

New generation of smart sensor WLANs

Zoltán Kiss Chief Development Officer

¹ *Endrich Bauelemente Vertriebs GmbH D-72202 Nagold Hauptstrasse 56.
z.kiss@endrich.com*

Abstract

Modern smart sensor systems are increasingly connected through well-established communication philosophies such as cellular IoT and Wi-Fi. These technologies offer clear advantages where infrastructure, bandwidth, and direct cloud access are available. However, many industrial, environmental, and large-area sensing applications require a different approach: low-power, long-lasting, self-forming sensor wireless local area networks that can operate reliably without dense infrastructure. This presentation discusses the technical and economic advantages of distributed sensor WLAN architectures such as NeoMesh. By using signal-friendly sub-GHz frequency bands and, where necessary, error-resilient modulation schemes such as LoRa within a local mesh network, node-to-node communication distances can be significantly extended while maintaining very low energy consumption. Such systems open new perspectives for robust, scalable sensor networks capable of covering large areas with thousands of nodes, while still meeting the strict European duty-cycle requirements. The paper compares point-to-point, multipoint-to-point, and distributed mesh communication technologies, highlighting their operational principles, scalability limits, energy behavior, and economic impact. Special attention is given to operational safety, reliability, data availability, and security-related aspects in real-world deployments. The goal is to provide a practical decision framework: when cellular or Wi-Fi connectivity is the right choice, and when a distributed mesh sensor network provides superior performance, lifetime, coverage, and cost efficiency. The presentation positions smart sensor WLANs not as a replacement for existing technologies, but as a complementary architecture for the next generation of resilient industrial sensor networks.

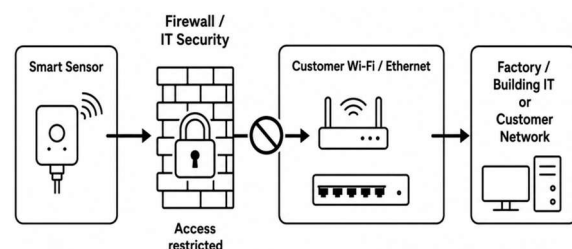
Keywords: Smart Sensor WLANs, Distributed Mesh Networks, NeoMesh, Low-Power Wide-Area Sensing, Sub-GHz Wireless Communication

Introduction – Smart Sensors, Connectivity, and Cloud-Oriented System Thinking

Smart sensors are becoming key building blocks of modern industrial, environmental, infrastructure, and building-monitoring systems. Their role is no longer limited to measuring a physical quantity. A smart sensor also identifies itself, preprocesses data, manages its own energy budget, communicates with higher-level systems, and contributes to a larger digital information chain. For this reason, the selection of the wireless communication technology is not only a radio-design question, but a system-level architectural decision.

In many applications, Wi-Fi or wired Ethernet may appear to be the simplest connectivity options. They are widely available, well understood, and suitable for high-bandwidth data transmission. However, in real industrial and commercial deployments, they often introduce serious practical limitations. The local network usually belongs to the owner or operator of the building, factory, supermarket, or infrastructure. From an IT security point of view,

external sensor devices are frequently not allowed to connect to the customer's Ethernet or Wi-Fi network. Firewall rules, access credentials, network segmentation, cybersecurity policies, and maintenance responsibilities can make such integration difficult or even impossible.



A more independent approach is to integrate cellular connectivity directly into the sensor device. In this point-to-point architecture, each sensor can communicate directly with the cloud without using the customer's local IT infrastructure. For low-power sensor applications, cellular LPWAN technologies such as NB-IoT and LTE-M are especially relevant. They offer long battery lifetime, wide-area

coverage, standardized 3GPP operation, SIM or eSIM-based authentication, and international usability. Their limited bandwidth is usually not a disadvantage for sensor systems, because most sensor payloads are small and consist of measured values, status information, alarms, or event messages.

However, smart sensor connectivity should not be evaluated only by the communication link itself. The real value of the system is created by the complete data chain:

Sensor → Connectivity → Cloud → Data Processing → Data Display → AI-supported interpretation

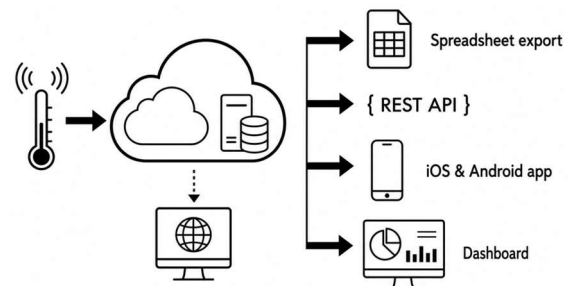


In this architecture, the cloud is not only a storage location. It becomes the central processing and intelligence layer of the sensor system. It validates and stores incoming data, creates historical records, generates alarms, supports dashboards, and enables AI-based functions such as anomaly detection, trend recognition, natural-language data analysis, and predictive maintenance support. The final goal is not simply to transmit data, but to transform physical measurements into meaningful operational knowledge.

This leads to the central question of this paper: if individual sensors can already communicate directly with the cloud through cellular LPWAN, why are distributed smart sensor wireless local area networks still needed? The answer lies in scalability, energy efficiency, deployment cost, radio coverage, network robustness, and the ability to connect large numbers of low-power nodes over extended local areas. Distributed sensor WLANs, especially self-forming mesh systems operating in signal-friendly sub-GHz frequency bands, can offer significant technical and economic advantages when many sensors must cooperate within one local or regional sensing environment.

The following chapters, therefore, examine two complementary connectivity philosophies. First, the paper discusses direct point-to-point cellular LPWAN connectivity using NB-IoT and LTE-M, including its advantages, limitations, and ideal use cases. Second, it introduces distributed smart sensor WLAN architectures such as NeoMesh, where many low-power nodes form a robust local network and forward data through one or more gateways to the cloud. Together, these two approaches form the basis for a

practical decision framework: when to use direct cellular smart sensors, and when a distributed sensor mesh network provides the better system-level solution.



Direct Cellular LPWAN Connectivity for Smart Sensors

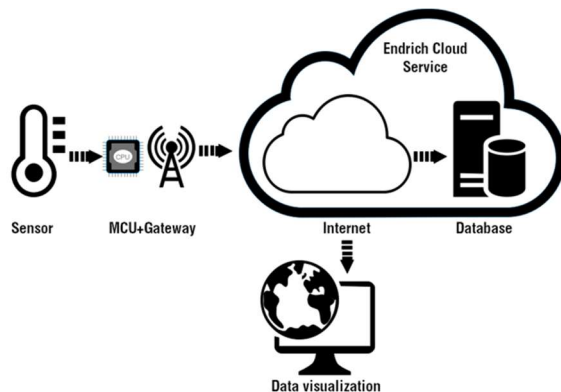
One of the most straightforward architectures for a wireless smart sensor is the direct point-to-point connection between the sensor and the cloud. In this concept, the sensor device contains not only the sensing element and the local microcontroller, but also an embedded cellular modem. The complete communication path is therefore independent from the local building, factory, or customer IT infrastructure. The device measures, preprocesses, packages, and transmits its data directly to a cloud endpoint through the mobile network.

This approach is especially attractive in industrial and commercial environments where access to local Ethernet or Wi-Fi networks is restricted. In many factories, supermarkets, logistics centers, public buildings, and infrastructure sites, the local network is owned and controlled by the real-estate owner, facility operator, or corporate IT department. Connecting external sensors to this network may be forbidden for cybersecurity reasons or may require complex approval procedures, firewall configuration, VLAN separation, credential management, and long-term IT support. In such cases, the technical availability of Wi-Fi or Ethernet does not automatically mean that they are practically usable.

Cellular connectivity solves this problem by making the smart sensor an autonomous communication endpoint. The sensor does not need the customer's router, Wi-Fi password, firewall rules, or local network maintenance. It only needs mobile network coverage, a suitable antenna, and a SIM- or eSIM-based connectivity service. From a system-integration point of view, this independence is a major advantage. It allows the sensor manufacturer or solution provider to control the complete communication chain from the device to the cloud.

For smart sensor applications, however, the most suitable cellular technologies are usually not classical broadband 4G or 5G solutions.

Most sensors do not need high data rates. They transmit small payloads such as temperature, humidity, pressure, vibration, door status, battery voltage, alarm states, counter values, or diagnostic information. For this reason, cellular LPWAN technologies such as NB-IoT and LTE-M are often better suited. GSMA defines Mobile IoT as low-power wide-area solutions in licensed spectrum, and its Mobile IoT initiative focuses on the commercial availability of such LPWA technologies for IoT applications.



NB-IoT, or Narrowband IoT, is a standards-based LPWA technology designed for a wide range of low-power IoT devices and services. Its key strengths are low device power consumption, improved system capacity, spectrum efficiency, and deep coverage. GSMA notes that NB-IoT can support battery lifetimes of more than ten years for a wide range of use cases, depending on configuration, traffic profile, and operating conditions. This makes NB-IoT highly suitable for stationary sensors, metering systems, environmental monitoring, infrastructure supervision, and applications where the device sends small amounts of data at relatively long intervals.

LTE-M, also known as LTE Cat-M1, follows the same cellular LPWAN philosophy but offers a somewhat different balance of capabilities. GSMA describes LTE-M as the simplified industry term for LTE-MTC, a 3GPP Release 13 LPWA technology standard, suitable for IoT devices with lower device complexity and extended coverage while reusing the installed LTE infrastructure. Compared with NB-IoT, LTE-M is generally more suitable when the application requires higher data rates, lower latency, mobility support, or more practical over-the-air firmware updates. AWS summarizes the engineering difference clearly: LTE-M tends to provide higher data rates, lower latency, better energy efficiency for larger payloads, and better suitability for mobile applications, while NB-IoT is often attractive for very small payloads and static devices.

From a design point of view, this means that NB-IoT and LTE-M should not be seen as competitors where one is always better than the other. They are two optimized tools within the same cellular IoT family. NB-IoT is often the better choice for very low-data-rate, long-lifetime, stationary applications where deep indoor or remote coverage is important. LTE-M is often the better choice for moving assets, more frequent communication, lower latency, larger payloads, and devices that may require firmware updates during their lifetime.

Aspect	NB-IoT	LTE-M
<i>Typical sensor profile</i>	<i>Static or rarely moving</i>	<i>Static or mobile</i>
<i>Payload size</i>	<i>Very small, infrequent data</i>	<i>Small to medium IoT payloads</i>
<i>Latency requirement</i>	<i>Usually not critical</i>	<i>More suitable for lower latency</i>
<i>Mobility</i>	<i>Limited</i>	<i>Better mobility support</i>
<i>Firmware update practicality</i>	<i>Possible but more limited</i>	<i>More practical</i>
<i>Best fit</i>	<i>Metering, environmental sensing, infrastructure monitoring</i>	<i>Asset tracking, mobile sensors, alarm devices, more interactive IoT nodes</i>

A major strength of both technologies is that they operate within the 3GPP ecosystem. This means that they benefit from standardized cellular infrastructure, licensed spectrum, operator-managed networks, and SIM-based authentication. Compared with many non-cellular LPWAN systems, this can provide an important advantage for international deployments. A device designed with the correct frequency-band support and a suitable connectivity provider can often be deployed across multiple countries without the solution provider having to build and maintain its own local gateway infrastructure.

The commercial ecosystem has also matured significantly. GSMA's Mobile IoT deployment resources show commercial launches for both NB-IoT and LTE-M, and its deployment map distinguishes countries with NB-IoT only, LTE-M only, or both technologies. The map was last edited in April 2026, while GSMA's commercial launch summary listed 129 LTE-M networks, 140

NB-IoT networks, and 269 total Mobile IoT networks in its November 2025 update. For system designers, this does not remove the need to check local operator availability, roaming, frequency bands, and certification requirements, but it shows that cellular LPWAN is no longer an experimental niche technology. It is a commercially deployed connectivity layer for professional IoT systems.

The economic model of direct cellular LPWAN sensors is also increasingly attractive. Low-cost IoT SIM cards, prepaid connectivity models, pooled data plans, and embedded SIM solutions reduce the entry barrier for smaller deployments. Since the payload of sensor applications is usually small, the monthly data volume per device can remain very low. In such cases, the operational cost is often driven less by the amount of transmitted data and more by subscription management, network availability, coverage, and the number of deployed devices. This last point is important. A direct cellular LPWAN architecture scales very well from one sensor to tens, hundreds, or even thousands of geographically distributed independent devices. Each device can be installed at a different site and communicate directly to the same cloud platform. This is ideal for distributed assets such as refrigeration units, containers, vending machines, utility meters, remote infrastructure, or mobile equipment. In these use cases, there may be no local concentration of sensors, and therefore no strong reason to build a local sensor network.

However, the same architecture becomes less efficient when many sensors are concentrated within the same local area. If hundreds or thousands of sensor nodes are installed in one factory, one agricultural area, one building complex, one city district, or one industrial site, equipping every single node with its own cellular modem and SIM subscription can become technically and economically inefficient. The modem increases device cost, antenna complexity, firmware complexity, power consumption, and certification effort. Each node also becomes individually dependent on cellular coverage and network registration.

This is where the limitation of the point-to-point cellular philosophy becomes visible. It is excellent for independent devices and geographically distributed assets, but it is not always the best solution for dense local sensor networks. In large local deployments, a more efficient approach may be to let many small, ultra-low-power sensor nodes communicate with each other in a local wireless sensor network and forward their data through one or more gateways. In this architecture, only the gateway needs cellular, Ethernet, Wi-Fi, or satellite

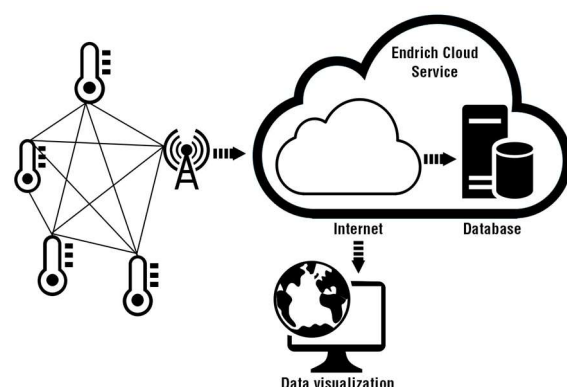
connectivity to the cloud, while the individual sensor nodes remain simpler, cheaper, and more energy efficient.

Therefore, direct cellular LPWAN connectivity should be understood as a powerful but specific smart sensor architecture. It provides independence from local IT infrastructure, strong cloud connectivity, standardized international operation, and excellent suitability for low-payload point-to-point sensor communication. Its ideal use case is the autonomous sensor node that must communicate directly with the cloud from almost any location.

The next chapter examines the complementary architecture: distributed smart sensor WLANs and mesh-based networks, where the goal is not to give every sensor its own wide-area modem, but to create a robust local network of cooperating low-power nodes.

Distributed Smart Sensor WLANs and Mesh-Based Architectures

While direct cellular LPWAN connectivity is an excellent solution for autonomous point-to-point sensor communication, it is not always the most efficient architecture for large local deployments. Many industrial, environmental, agricultural, building-monitoring, and infrastructure applications do not consist of single isolated sensors. Instead, they require tens, hundreds, or even thousands of sensor nodes distributed over a local or regional area. In such cases, the technical and economic question changes. The goal is no longer only to connect one sensor to the cloud, but to create a reliable, scalable, and energy-efficient local sensor communication system.



This is where distributed smart sensor wireless local area networks become highly relevant. In this concept, the individual sensor nodes do not necessarily communicate directly with the cloud. Instead, they communicate with each other through a local wireless network and forward their data toward one or more gateways. The gateway then provides the connection to the

cloud using cellular LPWAN, Ethernet, Wi-Fi, satellite communication, or another wide-area technology. The local network and the cloud connection are therefore separated into two functional layers.

This architecture brings an important system-level advantage. The sensor nodes can remain simple, low-cost, and ultra-low-power devices, while the more complex and energy-consuming wide-area communication is concentrated in the gateway. Instead of equipping every single sensor with its own cellular modem, SIM card, antenna system, and subscription, many local sensors share one or more gateway connections. This can significantly reduce device cost, power consumption, installation complexity, and long-term operating expenses.

A distributed smart sensor WLAN is especially useful when the physical sensing points are located within radio reach of each other, but the complete area is too large or too complex for a simple star network. In a classical star topology, every node must reach the gateway directly. This limits the usable area and makes the system sensitive to obstacles, antenna orientation, building structures, vegetation, terrain, or local interference. If one sensor is too far from the gateway, or if the radio path is blocked, the node may become unavailable.

Mesh networking solves this limitation by allowing nodes to forward data for each other. Each node becomes part of the communication infrastructure. A message can travel from the originating sensor to the gateway through several intermediate nodes. The network is therefore not only a collection of endpoints, but a self-supporting communication fabric. This is the fundamental difference between a simple wireless sensor system and a distributed smart sensor WLAN.

In a self-forming mesh network, the nodes automatically discover neighboring nodes and establish communication paths without manual routing configuration. This is a major advantage in practical deployments. The installer does not need to design every radio path in advance. The network can adapt to the actual physical environment, available signal paths, and installed node density. If the environment changes, or if individual nodes are added, removed, or temporarily unavailable, the network can reorganize itself and continue operating through alternative paths.

From an operational point of view, this self-forming and self-healing behavior is one of the strongest arguments for distributed mesh networks. Sensor systems are often installed in places where long-term accessibility is limited. Nodes may be mounted on ceilings, in industrial zones, inside cabinets, on outdoor poles, in

fields, in public areas, or in other locations where manual maintenance is expensive. A network architecture that can automatically adapt to changing radio conditions reduces maintenance effort and improves operational safety.

The choice of radio frequency is also highly important. Distributed smart sensor WLANs can benefit strongly from signal-friendly sub-GHz frequency bands, such as the European 868 MHz ISM band or comparable regional bands. Compared with 2.4 GHz systems, sub-GHz communication generally provides better propagation through obstacles and longer range at the same transmit power. This makes it attractive for industrial buildings, outdoor areas, agricultural environments, smart city infrastructure, and other applications where reliable coverage is more important than high data rate.

In sensor networks, high bandwidth is usually not the primary requirement. Most sensor messages contain only a few measured values, status bytes, counters, alarms, or diagnostic information. Therefore, the system can prioritize range, robustness, power consumption, and regulatory compliance instead of raw throughput. This is fundamentally different from consumer Wi-Fi, where the goal is usually high-speed data transmission for human users. A smart sensor WLAN is optimized for machines, not for multimedia traffic.

Error-resilient modulation schemes can further extend the possibilities of such networks. In certain cases, modulation methods such as LoRa can be used to increase node-to-node distance and improve communication robustness. The idea is not necessarily to build a classical LoRaWAN architecture, but to use robust physical-layer techniques within a local mesh or sensor WLAN concept. This can open new perspectives for large-area low-power networks, where the distance between nodes must be increased without giving every sensor its own cellular modem.

However, a distributed mesh network must also respect regulatory limitations. In Europe, unlicensed sub-GHz ISM bands are subject to strict duty-cycle rules. This means that a device cannot transmit continuously and must limit its radio airtime. A well-designed sensor mesh network must therefore minimize unnecessary transmissions, use compact payloads, optimize routing behavior, and avoid excessive network overhead. The low payload nature of sensor communication fits this requirement well, but the protocol design must still be efficient.

A key advantage of technologies such as NeoMesh is that they are designed specifically for this type of low-power distributed sensor communication. Instead of using a high-

bandwidth consumer communication model, they focus on robust many-node networking, self-forming operation, low energy consumption, and reliable data forwarding. Such networks can support very large numbers of nodes and cover extended areas, while still keeping the individual sensor nodes small and power efficient.

From a topology point of view, this architecture sits between classical point-to-point communication and wide-area infrastructure networks. It is local, but not limited to a single direct radio link. It is distributed, but still organized around gateways that connect the network to the cloud. It is low-power, but not isolated. It creates a bridge between the physical sensing environment and higher-level digital systems.

The comparison with point-to-point cellular LPWAN is therefore not a question of which technology is universally better. It is a question of application geometry and system economics. If one sensor is installed at one remote site, direct cellular connectivity may be ideal. If hundreds of sensors are installed in one large industrial area, agricultural field, building complex, or smart city zone, a distributed mesh WLAN may be technically and economically superior. The cellular modem can be moved from every individual sensor into the gateway layer, while the local sensors communicate through a low-power mesh.

This also changes the energy architecture. In a direct cellular sensor, the node must provide enough energy for network registration, cellular transmission, and sometimes repeated connection attempts. In a mesh sensor WLAN, the node only communicates locally with neighboring nodes. The energy demand per message can therefore be much lower, especially when the local radio protocol is optimized for short payloads and duty-cycled operation. This can extend battery lifetime or make energy-harvesting operation more realistic.

Distributed smart sensor WLANs also provide flexibility in gateway design. A gateway can be fixed, mobile, or temporary. It can use cellular LPWAN, broadband cellular, Ethernet, Wi-Fi, or even future satellite-based communication to reach the cloud. In some applications, the gateway may buffer data locally and forward it later when wide-area connectivity becomes available. This is especially relevant for mobile, remote, or infrastructure-zero deployments, where permanent cloud access cannot be guaranteed.

Security and operational safety must also be considered. In a cellular point-to-point system, each sensor has its own identity and communicates through the mobile network. In a

mesh sensor WLAN, the local network itself becomes part of the system security architecture. Node authentication, message integrity, routing behavior, gateway trust, and data forwarding rules must be designed carefully. At the same time, the separation between the local sensor network and the customer's IT infrastructure can still provide a strong practical security advantage, because the system does not need to connect every sensor to the customer's Ethernet or Wi-Fi network.

In summary, distributed smart sensor WLANs are not replacements for cellular LPWAN. They are complementary architectures for a different class of sensing problems. Their strength appears when many low-power sensors must cover a local or regional area with high reliability, long lifetime, low operating cost, and minimal infrastructure dependency. By using sub-GHz frequencies, efficient payload handling, self-forming mesh operation, and gateway-based cloud connectivity, such networks can form the basis of a new generation of robust smart sensor systems.

A practical decision rule can be formulated as follows: use direct cellular LPWAN when individual sensors must communicate independently from distributed locations; use distributed smart sensor WLANs when many sensors must cooperate within one local sensing environment. The following chapter compares these connectivity philosophies more systematically by examining point-to-point, multipoint-to-point, and mesh-based communication models.

The E-IoT Ecosystem as a Practical Reference Architecture

The architectural principles discussed in the previous chapters are not only theoretical considerations. They have been implemented and validated within the E-IoT ecosystem developed by Endrich R&D. This ecosystem was designed as a modular smart sensor platform that can support different connectivity philosophies within one common architecture.

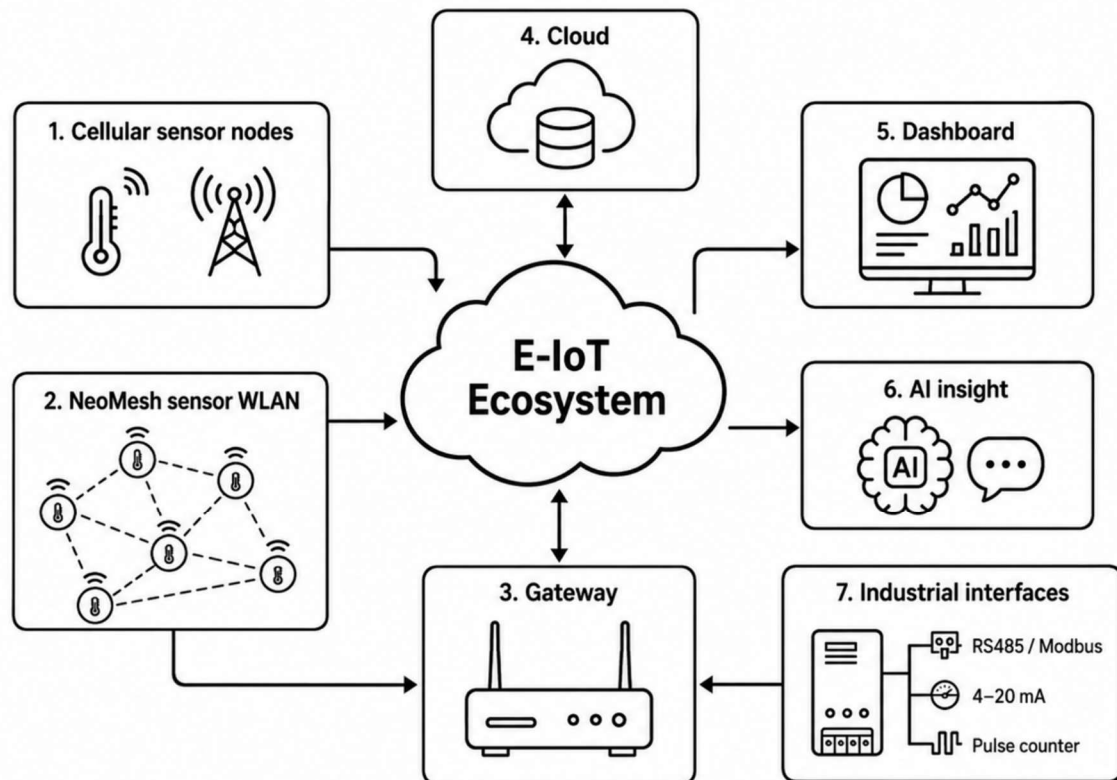
At the device level, E-IoT includes smart sensor nodes, data loggers, and interface modules for external industrial sensors, including digital, analog, and RS485/Modbus-based devices. These nodes can collect physical measurement data, preprocess it locally, and prepare compact payloads for wireless transmission.

For direct point-to-point communication, E-IoT devices can use embedded cellular LPWAN connectivity such as NB-IoT and LTE-M. This enables autonomous sensor-to-cloud operation without depending on the customer's Ethernet or

Wi-Fi infrastructure. Such an approach is suitable for geographically distributed assets, standalone monitoring points, and applications where each sensor must operate independently.

sensor → **local or cellular connectivity** →
gateway → **cloud** → **data processing** →
dashboard → **AI-supported insight**

E-IoT Ecosystem as Practical Evidence



For dense local deployments, the same ecosystem also supports distributed NeoMesh-based sensor WLANs. In this architecture, many low-power sensor nodes form a self-organizing local network and forward their data through one or more gateways. This reduces the need for individual cellular modems in every sensor and allows larger local areas to be covered with lower node complexity and improved energy efficiency.

The gateway layer connects the local sensor world with the cloud. Depending on the application, the gateway may use cellular LPWAN, broadband cellular, Ethernet, Wi-Fi, USB-connected host systems, or future satellite-based NTN communication. Gateways can also buffer data and forward it later, which is important when permanent wide-area connectivity is not available.

On the cloud side, E-IoT provides data reception, storage, visualization, alarm handling, and AI-supported interpretation. The complete chain can therefore be described as:

This practical implementation demonstrates that direct cellular LPWAN and distributed smart sensor WLANs should not be treated as competing concepts.

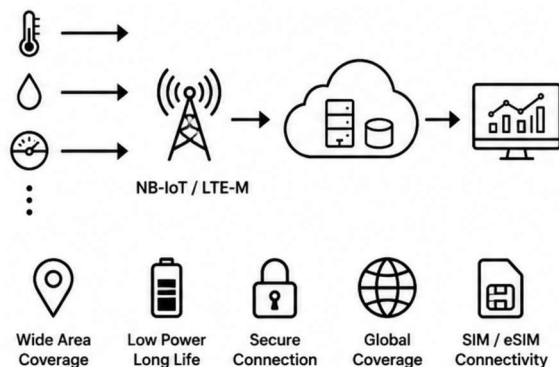
They are complementary building blocks. The optimal architecture depends on the number of nodes, deployment geometry, power budget, communication cost, required independence, and available infrastructure. The E-IoT ecosystem provides a reference platform where these options can be combined and compared in real applications.

Practical Decision Framework: When to Use Which Connectivity Architecture

After comparing direct cellular LPWAN connectivity and distributed smart sensor WLANs, the most important practical question is not which technology is generally better. The real question is: **which architecture fits the application, the deployment geometry, the energy budget, and the operational environment?**

A **direct cellular point-to-point architecture** is usually the best choice when individual sensors or data loggers are installed at geographically separated locations. In this case, each device must operate independently and communicate directly with the cloud. Typical examples include refrigeration units, vending machines, remote infrastructure, isolated measurement points, mobile assets, utility meters, or standalone industrial equipment. Here, NB-IoT or LTE-M connectivity provides a strong advantage, because the device does not depend on the customer's Ethernet or Wi-Fi network. The installation is simple, the communication path is clearly defined, and the sensor becomes an autonomous cloud-connected endpoint.

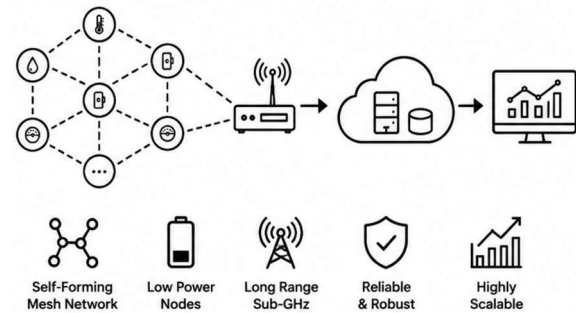
This architecture is especially suitable when the number of devices per site is low or moderate, when each device has access to mobile network coverage, and when the additional cost of a modem and SIM service is justified by the independence it provides. NB-IoT is often preferred for small, infrequent payloads and stationary devices, while LTE-M is more suitable for mobile devices, lower latency, more frequent communication, or applications where firmware updates are required.



A **distributed smart sensor WLAN or mesh architecture** becomes more attractive when many sensors are located within one local or regional area. In this case, equipping every node with its own cellular modem is often not the most efficient solution. Instead, many low-power sensor nodes can communicate locally through a self-forming mesh network and forward their data to one or more gateways. Only the gateway needs wide-area connectivity to the cloud.

This architecture is especially suitable for factories, building complexes, agricultural areas, smart city zones, warehouses, exhibition environments, infrastructure monitoring, and other applications where many sensing points must operate together. The main advantages are reduced node cost, lower power consumption, longer battery lifetime, better local coverage through multi-hop communication, and improved scalability. Sub-GHz communication and robust modulation schemes can further improve range

and reliability, especially in environments where 2.4 GHz communication is limited by obstacles or attenuation.



A **Wi-Fi or Ethernet-based architecture** can still be the right choice when the sensor system is installed inside a trusted and controlled IT environment. If the network owner allows access, if cybersecurity requirements are manageable, and if power and bandwidth are available, these technologies can be practical and cost-effective. However, they are less suitable when the sensor system provider must remain independent from the customer's local IT infrastructure.

A simple, practical rule can be formulated as follows:

Deployment situation	Recommended architecture
One sensor or a few independent sensors at different locations	Direct cellular LPWAN
Stationary sensor, very small payload, long lifetime	NB-IoT
Mobile sensor, more frequent data, lower latency, firmware update requirement	LTE-M
Many sensors in one local or regional area	Distributed mesh sensor WLAN
Dense local sensor network with low-power nodes	NeoMesh-type architecture
Customer IT network is trusted and accessible	Wi-Fi or Ethernet
Customer IT network is restricted or forbidden	Cellular or independent gateway-based architecture

Deployment situation	Recommended architecture
<i>Remote or mobile gateway with intermittent cloud access</i>	<i>Store-and-forward gateway architecture</i>
<i>Future infrastructure-zero or very remote deployments</i>	<i>Gateway with cellular or NTN/satellite backhaul</i>

The decision should therefore be based on the complete system, not only on the radio interface. Important selection criteria include:

- number of nodes,
- physical distance between nodes,
- availability of mobile network coverage,
- access to local IT infrastructure,
- required battery lifetime,
- payload size,
- latency requirement,
- installation and maintenance cost,
- cybersecurity model,
- cloud integration method,
- and long-term scalability.

In summary, **direct cellular LPWAN is strongest when each device must be autonomous**, while **distributed mesh sensor WLANs are strongest when many low-power devices must cooperate locally**. Wi-Fi and Ethernet remain useful where infrastructure access is allowed, but they are often limited by real-world ownership and security restrictions. The best smart sensor architecture is therefore not a single technology choice, but a system-level decision that balances independence, scalability, energy consumption, reliability, and cost.

Conclusion

Smart sensor systems are evolving from simple wireless measurement devices into complete digital information chains. Their value is no longer created only by the sensing element itself, but by the complete architecture that connects physical measurements to cloud-based processing, visualization, alarms, and AI-supported interpretation. For this reason, the selection of the communication technology must be treated as a system-level decision.

Wi-Fi and Ethernet remain useful where local infrastructure is available, trusted, and accessible. However, in many industrial and commercial environments, external sensor systems cannot freely use the customer's IT network because of cybersecurity policies, ownership restrictions, firewall rules, or maintenance responsibilities. Cellular LPWAN technologies such as NB-IoT and LTE-M solve

this problem by giving the sensor direct and independent cloud connectivity. They are especially suitable for autonomous devices, geographically distributed assets, and low-payload applications where long battery lifetime and infrastructure independence are required.

At the same time, direct cellular connectivity is not always the most efficient solution for dense local deployments. When many sensors must operate within one factory, building complex, agricultural area, smart city zone, or infrastructure environment, distributed smart sensor WLANs provide important technical and economic advantages. Self-forming mesh networks such as NeoMesh allow many low-power nodes to communicate locally and forward data through one or more gateways. This reduces node complexity, lowers power consumption, improves scalability, and enables robust coverage over larger areas.

The E-IoT ecosystem demonstrates how these connectivity philosophies can be combined in practice. It supports direct cellular smart sensors, distributed NeoMesh-based sensor WLANs, gateway-based cloud access, local buffering, data visualization, alarm handling, and AI-supported data interpretation. This shows that the future of smart sensor systems is not based on one universal communication technology, but on the intelligent combination of several complementary architectures.

The practical conclusion is clear: direct cellular LPWAN is the preferred choice when individual devices must operate independently, while distributed mesh sensor WLANs are the better architecture when many low-power nodes must cooperate locally. The best solution depends on deployment geometry, energy budget, payload size, infrastructure availability, security requirements, and total system cost.

By combining low-power sensing, independent connectivity, distributed wireless networking, gateway-based cloud access, and AI-supported interpretation, the next generation of smart sensor WLANs can provide robust, scalable, and economically viable solutions for industrial, environmental, and infrastructure monitoring applications.