type of comparison may be sufficient for a bump-in-the-wire network link, wherein the link exchange does not affect the underlying network topology. This type of switch is replacing a single wired link with a wireless link and as long as the comparison includes the different potential environments (smoke, fog, dust, aerosols, etc.) that the wireless link may be exposed to, this simplistic comparison should be a valid measurement. This is because at a link level, the reliability of the networks should be easily compared using these metrics.

While the metrics above can compare two links, if the network change is larger than replacing the single link, e.g., using Wi-Fi or 5G, then an application-based comparison will be needed. This is because the comparison is across networks composed of multiple layers of protocols and the different protocols may behave differently based on the underlying technology.

6.2 Effects of Wireless of Other Devices

Any comparison between wired and wireless communication approaches should account not only for communication performance, but also for whether wireless emissions could adversely affect nearby equipment or instrumentation. This includes evaluating transmitter location, expected field strength at nearby devices, antenna characteristics, and whether susceptible equipment could respond differently in the presence of the wireless signal.

6.3 Hardware/Infrastructure Reliability

A comparison of the hardware error rates, expected lifetime, and technology lifecycle is necessary to properly compare the two networks. This includes any wires needed for communications as well as power. Further, it is important to understand how the expected environment and use-cases will affect the wear and tear on the equipment and infrastructure.

6.4 Functionality, Upgradability, Extensibility and Cost

When comparing the two technologies it is important to also consider the functionality, upgradeability, extensibility and cost. Wireless networks provide features such as ease of installation and mobility that wired networks cannot match. A comparison should also include an assessment of how easy it is to upgrade technology or extend it to new applications. Finally, comparing the cost of the two networks, including the cost to install the networks along with any trenching, retrofitting, licensing costs, is necessary when comparing the wired and wireless networks.

7.0 Developing Wireless Reliability Metrics and Assessments

A network reliability assessment can use a probabilistic method, or a PRA-informed type of analysis where appropriate, to evaluate communication reliability. There are two main considerations: (1) the frequency of a message being received outside of the reliability metrics, or key performance indicators (KPIs) for a given application, and (2) the frequency that the communication network has an undesirable effect on a different system, e.g., a wireless signal causing a different component to malfunction.

7.1 Frequency of Messages Being Received Outside of the KPIs

KPIs need to be developed for an application using the metrics defined in Section 3.0. This will define KPIs such as required network throughput, maximum latency, maximum jitter, maximum error rates, etc. The KPIs need to start at the application layer and work down from there until KPIs are defined for the underlying network technology. This is because each layer in the network affects the overall throughput, latency, retries, etc. and small changes in the network configuration/load can significantly affect network performance and reliability for a given set of applications. For example, the maximum transmission unit (MTU) can have significant effects on the throughput of a network as well as error rates. Similarly, transmission control protocol window size can affect both the throughput and reliability on a network.

KPIs can initially be developed for a wireless network by using the corresponding wired network as a baseline if a wired network is already in use for a given application. Using this method the wired network's KPIs can be developed for each network layer. It is important to perform a comparison between the wired and wireless technologies at each network layer to understand the effects different solutions or configurations may have on a network. For example, 1,500 MTU is commonly used for IPv4 ethernet based networks, allowing for 1,500 bytes to be transmitted per packet. However, on 5G it is common that a smaller MTU is used, such as 1,420 or 1,428 MTU (Digi International 2024). In these cases, if a 1,500 byte packet is sent along and encounters a 5G link, the packet will be split into two fragments: one that maximizes the smaller MTU of the 5G link and a second packet for any data that is left over. This fragmentation can have significant effects on network performance and is an example of why it is important to perform an analysis between all layers of the network to ensure that the wireless network provides equivalent capabilities to the wired counterpart.

KPI acceptance criteria should include appropriate margin based on the application, network complexity, and a degree of determinism. For a single link supporting a predictable application load, less margin may be needed. For a shared, dynamic or less deterministic network, additional margin or compensatory controls such as QoS, redundancy, or deterministic networking may be appropriate.

Once KPIs are defined for the network at each layer from application down to the underlying network technology, estimations for a network's performance can be created from the underlying network technology up to the application. Estimations of network performance may be statistical modeling given the expected performance of network technology, simulation/emulation of the network, hardware in the loop testbed testing or test and evaluation of equipment before switching over to the network. The network performance should be

measured in a way that each KPI defined can be evaluated against the measured network's performance. Further, the network performance should be evaluated with nominal conditions as well as off-normal conditions to understand how the network performance is affected given specific events.

Using this data, a probabilistic reliability evaluation, or a PRA-informed evaluation where appropriate, can be used to estimate the likelihood that messages are received outside the desired KPIs. This will provide an understanding of the network's communication reliability. Further analysis will be required to assess the network's fault tolerance and whether any single points of failure exist. Standard methods for fault tolerance and single-points-of-failure analysis should be paired with the KPI evaluation to determine the effects that redundancies may have on the network.

7.2 Frequency that the Communication Network has an Undesirable Effect on Other Systems

The second factor to consider when evaluating the safety and reliability implications of a potential wireless network application for a nuclear facility is the effect the wireless network may have on existing infrastructure.

Further, TLR-RES-DE-2023-006 states that licensees do not have to rely on exclusion zones and can propose alternative methods to ensure protection of the safety system. These alternative methods may include site surveys or simulations to develop controls for wireless use. As such, the tools discussed in Section 4.0 could be utilized to create alternative controls instead of the exclusion zone distance calculations, which may not cover the specific scenario (e.g., light based wireless or higher frequency without data backing up the exclusion zone calculation).

8.0 Conclusion

This report evaluates methods for assessing the reliability of wired and wireless digital communication networks to inform future application-specific evaluations for nuclear facilities. This study presents a framework tailored to address reliability tradeoffs for potential wireless network applications in the context of safety, security, and monitoring functions. The authors propose the use of consensus standards to create performance-based assessments when evaluating wireless reliability as opposed to using rigid regulations.

The primary rationale for considering wireless networks is to provide operators with flexibility, cost-effectiveness and connectivity to remote locations. Wired networks provide a known transmission medium (e.g., copper cable or fiber) that provides physical security with shielding. Because wireless networks do not have a known transmission medium and require added physical security, the main questions from a safety perspective regarding the use of wireless networks revolve around the reliability of the wireless network connection and the impacts that a wireless network may have on other components in an operating facility.

Wireless network technologies have advanced significantly in the last few years and can meet or exceed older wired networking technologies in terms of performance. However, comparative analyses studying the reliability of wired vs. wireless networks are needed to understand the safety basis impacts for a facility in a scenario where a wireless network would replace a wired network.

Potential use of wireless networks for nuclear facility applications would require stringent reliability metrics and risk assessments for each application. Probabilistic reliability methods, supported by wireless performance and error metrics, can be used to estimate message failure likelihood for a given wireless link or network layer. Similar probabilistic evaluations can be applied at each network layer to understand the impact of each protocol on the underlying KPIs of the network and how it affects overall reliability. Simulation and over-the-air, real-world testing can be used to validate the calculations performed in the probabilistic analysis. Simulations and exclusion zone calculations can help inform decision makers about the impact wireless communications may have on other components in the nuclear facility and decision makers can utilize alternative site-specific controls to mitigate potential risks. Finally, from a safety perspective, the cybersecurity of a wireless network should be properly addressed, as the risk of a loss of confidentiality, integrity, availability, and unauthorized access can create safety concerns.

9.0 References

Ansys. 2026. “5G/6G The Future of Intelligent Connectivity.” Accessed January 26, 2026. https://www.ansys.com/technology-trends/5g.

Digi International. 2024. “Recommended MTU/MRU Settings on Cellular Networks.” *Digi International Support Knowledge Base*. Accessed January 26, 2026. https://www.digi.com/support/knowledge-base/recommended-mtu-mru-settings-on-cellular-networks.

Eaton. 2026. *“*Ethernet Cables Explained.*”* Accessed January 20, 2026. https://tripplite.eaton.com/products/ethernet-cable-types.

Galati-Giordano, L., G. Geraci, M. Carrascosa, and B. Bellalta. “What Will Wi-Fi 8 Be? A Primer on IEEE 802.11bn Ultra High Reliability.” *IEEE Communications Magazine* 62, no. 8 (August 2024): 126–132. https://doi.org/10.1109/MCOM.001.230072.

GNS3. 2026. “GNS3 Version 2.2.56 available.” Accessed January 26, 2026. https://www.gns3.com/.

IEC 192-01-22. 2026. “Electropedia” Accessed January 26, 2026. https://www.electropedia.org/iev/iev.nsf/display?openform&ievref=351-49-06.

IEC 351-49-06. 2026. “Electropedia” Accessed January 26, 2026. https://www.electropedia.org/iev/iev.nsf/display?openform&ievref=351-49-06.

IEEE. 2016. *IEEE Standard for Low-Rate Wireless Networks.* IEEE Std 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011), 1–709. New York: IEEE, April 22, 2016. https://doi.org/10.1109/IEEESTD.2016.7460875.

International Engineering Task Force (IETF). 2025. *“*Reliable and Available Wireless Architecture.*”* Internet-Draft draft-ietf-raw-architecture-30 (Informational), edited by Pascal Thubert, last updated December 22, 2025, expires January 26, 2026. Accessed January 20, 2026. https://datatracker.ietf.org/doc/draft-ietf-raw-architecture/.

Internet Engineering Task Force (IETF). 2026. “Deterministic Networking (detnet) Working Group — About.*”* IETF Datatracker. Accessed January 20, 2026. https://datatracker.ietf.org/group/detnet/about/.

Khana, Atta ur Rehman, Sardar M. Bilal, and Mazliza Othman. “A Performance Comparison of Network Simulators for Wireless Networks.” *arXiv*:1307.4129 (July 15, 2013). https://arxiv.org/abs/1307.4129.

Kuiper. 2026. Accessed January 26, 2026. “Amazon LEO.” Accessed February 12, 2026. https://www.aboutamazon.com/what-we-do/devices-services/amazon-leo

MATLAB. 2026. “wirelessNetworkSimulator.” Accessed January 26, 2026. https://www.mathworks.com/help/comm/ref/wirelessnetworksimulator.html.

Muhlheim, M. D., L. A. Hardin, and R. J. Belles. 2023. *Criteria for Determining the Safety of Wireless Technologies at Nuclear Power Plants*. Oak Ridge National Laboratory, report for the U.S. Nuclear Regulatory Commission. https://www.osti.gov/servlets/purl/1996676.

National Aeronautics and Space Administration. 2017. *NASA-STD-8729.1A: Reliability and Maintainability Standard for Spaceflight and Support Systems*. Washington, DC: NASA, June 13, 2017. PDF file. https://s3vi.ndc.nasa.gov/ssri-kb/static/resources/nasa-std-8729.1a.pdf.

Natural Resources Canada. 2025. "Small Modular Reactors (SMRs) for Mining." *Natural Resources Canada*. Accessed January 26, 2026. https://natural-resources.canada.ca/energy-sources/nuclear-energy-uranium/small-modular-reactors-smrs-mining.

NetSim. 2026. "NetSim Network Simulator." Accessed January 20, 2026. https://netsim.boson.com/.

ns-2 Project. 2026. "The Network Simulator – ns-2." Accessed January 20, 2026. https://www.isi.edu/websites/nsnam/ns/.

ns-3 Project. 2026. "ns-3 Network Simulator." Accessed January 20, 2026. https://www.nsnam.org/.

NVIDIA. 2026. "Developing Next-Generation Wireless Networks with NVIDIA Aerial Omniverse Digital Twin." Accessed January 26, 2026, https://developer.nvidia.com/blog/developing-next-gen-wireless-networks-with-nvidia-aerial-omniverse-digital-twin/.

OMNeT++. 2026. "Discrete Event Simulator." Accessed January 26, 2026. https://omnetpp.org/.

Pacific Forum International. 2022. *Small Modular Reactors: The Next Phase for Nuclear Power in the Indo-Pacific?* Issues & Insights Vol. 22, SR4. Honolulu, HI: Pacific Forum International. https://www.pacforum.org/wp-content/uploads/2022/08/V2-FINAL_II_SMRStudy.pdf.

Prakash, Monika, and Atef Abdrabou. "On the Fidelity of NS-3 Simulations of Wireless Multipath TCP Connections." *Sensors (Basel, Switzerland)* 20, no. 24 (December 18, 2020): 7289. https://doi.org/10.3390/s20247289.

Pulgarin, E. J. L., G. Herrmann, C. Hollinshead, J. May, K. N. Gebremicael, and D. Daw. 2024. "Towards Wireless Communication in Control Systems of the Civil Nuclear Energy Sector." *Annual Reviews in Control* 57: Article 100936. https://doi.org/10.1016/j.arcontrol.2024.100936.

Starlink. 2026. "Reliable High-Speed Internet from Space." Accessed January 20, 2026. https://www.starlink.com/.

Taara Connect, Inc. 2026. "Taara." Accessed January 20, 2026. https://www.taaraconnect.com/.

U.S. Nuclear Regulatory Commission. 2019. *Regulatory Guide 1.180, Revision 2: Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems*. Washington, DC: U.S. Nuclear Regulatory Commission. Accessed January 26, 2026. https://www.nrc.gov/docs/ML1917/ML19175A044.pdf.

U.S. Nuclear Regulatory Commission. 2021. "Safety-related." Accessed January 26, 2026. https://www.nrc.gov/reading-rm/basic-ref/glossary/safety-related.

U.S. Nuclear Regulatory Commission. 2023. *Criteria for Determining the Safety of Wireless Technologies at Nuclear Power Plants*. TLR-RES-DE-2023-006. Washington, DC: U.S. Nuclear Regulatory Commission. Accessed January 26, 2026. https://www.nrc.gov/docs/ML2322/ML23222A166.pdf.

Wang, Ruofei, Samuel Audia, and Dinesh Manocha. "Indoor Wireless Signal Modeling with Smooth Surface Diffraction Effects." In *Proceedings of the 18th European Conference on Antennas and Propagation (EuCAP)*, 1–5. Glasgow, United Kingdom, 2024. https://ieeexplore.ieee.org/document/10501079.

World Nuclear News. 2023. "Partnership Formed to Deploy Seaborg's Power Barge." *World Nuclear News.* April 21, 2023. https://www.world-nuclear-news.org/articles/partnership-formed-to-deploy-seaborg-s-power-barge.

World Nuclear News. 2025. "Nordic Partnership for SEALER SMR Deployment." *World Nuclear News*, February 26, 2025. https://www.world-nuclear-news.org/articles/nordic-partnership-for-sealer-smr-deployment.

World Nuclear News. 2025. "Thorcon Applies to Build Indonesia's First Nuclear Power Plant." *World Nuclear News.* March 5, 2025. https://www.world-nuclear-news.org/articles/thorcon-applies-to-build-indonesias-first-nuclear-power-plant.

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354
1-888-375-PNNL (7665)

www.pnnl.gov* | *www.nrc.gov