Thomas Steen Halkier CEO of NeoCortec
Zoltan Kiss Head of R&D Endrich Bauelemente Vertriebs GmbH

How to set up a IoT network to get associated data from sensor to Cloud?

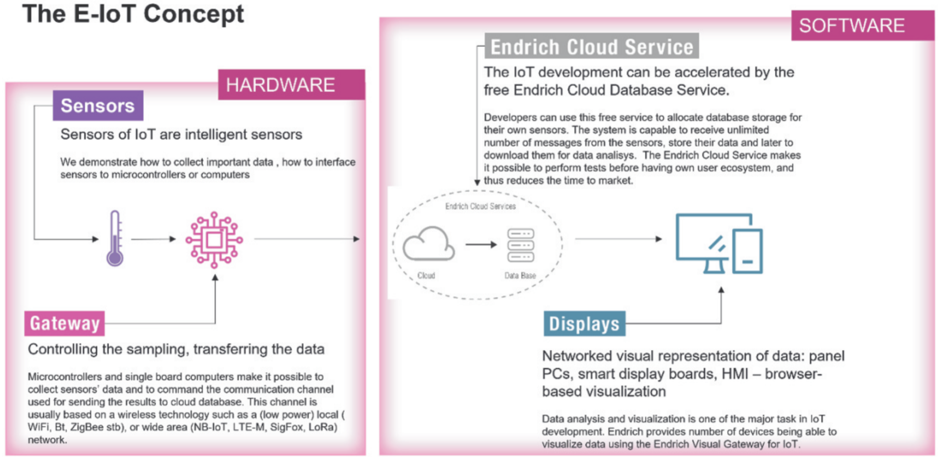
In this paper we are going to discuss the different possibilities to collect sensor data and get them into Cloud using the E-IoT ecosystem. One way of the data transfer is using smart sensors directly connected to the Internet, but there are many cases where a local wireless network of sensors with a single Internet gateway is a better and a more economical solution. We will discuss these options illustrated by the E-IoT ecosystem, which offers cellular LPWAN connectivity for direct sensor - database communication, and recently uses NeoCortec's revolutionary NeoMesh protocol for having an ad-hoc, real low power, sub-GHz mesh WLAN to collect the data locally and gateway them to Internet from a single access point.

What is the E-IoT ecosystem?

Industry 4.0 expects machines and equipment to be connected, exchange and use data collected by sensors. An MCU based electronics takes care of controlling the sensors, even offering the possibility to edge-computing the data and transfer them to a database for analysis or visualization. The ecosystem makes it all possible is called IoT, Internet of things, containing hardware elements and software services such as databases, visualization tools. Endrich's own E-IoT system is one of the possible choices offering all from one hand. Several IoT nodes, smart sensors, gateway devices as well as Cloud services are there for the partners to start their IoT development.

Endrich works on three major area, where the first one is about converting conventional devices into SMART. For that a RISC-V based general IoT Single Board Computer has been developed under open hardware and software structure; all technical data is freely available for the engineers of the market. The device is made as an engineering evaluation board to establish connection and carry out tests with the whole platform of E-IoT. This can be a basis of more specific product development, and

The E-IoT Concept



HARDWARE

Sensors

Sensors of IoT are intelligent sensors

We demonstrate how to collect important data , how to interface sensors to microcontrollers or computers

Gateway

Controlling the sampling, transferring the data

Microcontrollers and single board computers make it possible to collect sensors' data and to command the communication channel used for sending the results to cloud database. This channel is usually based on a wireless technology such as a (low power) local (WiFi, Bt, ZigBee stb), or wide area (NB-IoT, LTE-M, SigFox, LoRa) network.

SOFTWARE

Endrich Cloud Service

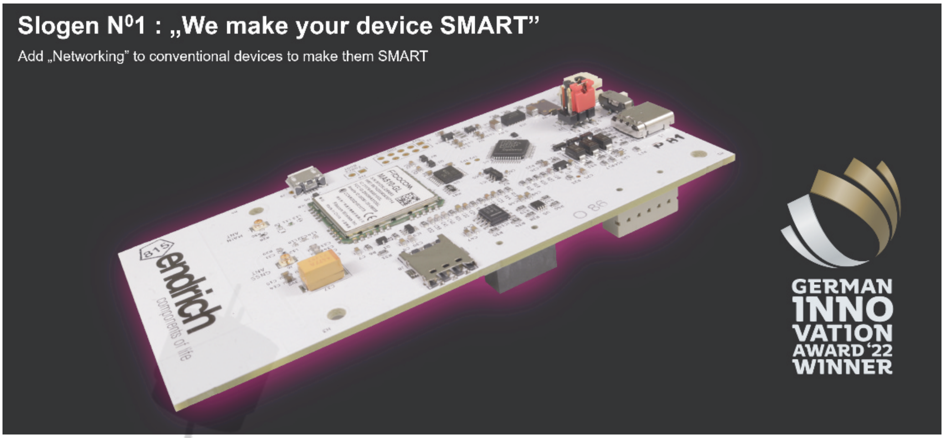
The IoT development can be accelerated by the free Endrich Cloud Database Service.

Developers can use this free service to allocate database storage for their own sensors. The system is capable to receive unlimited number of messages from the sensors, store their data and later to download them for data analisys. The Endrich Cloud Service makes it possible to perform tests before having own user ecosystem, and thus reduces the time to market.

Displays

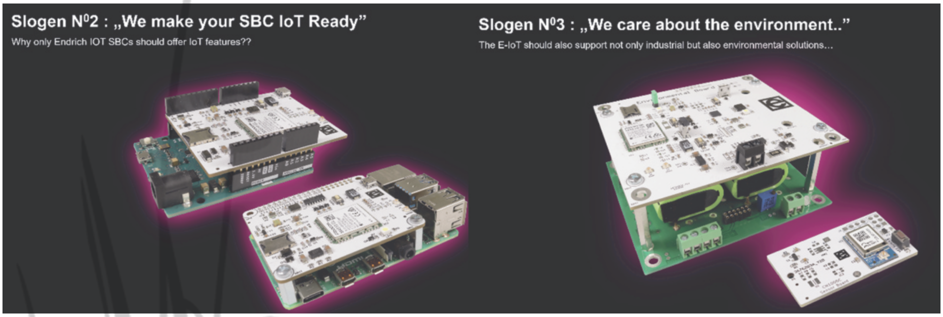
Networked visual representation of data: panel PCs, smart display boards, HMI – browser-based visualization

Data analysis and visualization is one of the major task in IoT development. Endrich provides number of devices being able to visualize data using the Endrich Visual Gateway for IoT.



Slogen N°1 : „We make your device SMART”

Add „Networking” to conventional devices to make them SMART



Slogen N°2 : „We make your SBC IoT Ready”

Why only Endrich IOT SBCs should offer IoT features??

Slogen N°3 : „We care about the environment..”

The E-IoT should also support not only industrial but also environmental solutions...

the slogan characterizes the project is the following:

“We make your device smart “.

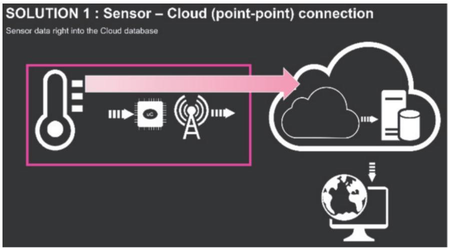
The second area is to also involve other SBCs available in the market such as Arduino or Raspberry Pi, where Endrich

offers extension shields to convert these MCU boards to a full IoT endpoint by adding sensors and communication possibilities, we simply “Make your SBC IoT ready”.
To also offer better environment for people, Endrich calls IoT for help in the area of environmental parameter monitoring as “we care about the environment “.

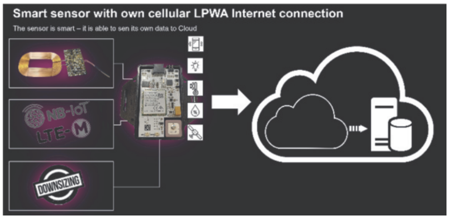
Above three area require detection of one hand operational parameters (machines, equipment mainly for tele-metrics supporting predictive maintenance) on the other hand environmental parameters, such as air quality, temperature distribution or other important measure describing the properties of a certain environment (buildings, warehouses, cities and any kind of residential area).

What architecture of sensor network can be best used to serve above tasks?

There are two major directions engineers of IoT solution may choose: having a smart sensor with own connection to the WAN (point to point or Sensor to Cloud solution) or using a local network of sensors and have a dedicated access point for this LAN to gateway the data to WAN. E-IoT platform started with direct sensor to cloud communication, our classical sensor nodes had integrated LPWAN access using NB-IoT, and LTE-M modems.


SOLUTION 1 : Sensor – Cloud (point-point) connection

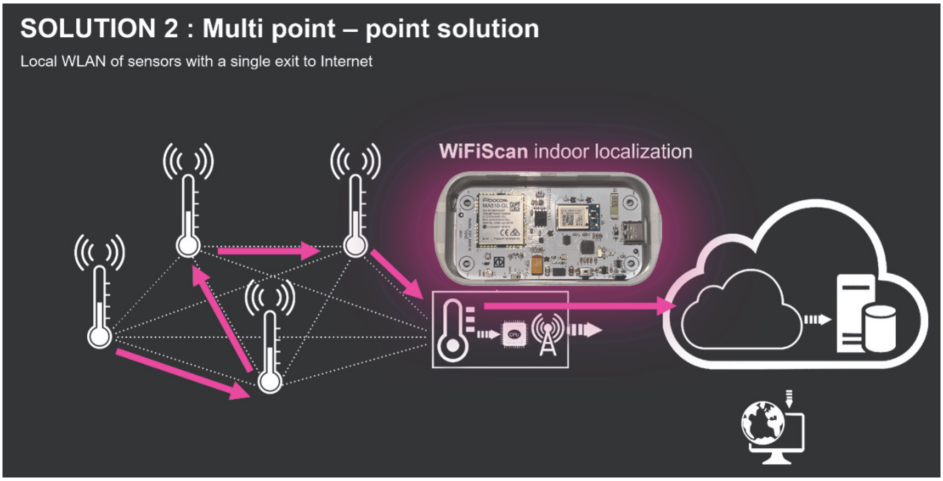
Sensor data right into the Cloud database


Smart sensor with own cellular LPWA Internet connection

The sensor is smart – it is able to sen its own data to Cloud

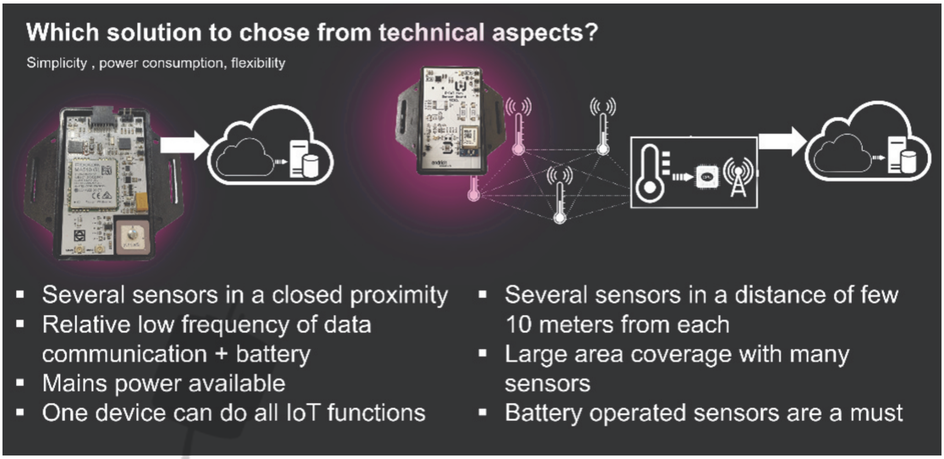
For cases when the sensors are in closed proximity, such as in machines, we can use this solution powerfully. The E-IoT bad family offers a great selection of proof of concepts to derivate into customer specific products. One of the most compact and versatile devices is the Mini E-IoT board with integrated LPWA modem, sensors, external sensor interface and wireless recharging circuit for the accumulator.

There are however cases when these devices offer limited services that are not good enough. Especially when you need a more frequent communication from many detection devices in a few ten- or hundred-meters distance from each other, point to point solution is both too expensive and not sustainable from battery lifetime point of view. In this



SOLUTION 2 : Multi point – point solution

Local WLAN of sensors with a single exit to Internet

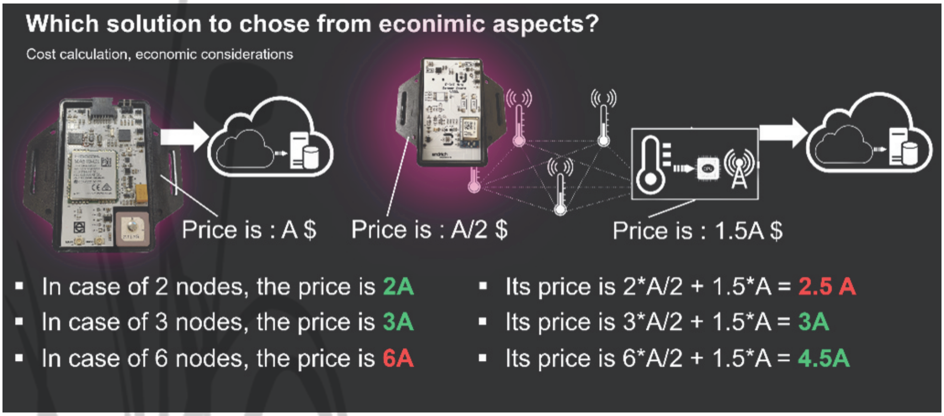


Which solution to chose from technical aspects?

Simplicity , power consumption, flexibility

- Several sensors in a closed proximity
- Relative low frequency of data communication + battery
- Mains power available
- One device can do all IoT functions

- Several sensors in a distance of few 10 meters from each
- Large area coverage with many sensors
- Battery operated sensors are a must



Which solution to chose from econimic aspects?

Cost calculation, economic considerations

- In case of 2 nodes, the price is 2A
- In case of 3 nodes, the price is 3A
- In case of 6 nodes, the price is 6A

- Its price is 2*A/2 + 1.5*A = 2.5 A
- Its price is 3*A/2 + 1.5*A = 3A
- Its price is 6*A/2 + 1.5*A = 4.5A

case it is smarter to use a real low power wireless communication protocol running on a mesh sensor network, offering a reliable, cheap, and sustainable way of collecting the data from the environment. A single gateway offers an exit to the WAN as described in the next figure.

From technical point of view best cases to use point to point solution appear, when the number of sensors are limited in number, they are close together, the frequency of data sending is relative low and can be supported even by battery for long time, or when mains power is available to supply the node. In all other cases it was better to use he multipoint point solution.

From economical point of view there are advantages of the point-point solution in case of single nodes. Of course there is an additional telecommunication cost for using the cellular network, but due to the low data volume and the relative rare connection a prepaid IoT SIM card of 10 EUR/ 10 years offers a significant lower cost compared to legacy GSM services.

However, in case of 3 nodes the price and the total cost of ownership are equal for both solutions. In this case technical aspects such as battery lifetime expectations should dominate in the decision. Over this number of nodes however it is better to use mesh and a gateway as the calculation of below figure clearly indicates.

What kind of local network is suitable for the smart sensors?

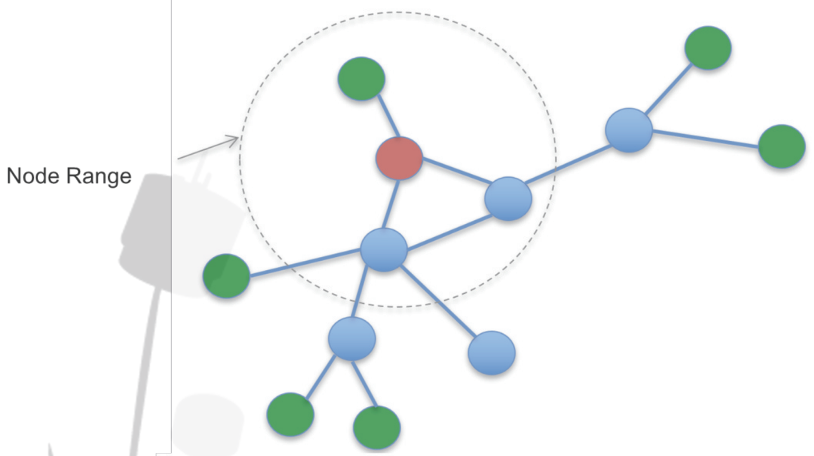
The ideal networking architecture is a mesh topology to be able to cover a large area compared to the distance of neighboring nodes. As the network should be operating from battery, we cannot afford to have highly draining network coordinators and segment routers, ideally all nodes should take care of their own sensors and routing neighbors' data over the mesh. The higher the distance between neighboring nodes and the higher the number of nodes in the network the higher the covered area will be. This is helped by using sub gigahertz radio communication, which also offers more reliable solution in harsh industrial environments due to the better (indoor) penetration. The networks should be easily extendable, and as-hoc, installation should be self-explanatory. Reliability and data security are key factors in any kind of connected sensor systems, the desired wireless solution need to be cable like reliable and the used security measures must offer a way to keep out eavesdropping and attacks. Finally, the used technology should be affordable, royalty free and approvals should be possible (FCC, CE-RED) to get easily. For this reason, the developers of the Endrich's E-IoT ecosystem have chosen NeoMesh to be the right protocol running on the local smart sensor network.

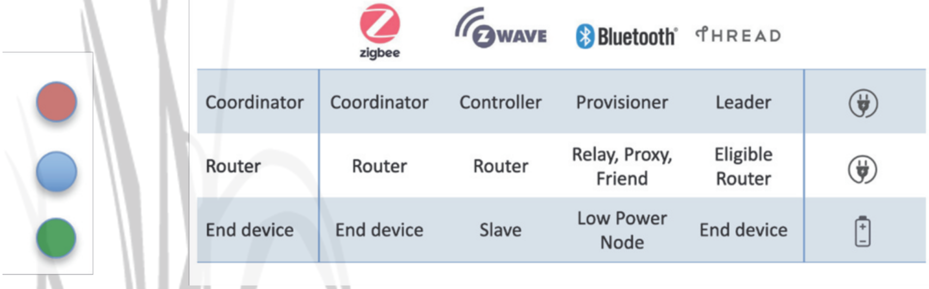
Legacy mesh network technologies on the market

There are many successful MESH technologies are available on the market. They usually offer a very adequate solution for the original purposes they have been developed for but may have some challenges if we want to use them in the industrial environment fully battery operated as described in the ideal network definition for the E-IoT smart sensors.

Usually, those technologies go with different kind of nodes, having different kind of tasks, such as network coordinators, routers and end devices (called differently in each technology) as seen on the picture (picture source NeoCortec).

For those technologies you always need a set of devices, which usually needs to be powered by mains for sustainable





		zigbee	Z-WAVE	Bluetooth	THREAD	
🔴	Coordinator	Coordinator	Controller	Provisioner	Leader	🔌
🔵	Router	Router	Router	Relay, Proxy, Friend	Eligible Router	🔌
🟢	End device	End device	Slave	Low Power Node	End device	🔋

operation, as they should continuously listen to the network, and in return the end devices have such low power consumption, that could be energized from battery. Very good example is the perfect use case of Philips Hue, where a dozen mains powered LED bulbs form a wireless mesh network. Here the limited number of devices used in a residential real estate and the presence of mains power in the bulbs make the use case perfectly fit to the used wireless technology. But what if we need to connect hundreds or thousands of devices into such a mesh? Centralized network management usually limits the number of nodes to few hundred due to the inefficient routing strategies, which causes lack of scalability. This is a no go for those smart sensor applications when you need to cover a large area, instead of a residential house, a hotel or a large industrial building. Furter issues come with the GHz frequency used in many of the common wireless technologies, 2.4GHz would suffer indoor penetration problems in industrial environment, instead of this a sub-GHz technology fit better. Asynchronous operation results in the necessity of nodes that always listen, thus the entire network cannot be powered from battery. Also there may be reliability problems on the data exchange as the end-to-end package error rate is negatively affected by the lack of local handshake of neighbors as well as using only single channels. Of course, just as in the example of Philips Hue, there are perfect application fits even with the mentioned limitations.

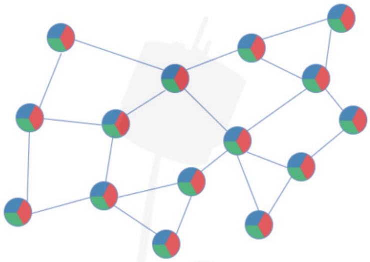
NeoMesh, the 2nd generation mesh network

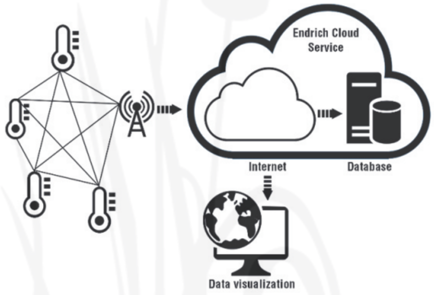
NeoCortec’s NeoMesh technology offers a different kind of mesh architecture. No more nested tree topology, no more partial mesh or incomplete network, NeoMesh offers a fully connected mesh, with nodes offering single node solution to multiple tasks of routing, coordination and being end-device (picture source NeoCortec)..

This solution at its core with NeoMesh, the Wireless Mesh Networking Protocol represents a paradigm shift from traditional network architectures. Unlike the conventional solution with a central Network Manager to control communication between nodes, this protocol employs autonomous intelligent nodes as its backbone. This feature empowers each node to act as an independent entity, facilitating direct communication between nodes without the need for a central authority. The result is a unified network that simply works, no matter how large or complex it grows. As more nodes join the network, they seamlessly link with existing nodes, forming an interconnected web of communication that can span vast distances. This adaptability and scalability are particularly valuable as an extension of the E-IoT platform when applied in an area, which should be covered by hundreds or thousands of sensors. One of the protocol's most impressive features is its patented routing mechanism. This mechanism ensures that data travels seamlessly through the network, even in the face of obstacles in the RF (Radio Frequency) path or the movement of nodes within the network. Traditional networks often suffer from performance issues when nodes are blocked or dynamically change their positions. However, the NeoMesh Networking Protocol eliminates such concerns, guaranteeing reliable data transmission at all times. In practical terms, this means that the network's performance remains unaffected by environmental factors or dynamic changes within the network itself. Whether nodes are added, removed, or repositioned, the network remains robust and fully functional, ensuring uninterrupted connectivity for all devices and users. The protocol's ability to address weak spots in real-life networks is noteworthy. By simply adding another node, assigned with the appropriate network ID, it seamlessly integrates with the existing network, reinforcing its coverage and performance.

At the heart of the NeoMesh technology lies a robust protocol stack with integrated security and reliability features. A key aspect of this security measure is the encryption of all wireless communication between nodes using AES128. By employing this encryption, the payload data and the network communication remain impervious to monitoring by any untrusted entity. The system is built for long-lasting performance. The power consumption is exceptionally low, enabling the batteries to last for several years. The NeoMesh network follows a time-synchronized protocol, wherein each node spends most of its time in a sleeping state. This architectural approach ensures a highly predictable power consumption pattern for every node in the network. As a result, all nodes consume nearly the same amount of energy, enabling each network node to operate efficiently for many years.

The E-IoT with its Neo-Mesh local sensor network extension operates at sub-Gigahertz frequency to overcome the problems of other protocols in harsh industrial environments. When comparing sub-GHz networking to Wi-Fi and Bluetooth, using the same antennas and transmission power, it becomes evident that sub-GHz networking offers a longer range. The reason behind this extended range lies in the fact, that the lower radio frequency waves are not as easily absorbed by physical matter as the 2.4 GHz signals utilized in Wi-Fi and Bluetooth. Due to the automating routing embedded into the NeoMesh stack running on their microcontroller, the network coordination is distributed between the nodes which then operate at low power. As a result of the decentralization, the efficient speed-routing protocol and the ad-hoc network construction a massive scalability with thousands of nodes can be achieved. And NeoMesh does it on the way that data exchange goes with cable-like reliability die to the handshake between nodes applied at each hop with 32bit CRC and automatic retry in case of CRC error. Instead of communicating on single channel, a frequency hopping across 15 channels is being used to avoid noise.





These capabilities of the NeoMesh Protocol make it an ideal solution for smart sensors installed across large-scale industrial complexes, such as factories, buildings, real estates, and shop, offering also a perfect local wireless networking solution to extend E-IoT concept with this important feature.

Reliability factors to consider for wireless networks.

It is often said there are no more reliable solution in communication than cables, but are cables not suffering for possible damages such as breaking, collecting noises? They do and the installation is usually costly and sometimes not even possible, for instance when network organization is a subject of frequent changes. In systems where high reliability is a must redundant communication channels are required, which needs double cable installation, so cabled solutions’ reliability comes with a cost. Offering all advantages of wireless networking, NeoMesh is a cable-like reliable solution while offering much higher level of scalability and lower cost. Let us see why it is reliable.

To understand key reliability measures of wireless networking let us look at the performance indicators of such networks. Noise in wireless networks can significantly affect communication performance in both the ISM (Industrial, Scientific, and Medical) and licensed bands. In the unlicensed and often crowded ISM bands, interference and non-cooperative transmission can lead to increased noise levels, which degrades the overall signal quality. On the other hand, even in licensed bands where specific frequencies are allocated to specific users, external factors such as environmental conditions and interference from neighboring bands can cause noise, necessitating effective noise reduction strategies for reliable wireless communication. Static obstacles such as buildings and walls can attenuate and block wireless signals, leading to signal degradation and reduced coverage. Dynamic obstacles such as moving vehicles or people introduce additional challenges with signal interference and fluctuations affecting the reliability of wireless communication in real-time scenarios. In unidirectional communication, where there is no place for handshake and thus no chance for data acknowledgement, the reliability dramatically reduces compared to bi-directional networks with ACK/NAK handshake. To validate the data being received the most common method being used is the cyclic redundancy check (CRC). Cyclic Redundancy Check (CRC) is an error-detection technique used in digital communication to verify the integrity of data. It involves appending a fixed-size check value to the data, which is calculated based on the remainder of polynomial division, and the recipient can use this check value to identify and correct errors that may have occurred during transmission. Cyclic Redundancy Check (CRC) is particularly effective in detecting burst errors referring to consecutive bits that are corrupted during transmission. CRC, by its nature of polynomial division, is capable of detecting burst errors because it relies on the fact that errors close to each other in the data stream will result in distinct and detectable patterns in the remainder of the division process, allowing for efficient error detection and correction. CRC16 is generally effective in detecting errors, including longer random errors, within the limits of its design. The effectiveness of CRC (Cyclic Redundancy Check) in detecting errors is determined by the size of the CRC, which in the case of CRC16 is 16 bits. This means that it can detect errors of up to 16 bits in length. However, it's important to understand the limitations of CRC. While it is robust for many applications, it is not foolproof, and there is always a small possibility that certain types of errors may go undetected. Additionally, CRC is more effective at detecting burst errors rather than random errors.

If the requirement is to detect longer random errors with higher certainty, a larger CRC or other error-detection and correction codes with greater capabilities may be considered. The choice of error-checking method depends on the specific requirements of the application and the desired level of error detection and correction. We can however say that CRC16 is able to detect longer random errors with the probability of 99,998474%. This means that payload messages with bit errors received, may be marked to be ok by the CRC error check algorithm. In case of thousands of payload packages delivered each day in a large network, at least a few packages will be accepted as “good” although they are “bad”. If the CRC checksum is as high as 32 bits, the undetectable burst error length will be longer, and the probability of blocking such packages will be 99,99999997671%, significantly better than CRC16, nearly zero chance to let through errors.

In point-to-point topology, or even a star network topology, if the link between the sending device and the receiving device is no longer reliable, then the communication breaks down – there is no alternative path for the data to flow. The link between two devices can break for different reasons; it may be due to noise, or because the link is obstructed either temporary or permanently by some obstacles. The noise level will vary from location to location, and also over time. This means that even though a system installed in one location works flawlessly, it may not work as reliably in another location. Similarly, a system may work with no issues at install time, but sometime later, issues may start to occur. It could for instance be due to other systems being installed which operates in the same frequency band.

NeoMesh reliability and security

After discussing that NeoMesh offers the possibility to create a large wireless ad-hoc network with thousands of nodes, which are all battery operated, all acting as routers, coordinators, and end-devices as single item, no need for repeaters, while there is a redundancy in the signal path, it is time to talk about the reliability and the security of this solution. NeoMesh, which is a mesh topology-based connectivity solution, incorporates various features designed to enhance reliability. The mesh topology ensures redundant links, enabling the flow of payload data through alternative paths if a link breaks down. The patented routing protocol, Speed Routing, optimized for low-power mesh networks, ensures real-time handling of connection issues due to noise or link blockage by routing data along the fastest path.

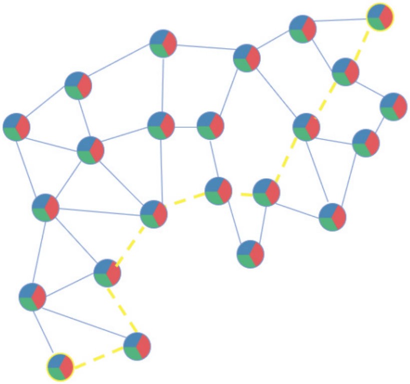
In the NeoMesh network, the exchange of payload data between nodes relies on local ACK/NACK, with package transfer retries in case of failure. The ACK/NACK employs CRC checking with a 32-bit checksum, ensuring a high probability of error-free received and acknowledged packages. NeoMesh also supports end-to-end acknowledgment, automatically notifying the source node upon successful delivery at the destination.

To further enhance reliability, NeoMesh employs frequency hopping, spreading communication across the entire frequency band and avoiding heavily used channels, while improving also noise immunity. Reliability is not only a matter of ensuring data is delivered at the destination, it also implies that the correct data is delivered. CRC checking as previously discussed is good for making sure there a no bit errors, but it does not guarantee that payload data was not generated by a malicious source. Reliability and security is often mixed up when discussing networking, however they are fairly different properties. While reliability describes the ability of the network to keep data and service integrity, security level tells how much the network is immune for eavesdropping and attacks.

Strong encryption is integral to NeoMesh, with data exchanged between nodes encrypted using industry-standard AES128, and a challenge-response handshake implemented for fully acknowledged communication, preventing playback attacks, and ensuring secure payload data exchange.

NeoMesh has two strong features built into the core of the protocol stack which increases the reliability even further by securing the communication link:

First off, all data exchanged between nodes in the network, as well as the complete RF communication are encrypted using industry standard AES128. The key for the AES, is the network key which is programmable by the system configurator and stored securely in each module. Secondly, when using fully acknowledged communication between the source and the destination, there is an automatic

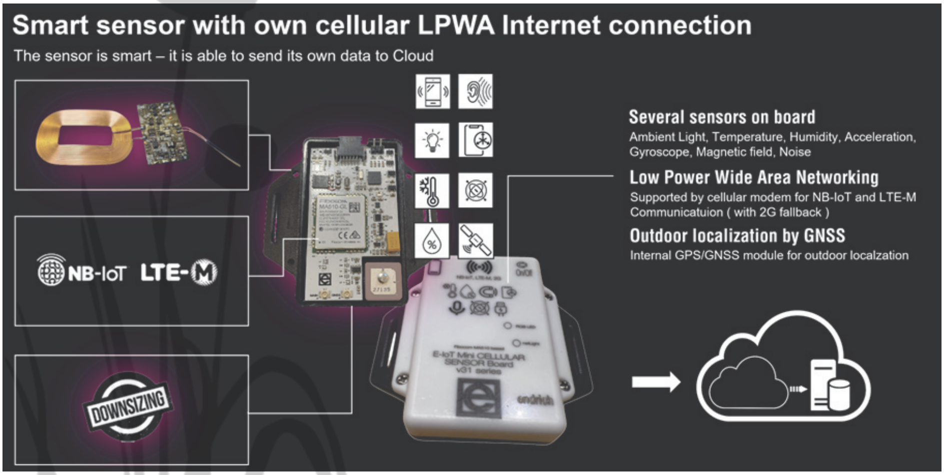


challenge-response handshake implemented, which ensures that a destination node will only accept payload data from another node (source) if the payload data includes the correct response to a challenge given by the destination. This challenge-response authentication is unique to NeoMesh and is handled completely seamless by the protocol stack. It prevents so-called playback attacks where a malicious device records a previously sent payload package which may contain a certain control function like for instance “unlock door” or similar. The perpetrator later re-transmits (playback) the message which would unlock the door. With challenge response authentication this is not possible.

What kind smart sensor devices are available as PoC products these days at the E-IoT family?

The ideal sensor device for point-to-point communication is the mini-E-IoT board of Endrich having several sensors, such as temperature, humidity, acceleration, ambient light- and magnetic field sensors, with gyroscope and microphone on board. The built in GNSS module offers outdoor localization services. The communication protocol being used is a cellular NB-IoT/LTE-M (LPWA) or 2G GSM technology depending on service availability. Data will be directly sent by the sensor node to the E-Cloud or any other public cloud services using UDP or MQTT protocol. Some of the models offer USB charging, others use wireless charging method for the on-board lithium-ion battery. In case of no battery needed, the USB connector can be used to power the device.

In case of using the multipoint-point sensor organization, the ideal node is the



Smart sensor with own cellular LPWA Internet connection

The sensor is smart – it is able to send its own data to Cloud

Several sensors on board

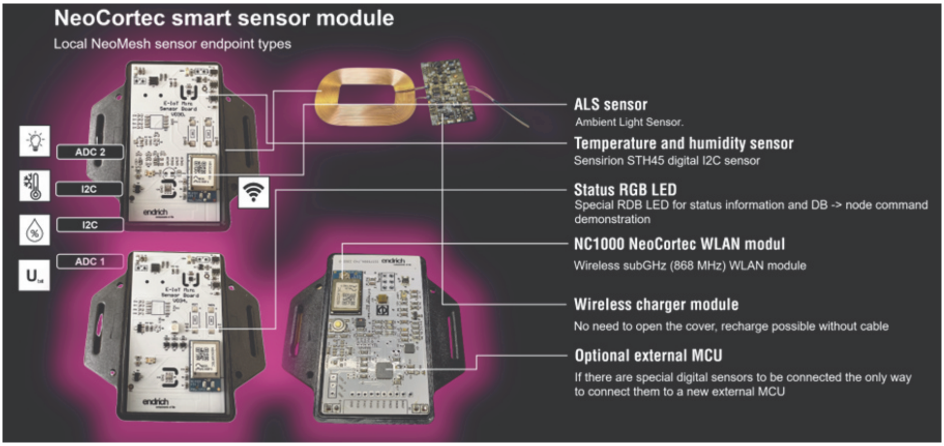
Ambient Light, Temperature, Humidity, Acceleration, Gyroscope, Magnetic field, Noise

Low Power Wide Area Networking

Supported by cellular modem for NB-IoT and LTE-M Communicatuion (with 2G fallback)

Outdoor localization by GNSS

Internal GPS/GNSS module for outdoor localzation


NeoCortec smart sensor module

Local NeoMesh sensor endpoint types

ALS sensor
Ambient Light Sensor.

Temperature and humidity sensor
Sensirion STH45 digital I2C sensor

Status RGB LED
Special RDB LED for status information and DB -> node command demonstration

NC1000 NeoCortec WLAN modul
Wireless subGHz (868 MHz) WLAN module

Wireless charger module
No need to open the cover, recharge possible without cable

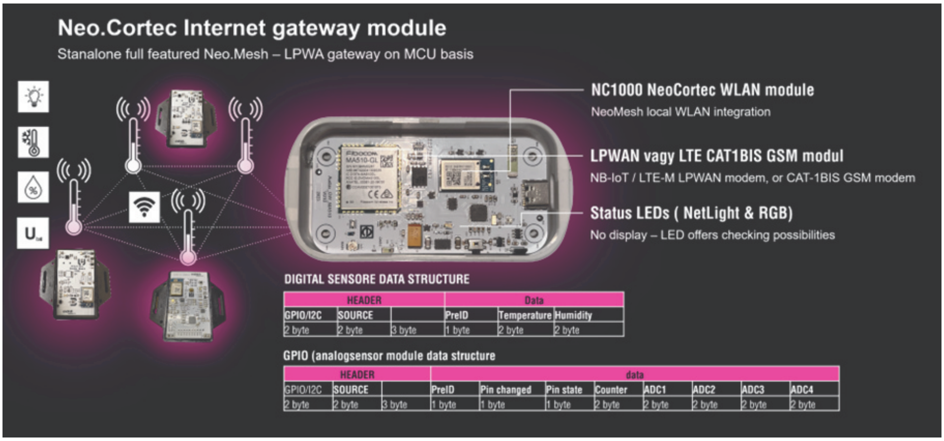
Optional external MCU
If there are special digital sensors to be connected the only way to connect them to a new external MCU

local WLAN sensor module built around the NeoCortec MESH modem. This module is optimized for battery operation, featuring wireless charging for the on-board lithium polymer cell. The product exists with optimal low power consumption using the internal ARM Cortex M0+ MCU built in to the NC1000 mesh module, other version offers an external low power MCU and a further feature connector for external I^{2}C and analogue sensors.

What gateway solutions can be used in the multipoint-point topology?

In the case of using a local WLAN of smart sensors, the topology needs one of the E-IoT NeoMesh-LPWA gateways. There are several task specific gateways created for amongst others industrial, agricultural and demonstration purposes, featuring wired interfaces used in those applications next to the ability of integration into the NeoMesh and at the same time using cellular communication to the cloud. The most general-purpose gateway device has only NeoMesh and LPWA connectivity on board.

Building into the NeoMesh this device constantly collects the data arriving one of the sensor nodes. After decoding them it creates the JSON telegram required by the E-Cloud service and uses the LPWA (NB-IoT/LTE-M) cellular network to get them into the cloud. It offers a fall back to 2G when LPWA services are unavailable. Powered from mains via the USB-C connection, the gateway device offers an affordable, sustainable and stabile way of collecting data from the possibly large sensor mesh and connecting that to the Internet of Things.
Other - more enhanced - version of the gateway is equipped with legacy LTE modem, with higher bandwidth and the



Neo.Cortec Internet gateway module

Stanalone full featured Neo.Mesh – LPWA gateway on MCU basis

NC1000 NeoCortec WLAN module
NeoMesh local WLAN integration

LPWAN vagy LTE CAT1BIS GSM modul
NB-IoT / LTE-M LPWAN modem, or CAT-1BIS GSM modem

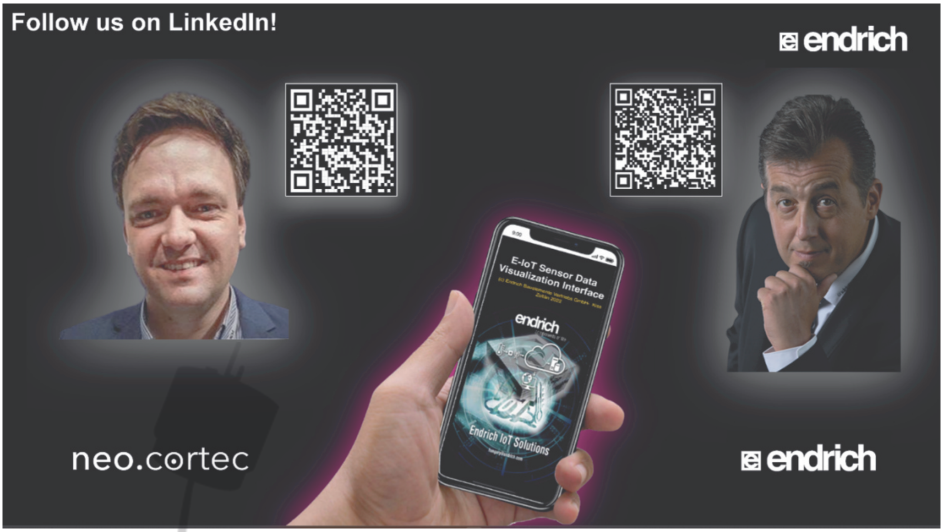
Status LEDs (NetLight & RGB)
No display – LED offers checking possibilities

DIGITAL SENSORE DATA STRUCTURE

HEADER			Data		
GPIO/I2C	SOURCE		PreID	Temperature	Humidity
2 byte	2 byte	3 byte	1 byte	2 byte	2 byte

GPIO (analogsensor module data structure

HEADER			data							
GPIO/I2C	SOURCE		PreID	Pin changed	Pin state	Counter	ADC1	ADC2	ADC3	ADC4
2 byte	2 byte	3 byte	1 byte	1 byte	1 byte	2 byte	2 byte	2 byte	2 byte	2 byte



Follow us on LinkedIn!

possibility to either using WiFi-Smart feature to indoor localization and can also gather location information from the GSM towers in case GNSS services could not be used.

All above products exist as proof of concepts and evaluation boards, we are there to help you to develop your own product or let us develop for you according to Your wishes.