FACT SHEET

A wireless sensor

V1.0

22.Jan.2020

Contents

1. A wireless Sensor ... 3
1.1. What is a wireless sensor? ... 3
1.2. Private vs. Public Infrastructure? ... 4
1.3. Frequency band ... 4
1.4. Micro-position of sensor ... 5
1.5. Interference factors ... 5
1.6. Mitigation measures ... 6
1.7. Functionality of a wireless sensor ... 6
1.8. Monitoring of Connection ... 7

1. A wireless sensor

These days, working with wireless (temperature) sensors in GxP-compliant temperature monitoring solutions is state-of-the-art. However, what is “wireless,” and what are the implications? What are the risks of wireless sensors and how can they be mitigated?

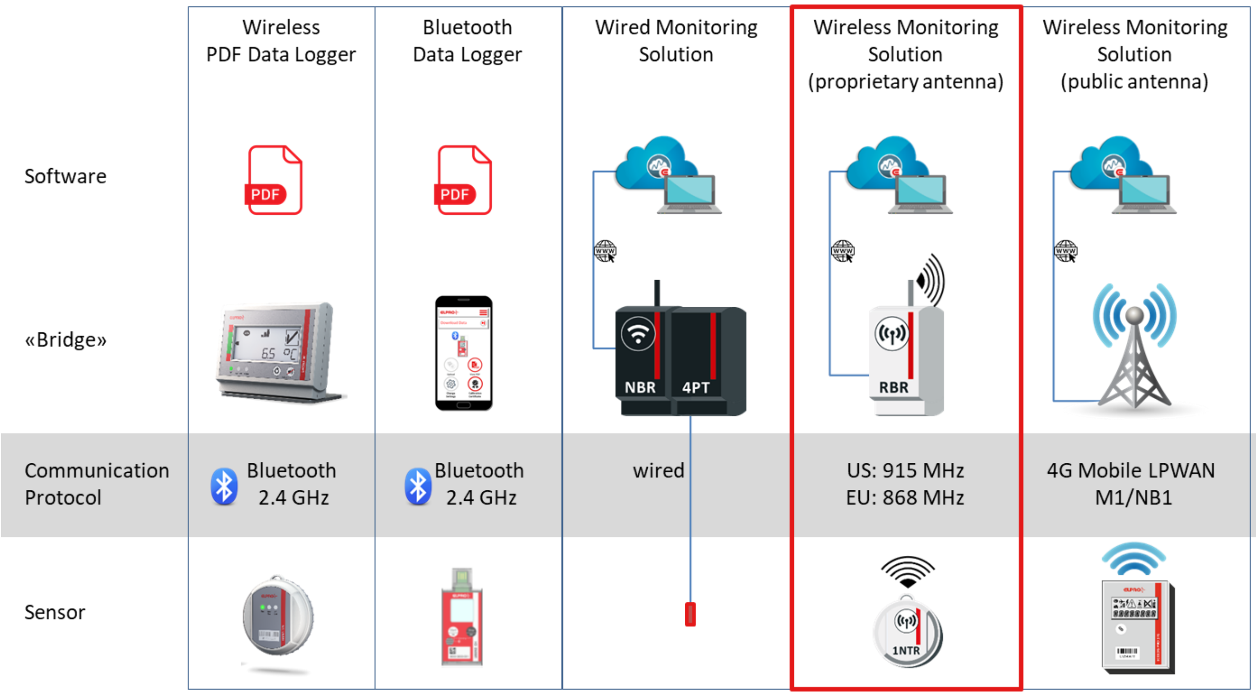
This paper gives an overview about the following topics:

- What is a wireless sensor?
- What are the frequencies?
- What is the wireless performance?
- What are interference factors?
- What is the typical functionality of a wireless sensor?
- Recommendations

1.1. What is a wireless sensor?

In GxP-compliant monitoring solutions temperature is measured by a sensor, and then transmitted via “bridge” to software in which data is archived and reports can be generated. The graph below shows five different examples of this procedure:

- The two examples on the left show data loggers using Bluetooth for the wireless communication and then generating PDF reports.
- The middle example is a wired central monitoring system.
- The two examples on the right aggregate the data in a cloud-based software and use non-wired communication bridges (e.g. signals) to communicate wirelessly with the sensor.

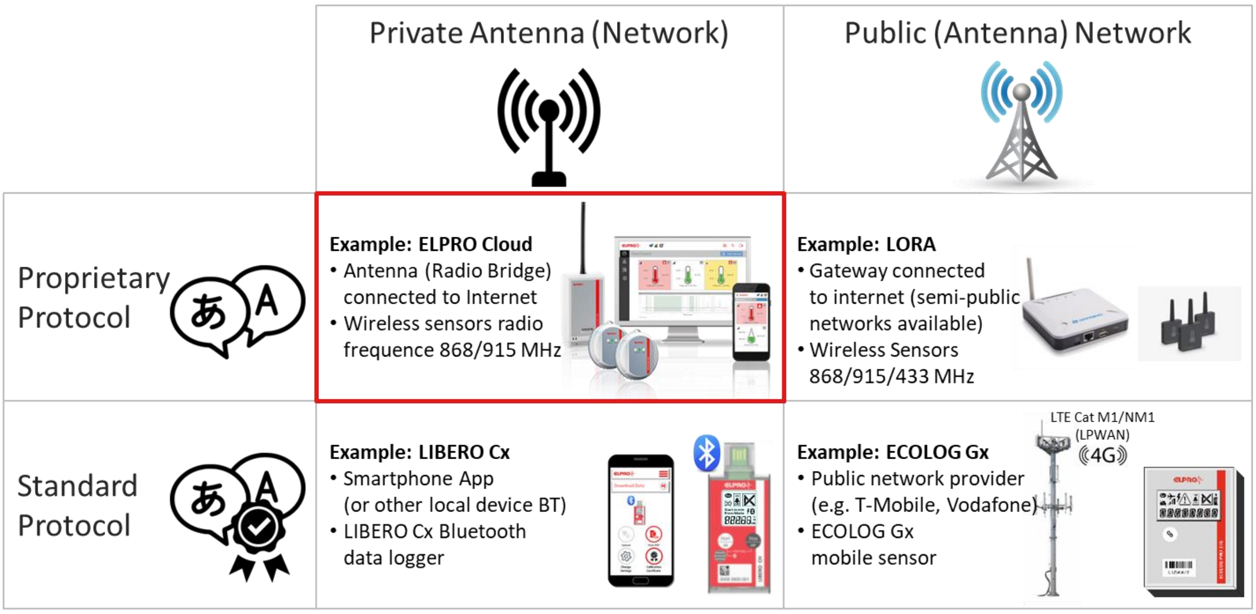


In this factsheet, we mainly discuss wireless monitoring solutions using a proprietary antenna in the 868/915 MHz frequency. This is the most common frequency band available for implementing a proprietary wireless protocol.

1.2. Private vs. Public Infrastructure?

When using wireless technology, it is important to choose the right infrastructure and protocol.

- Does the communication protocol use a known standard?
- Do we use a public antenna network?



What are the pros and cons of Public vs. Private Antenna Networks:

- The disadvantage of a Private Antenna Network is that you need your own antenna at every place to and from you wish to communicate. In the case of Bluetooth, you may use an available antenna (e.g. of a Smartphone) but you still need to install an app and pair the device with the antenna.
- When using a Public Antenna Network, one can benefit from existing infrastructure. However, the disadvantage here is the dependency on the network provider, who will have to grow and strengthen the network.

1.3. Frequency band

When comparing the theoretical radio strength of different frequencies, one has to look at the signal range and the wavelengths. To illustrate the two performance parameters, the following table compares the Bluetooth standard with the 868/915 MHz:

Frequency band	Range	Wave lengths	Implication
Bluetooth (2.4 GHz)	10 bis 50 m	12 cm	Perfect for transmitting large amount of data (e.g. voice, documents) on a short range (short distance between antenna and device). Many peripheral devices (e.g. headsets, speakers) heavily use the Bluetooth band.
915 MHz **868 MHz**	500 bis 1000 m	33 cm 35 cm	Perfect for transmitting small amount of data on larger distances. The frequency band 868/915 MHz is primarily used in many different industrial applications (e.g. temperature sensors, fire systems, burglar systems).

Due to the large range, the 868/915 MHz frequency band is very popular for wireless temperature monitoring solutions.

1.4. Micro-position of sensor

As shown in above table, the frequency band also defines the wavelengths. The radio signal is a function of time, therefore the wave peak and the wave base are moving through the room. Under ideal circumstances (e.g. no signal reflection, absorption or interference) the wave peak and base will go through every point within the range of the RBR. Moving the sensor that is already within the range of the RBR only makes sense when there is a zone of interference that results in a standing wave. Interferences and standing signal waves can results in a weak connection. In this case moving the sensor might improve the strength of the connection, when the sensor has been moved out of a zone of interference. To avoid such a situation we recommend preventing the following interference factors.

1.5. Interference factors

There are various interference factors, which permanently or punctually influence the radio connection. It is important to realize that radio systems are by definition used in a dynamic environment. This means that the various interference factors are not static, but changing constantly over time.

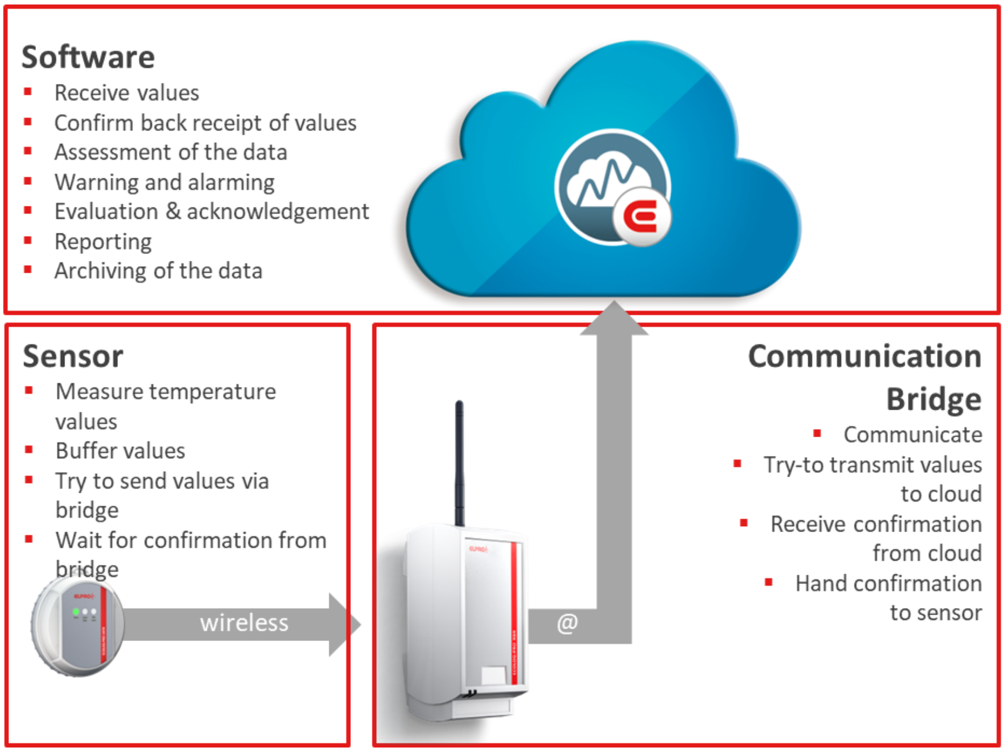
1.6. Mitigation measures

The following list gives hints on how to mitigate interference factors.

Source of interference	Interference	Mitigation measures
Walls & racks	Concrete and in particular metal between data loggers and transmitters are partially absorbing and/or reflecting the radio signal. Both effects can significantly weaken the radio signal.	Whenever possible, data loggers and transmitters should have direct intervisibility.
Pallets & products	Mass (material) between data loggers and the transmitters can weaken the radio signal.	Define the final position of the transmitters only in a fully loaded facility. If needed, slightly relocate transmitters.
Forklifts, loaders, Humans	Moving forklifts, loaders, humans or other moving, living beings may cause short interruptions in the radio connection.	It is the nature of radio connections that short interruptions are inevitable. Use an alarm delay for Sensor-Failure. Since the sensors have a buffer storage, the values are transmitted as soon as a connection is re-established.
Other radio systems	The use of other devices or radio systems that are using the same or a neighboring radio band may cause short interruptions in the radio connection.	It is the nature of radio connections that short interruptions are inevitable. Use an alarm delay for Sensor-Failure. Since the sensors have a buffer storage, the values are transmitted as soon as a connection is re-established.

1.7. Functionality of a wireless sensor

The loss of a wireless connection does not mean the loss of data. The systems have mitigation strategies to buffer and resend measurement values after the connection is re-established. The following graph gives an overview of this functionality:

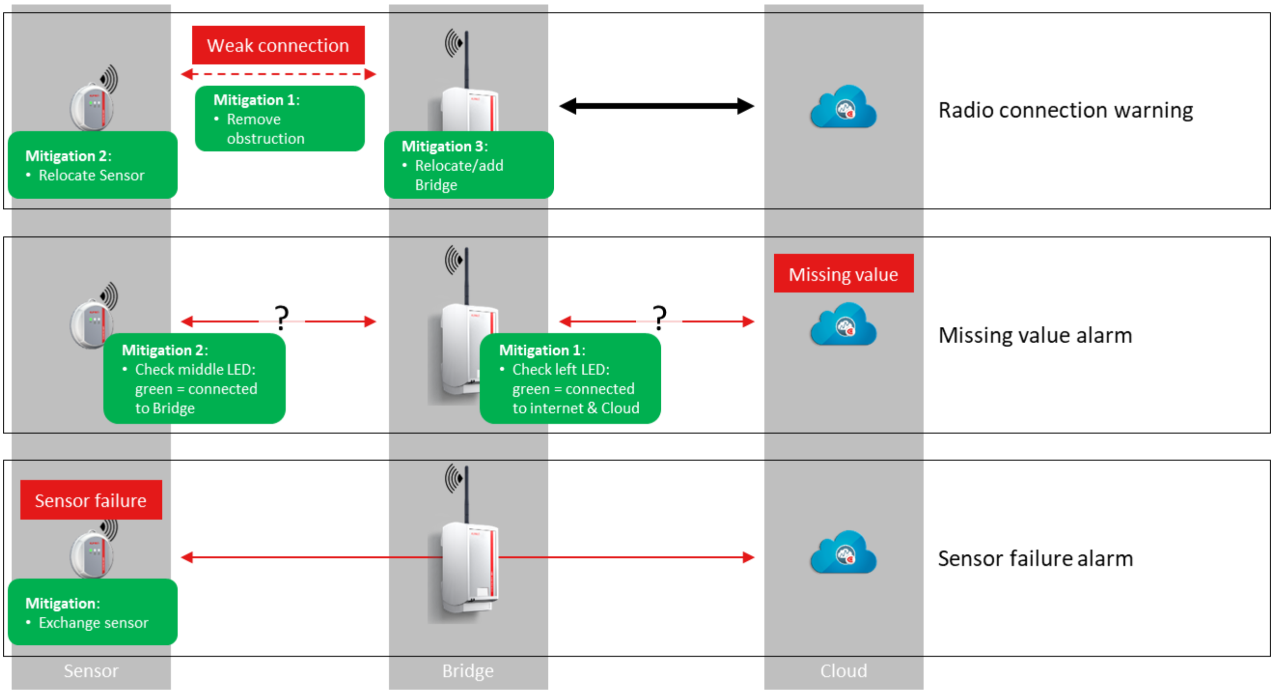


1.8. Monitoring of connection

Once installed and successfully tested, the measurement chain still includes various risks and elements that can be disturbed, damaged or interrupted in operation. It is therefore important that the monitoring hardware (the bridge) constantly monitors the connection of the entire measurement chain and provides meaningful warnings and alarms to the user.

Operational risk	Warning/Alarm	Mitigation measures
Wireless connection obstructed	Radio collection warning Configurable: "Weak" = Warning "Bad"= Warning	▪ Mitigation 1: Remove obstruction (e.g. Pallets) ▪ Mitigation 2: Relocate sensor (see chapter "Micro-position of Sensor" ▪ Mitigation 3: Relocate bridge (or install additional* bridge) ▪ *If more than one communication bridge is within range of a sensor, the sensor will choose the bridge with the strongest connection for communication.
Value missing in the Cloud software	Missing value alarm	▪ Mitigation 1: Check left LED on bridge, green = connection to internet & Cloud established ▪ Mitigation 2: Check middle LED on sensor, green = connected to bridge
Sensor damaged	Sensor failure alarm	▪ Mitigation: Sensor physically damaged or has an internal electronic failure. The sensor must be exchanged.

The following illustration provides a good overview on the warnings/alarms as well as possible mitigations:



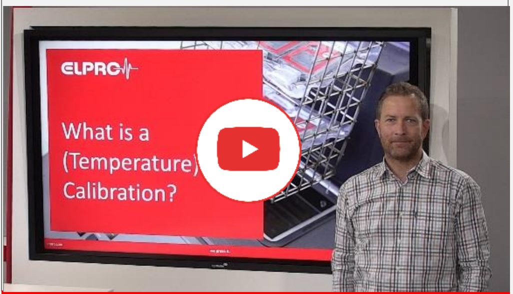
This fact sheet is an addition to our expert guideline to Temperature Monitoring of Pharmaceutical Products.

Most content in this fact sheet can also be found on https://www.elpro.cloud/en/temperature-monitoring/ It discusses the requirements for monitoring solutions in a complex pharma supply chain and sheds light on compliance requirements, the process of qualification and mapping, and the different techniques of calibration.

If you have further questions about our monitoring solutions contact us today at online@elpro.com.

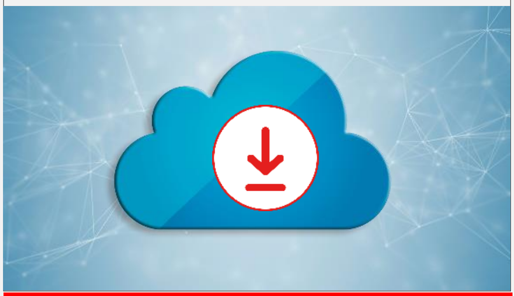
More ELPRO Knowledge online: https://www.elpro.cloud/en/resources

Video Series about GxP-compliant Calibration



WATCH NOW

Checklist for cloud-based Temperature Monitoring



DOWNLOAD NOW