VAISALA

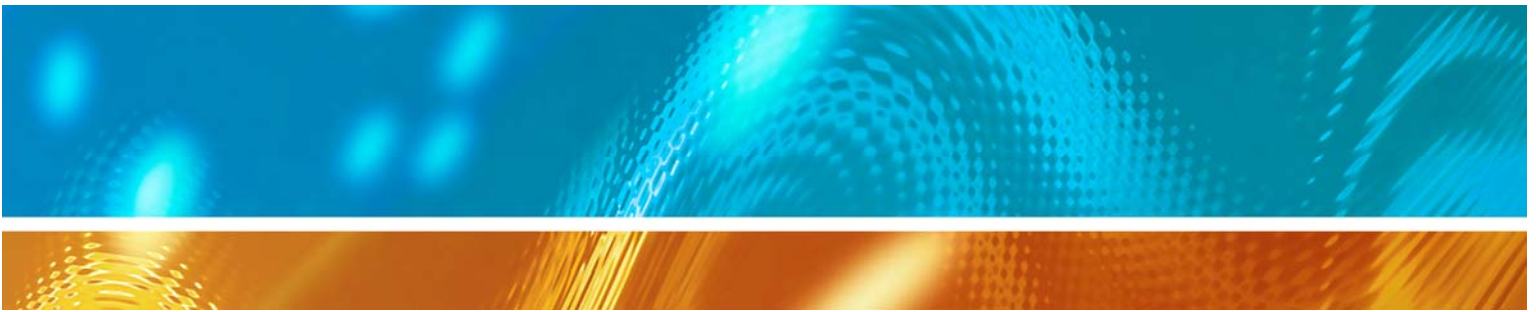# Compliance, Risk and Cost of Ownership Comparisons for Pharmaceutical Continuous Monitoring —
Wired, Wireless and Standalone Monitoring Systems

Compliance, Risk and Cost of Ownership Comparisons for Pharmaceutical Continuous Monitoring — Wired, Wireless and Standalone Monitoring Systems

Executive Summary: Recent agreements between the US FDA and its European Union counterparts to cooperate on pharmaceutical plant inspections to enable stepped up enforcement of safety guidelines require every pharmaceutical manufacturer to be on higher alert to maintain a best-practice focus on quality systems. These agreements will help regulators be more efficient with their resources. Mutual agreement among agencies, combined with a focus on risk-based processes, raise the likelihood of more GxP facilities being audited. Revisiting cost-vs.-benefit analyses for continuous monitoring modalities (wired or wireless networks and standalone monitoring instruments) that facilitate the ability to comply with auditors' requests for proof of regulatory compliance is very timely. Moreover, the ever increasing costs for APIs and the R&D efforts to create them are such that the economic costs of failure in the totality of monitoring systems are greater than ever before. All monitoring methods—whether wired, wireless or standalone instrumentation—need to be scrutinized for systemic weaknesses that allow human error to compromise product quality, system failure probabilities and overall costs of ownership.

This white paper discusses five approaches to monitoring critical environments such as pharmaceutical freezers, stability rooms and warehouses. Quality, facility and IT managers employ different methods for maintaining the quality products and information. This paper and evaluates each the different methods and presents the risks and cost of ownership for each type.

Introduction – Modalities for Monitoring Critical Environments

There are many competing monitoring technologies and brands of systems purporting to provide for regulatory compliance. For purposes of this paper we will examine six modalities for temperature and humidity monitoring: 1) wired systems with UPS power backups; 2) wired systems with UPS power backups and use of PoE (Power over Ethernet); 3) wireless WiFi; 4) wireless mesh; 5) non-networked/standalone data loggers; and 6) chart recorders.

Briefly, chart recorders are the oldest technology — paper-based, and powered either by AC or batteries. Standalone non-networked data loggers also use either AC or batteries, and require manual downloading of data at regular intervals. Wired networking technology has been around for decades. While this technology continues to evolve and remains the mainstay of most pharmaceutical operations, wireless has fast become an interesting alternative. Each method of communicating data has its advantages and disadvantages. When it comes to regulatory-compliant applications involving public health, however, the criteria for using one method over the other should be well understood. The following two charts provide an overview of risk factors and cost-of-ownership differences between the continuous monitoring modalities.

Figure 1 – Risk Factors — Continuous Monitoring Modalities

The following chart provides general guidelines only to risks associated with meeting GMP requirements—click here to apply for an evaluation of current risk factors in your pharmaceutical plants and warehouses.

Risks	Chart Recorders	Standalone Data Loggers	Wired—UPS only	Wired—PoE	Wireless WiFi	Wireless Mesh
Power outage risk impacts to data loss	Moderate (3-yr battery) to High (AC only)	Moderate—3-yr battery and data storage capacity	Low—dependent on device battery maintenance	Low—dependent on device battery maintenance	Low to Moderate—dependent on device and radio battery maintenance	Low to Moderate—dependent on device and radio battery maintenance
Human error risk—Adhering to maintenance schedules	Highest—charts, pens, batteries need frequent attention	High—data downloading before overload capacity and battery life	Lowest	Lowest	Low (if AC-powered)—Higher (dependent on battery replacement frequency)	Moderate—unpredictable drains on battery life require more frequent attention
Data security risks	High—paper chart data can be manipulated	Low	Low	Low	Moderate—access to data possible from outside facility	Low—proprietary networks prevent easy access
Risk of gaps in data records due to network downtime	Not Applicable	Not Applicable	Low—with redundant data capability, otherwise high risk	Low—with redundant data capability, otherwise high risk	Low—with redundant data capability, otherwise high risk	Low—with redundant data capability, otherwise high risk
Risks of IT training gaps and breakdown in IT staff turnovers	Not Applicable	Not Applicable	Low—Ethernet protocols widely understood	Low—Ethernet protocols widely understood	Low—WiFi protocols widely understood	Moderate—proprietary networks requiring additional training
Combined sources of human error posing risks to quality	High—frequent staff hours required to stock supplies, change paper & pens; check readings; retrieve records	Moderate—adherence to data download schedules required and to check for excursions and/or change batteries	Low—requires adherence to schedule of changing device batteries	Lowest—system least dependent on battery maintenance	Low—requires adherence to schedule of changing device batteries	Low to Moderate—requires adherence to schedule of changing device batteries and IT training on proprietary protocols

Figure 2 – Costs of Ownership Factors—Continuous Monitoring Modalities

The following chart provides general guidelines only for some of the more salient factors affecting costs of ownership related to the six monitoring options. Varying plant sizes and scale of operations affect the impacts of various cost factors. Click here to apply for an evaluation of total costs-of-ownership for the continuous monitoring systems currently in your pharmaceutical plants and warehouses.

Cost of Ownership	Chart Recorders	Standalone Data Loggers	Wired—UPS only	Wired—PoE	Wireless WiFi	Wireless Mesh
Inventory costs required for operation	High—paper, pens, batteries	Moderate to Lowest with 3 to 10-year battery systems	Moderate to Lowest with 3 to 10-year battery systems	Moderate to Lowest with 3 to 10-year battery systems	Moderate to Lowest with 3 to 10-year battery systems	Highly variable depending on need to change batteries
Labor required for operation	Highest—daily or weekly maintenance	High—frequent data downloads	Low	Low	Low	Variable—dependent on need to change batteries
Costs for adding AC power or network cabling	Low	Low to Moderate	Low to Moderate	Low to Moderate	Lowest	Lowest
Labor costs for audit compliance	High—deviation reporting and manual retrieval & compilation of records	Moderate to High—deviation reporting and labor to show complete records	Lowest (with redundant data capability) to High (without redundant capability)	Lowest (with redundant data capability) to High (without redundant capability)	Lowest (with redundant data capability) to High (without redundant capability)	Lowest (with redundant data capability) to High (without redundant capability)
Energy and/or battery costs	Low to Moderate—dependent on battery type	Low to Moderate—dependent on battery type	Low to Moderate—dependent on battery type	Lowest—no local battery or AC, power required for PoE devices	Low to Moderate—dependent on battery type	Low to Moderate—dependent on battery type
Potential costs from human error	Highest—requires frequent human intervention	High—requires frequent human intervention	Low with redundant data, remote alarming & infrequent battery changes; High without these capabilities	Low with redundant data, remote alarming & infrequent battery changes; High without these capabilities	Low with redundant data, remote alarming & infrequent battery changes; High without these capabilities	Low with redundant data, remote alarming & infrequent battery changes; High without these capabilities

We will now examine each of the six modalities and their challenges and advantages.

Paper-Based Chart Recorders

In the last decade, nearly every leading pharmaceutical company that had relied on paper chart recorders has either replaced them with one network-based system or another or is in the thinking stages to do so. Chart recorders can still be found in the marketplace that cost as little as a few hundred dollars. Most pharmaceutical quality managers consider this obsolete technology due to both the considerable costs of maintaining chart recorder-based monitoring systems, and the obvious risks of handling paper-based records and limited or no alarm notification. It does not go unnoticed that chart recorders rely on humans for daily or weekly checks to replace paper, check pens and write deviation reports. In any event, costly staff hours must be devoted to tracking which charts need to be changed when, and which batteries need to be changed, in what intervals. AC-power based chart recorders without batteries offer no ability for continuous data records in the event of power outages.

The possibilities for human error are multifold.   At the time of this writing there have been no known instances of regulators rejecting chart recorder based monitoring systems. However, regulatory agencies encourage the move away manually-intensive processes to more automation with the purpose of tightening up quality systems, and make better use of quality resources.

Standalone Data Loggers

Unlike paper chart recorders, standalone data loggers are not as likely to break. They do however incur considerable labor costs for manually downloading data, especially in large plants where hundreds of data loggers are required to ensure environmental standards in both processing and storage areas. These costs are magnified in the current environment where inspection-readiness can be an issue. (Remember the new 15-day period that the FDA requires for responding to observational deficiencies.) Operational costs for complying with regulators requests for information and the interference on normal operations that audits can involve can be considerable. As with chart recorders, the capability to access accurate and complete records throughout the record retention period as required FDA 21 CFR Part 11 and EU GMP Annex 11 may be compromised if it takes too long to the locate records or they are incomplete.

There are also multiple human-error sources with standalone data logger based systems. First, staff may neglect to download data before the storage capacity of the instrument is exceeded. Secondly, battery-powered standalone data logger systems also require ongoing monitoring of batteries, which also creates an opening for lost data, even when so-called battery alerts are in place, because someone has not been there to see it. Third, AC-powered data loggers without batteries may not provide gap-free records in the event of power outages.

If one thinks of technology investments as ways to automate routine tasks to eliminate the costs of labor and potential error, any time there is human intervention standalone data loggers do not generally pass muster. The reliance on human labor to download data, investigate deviations because they were not seen in time, and maintain these files

opens the door to regulatory objections and the staggering costs that ensue with production delays. With the exception of monitoring the contents of a few chambers, standalone recorders put undue risk on companies over other monitoring methods that automate more procedures and reduce reliance on human systems.

Wired Networks – With and Without PoE Capabilities

The pharmaceutical industry, like many others, has long relied on a wired infrastructure using Ethernet standards for making the connection to transmit and receive data. A hard-wired network allows communications to proceed securely and continuously with few possibilities to intercept or interrupt the flow of data.

Uninterruptable Power Supplies (UPS) ensure that servers are always available for data exchange. However, a potential problem with data continuity of monitoring controlled environments arises with a power outage to the facility. The UPS maintains network uptime but devices connected to the network may be without power, which could mean loss of critical data. Until recently, traditional wired networks lacked a cost-effective alternative to maintain data flow with these critical devices.

Power over Ethernet (PoE), originally implemented for voice over Internet (VoIP) technology, allows electrical power and data to travel on the same Ethernet cable. Since 2003, companies have been integrating data and power standards on the manufacturing floor with PoE (IEEE 802.af) capable devices. The advantages to deploying a PoE network are many: 1. Saves the cost of running additional AC power, which usually requires a licensed electrician, aided by the low cost of network switches with built-in PoE power capability; 2. Provides greater flexibility to locate devices around the plant because they can be installed wherever a LAN cable can be run; 3. Increases data communication protection from power outage because the server's UPS provides backup to PoE connected devices; 4. Uses less energy and managed from a central location; and most importantly; 5. Protects critical data through the outage period. With PoE, security, maintenance and access can all be managed within an existing IT framework because staff is trained on setting up and maintaining communications networks based on worldwide standards.

Wireless Networks – WiFi and Mesh

For many pharmaceutical plants, and especially those in older facilities where there are difficulties in running Ethernet cabling, wireless communications can be a convenient and cost effective method of connectivity. Ease of installation, reduction in cabling cost, measurements in inaccessible areas are among the major factors driving the adoption of wireless networking.

Unlike the wired 802.3 international standard, several wireless communications protocols have emerged including the popular wireless version of Ethernet, commonly referred to as WiFi (802.11b and more recently 802.11g). Other network methodologies used for monitoring include a mesh structure based on the Zigbee (802.15.4) protocol. WiFi is often the wireless system of choice because it uses the same IT infrastructure already in place in an organization. Wireless mesh (Zigbee) is a network architecture that uses access points or nodes to communicate with one another as well as with the

host. It is designed to detect a degraded signal at one access point and reroute it to another nearby access point. Nodes have a low power requirement, which has the expectation of less drain on battery life but at the same time low power inherently means less signal strength than WiFi. The low power requirement of Zigbee networks also means that there needs to be a sufficient number of nodes to maintain continuous data flow.

Whether WiFi or wireless mesh, the greatest downside is the possibilities for network interruptions such as those that occur when lift trucks move throughout a plant or when inventory is re-arranged, equipment is moved out of range or other potential obstacles to transmission and in turn the ability to ensure gap-free records. Fixed obstacles that could block the signal can be overcome using a sufficient number of wireless access devices. Intrusions from a fork lift or storage equipment such as water-based gel packs or office modifications may not be so well anticipated.

Figure 3 – Topology of WiFi and Mesh Wireless Networks
WiFi devices connect directly to the company network and uses WiFi access points to transmit data to a central host (server). Mesh devices connect to a gateway that can either host the data or forward to a central server.

Wireless mesh network topology   Wireless WiFi network topology
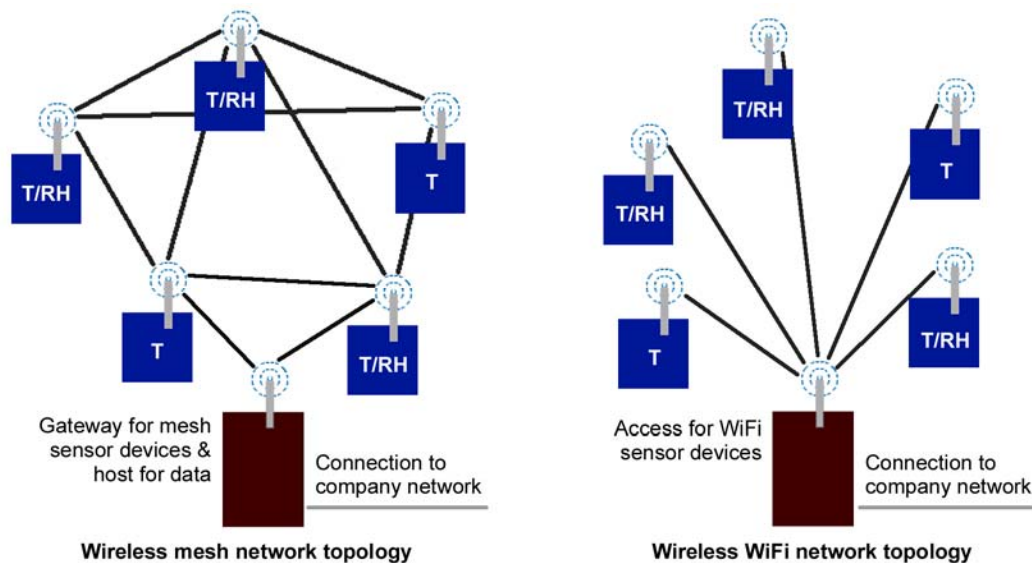
The range for a wireless device is largely dependent on radio strength, which is also tied to the battery power. Installations using wireless monitoring technology have to accommodate signal range and barriers, which become important factors when continuous data is required. It can mean, for example, that more wireless devices are needed (and greater upfront cost) to ensure network transmission integrity in all situations.

With wireless mesh networks, signals are diverted to maintain data flow but this increases the load on other nodes picking up the signal, having implications for reduced battery life in unpredictable ways. These type systems need a vigilant source for detecting and alerting for low battery issues well before data is lost.

With wireless systems, signals carrying critical data can also degrade from interfering sources such as other devices communicating in the same 2.4 GHz band (WiFi & Zigbee), and in today's pharmaceutical plants this especially includes security cameras, microwave ovens and Bluetooth devices. Wireless mesh is a proprietary network that needs to be integrated with the different standards of the existing infrastructure—involving IT hours, which potentially impact costs of ownership.

The batteries used in wireless devices are specified with 'up to' so many months or years of life. The 'up to' condition is often stated for ideal or laboratory conditions. This is because there are no typical operating conditions where power consumption can be calculated. Devices draw down battery power with each transmission, which includes the frequency of measurement updates established by the user, events such as alarms or communication problems brought on by many circumstances including a blocked access device. Battery drain is even less predictable in a mesh infrastructure. For example, when the signal between a temperature device and node is blocked another nearby node picks up the signal for transmission. It now adds the new transmissions to those from other measurement devices it was already communicating with. The extent to which a wireless network requires battery replacements re-introduces human error potentials into what are assumed to be relatively error-proof automated systems.

Most connectivity methods have low risk of losing data when the time between real-time updates for data and alarms is long. For example, the initial requirements of a monitoring system may not have needed frequent data updates, but at some point someone may want to know if a chamber door was left open or other behavior that led up to a temperature excursion. In these instances, a faster sample rate would be needed, requiring more transmissions and thus making more demands on the battery. Reduced battery life is well and good if SOPs can anticipate the need, staff has the time for required maintenance without fail, and the expense of more frequent service (labor hours, replacements) are not burdensome. Some devices provide low battery indicators and alarms. However, the question is: What happens to data if batteries are not replaced in time? Moreover, it is highly probable that data will be lost in systems that use the same batteries to power both the wireless radio and data memory electronics. Battery life therefore is not a minor specification but in fact has great impact on the ability to ensure compliant gap-free records and minimizing impacts of human error on quality assurance systems.

Data Redundancy

Whether deploying a system of standalone devices, or a wired or wireless network for monitoring critical environments, the need to have a continuous record of data and events are the same. There will be times when the facility experiences network and power interruptions, among other unexpected disruptions. Assuming the need for a continuous record of quality, the monitoring system should be capable of filling in a database when temperature, relative humidity, pressure and other data cannot be communicated in real-time. This is nearly impossible and impractical with standalone monitoring instruments, making them obsolete technology.

In networked systems, recording data independently at the point of measurement is one key factor in protecting data. A system capable of identifying the time period of a

communication interruption and bringing in data and events to fill the gap is essential to ensuring complete and accessible records. This assumes measurement devices have calibrated time-base clocks (specified with an accuracy over a temperature range) to ensure correct time/data recording. The capability to backfill data after power or network interruptions ensures a continuous record of data and events. Completeness of records also assumes there is an audit trail to capture all system events. Documented evidence of data and events during an outage will reduce quality management's involvement in having to review excursions and investigate deviations. Gap-free records save time during and after an audit, reduce unnecessary staff involvement and limit disruptions to ongoing production and shipments.

Data Security

There are two aspects of security that regulatory compliance (21 CFR Part 11) requires: protecting data from unauthorized access, and preventing alteration to data. Secure data begins at the measurement device and ends at a designated collection point, usually a network server. Secure access refers to specific levels of permission given to authorized users and other protocols for ensuring authenticity.

Devices communicate using protocols or common rules for data format and can be either open (public) or proprietary. An open protocol means just that—anyone who knows the rules can potentially access the files. A secure monitoring system ensures that the measurement device has a secure protocol in addition to other authentication and confidentiality features. This is a major factor in how and why communicating over wire is inherently more secure. In wired systems devices are only accessible within the building. A wired network can potentially be compromised only by someone who has already gained access to the facility.

On the other hand, wireless communications is inherently less secure and requires additional measures to maintain protections. Wireless devices are also manufactured with security features built in but may not be upgradable to the changing standards or security requirements of an organization. A capital investment made now may need replacement in 2 years time. Non-standard proprietary wireless networks require IT training and increased risk due to IT staff turnovers.

Conclusion: Quantify Risk and Cost

Whether you use standalone monitoring instruments or wired or wireless connectivity for your temperature and humidity measurement devices, it is important to understand the limitations of each methodology. For the most part, the significant labor costs involved in standalone monitoring devices combined with the multiple ways in which such systems insert human error potential make them less than desirable compared to more automated network-based monitoring technology.

Wireless communication has the advantages of being flexible to install and providing for monitoring of environments that either have limited access to running cable or where refrigerators, freezers or other monitored storage units are moved on a frequent basis. Wired networks have the advantage of speed, security and data redundancy. Generally speaking, if your goal is to reduce the risk of data loss to zero or nearly so, then wired

systems are the best course. The lower upfront cost of wireless can disappear quickly if you have to write deviation reports from missing data, experience product loss or regulatory missteps. The good news is that connectivity technologies can be mixed—wired and wireless, solving the physical installation challenges that many facilities pose.

Of course network connectivity methods alone do not maintain product quality. They have to be used in conjunction with the capabilities of the facility's monitoring system, with specific attention to automating records—data, events, audit trail—that present a continuous gap-free history.

The details of how humans interact with systems—whether driving lift trucks, replacing batteries, downloading data, etc.—are important factors in determining if a particular continuous monitoring technology truly minimizes risks introduced by the inevitability of human error. You have to weigh the costs of potential problems versus how much your organization is willing to invest to protect your operations. Risk really comes down to consequences or the implications of system failure. Analysis of risk is both qualitative and quantitative. Ideally, you should be able to answer the following questions:

- Can you afford to handle the expense of downtime? This can be in the form of missing data, equipment failure or human error.
- For an unplanned production stoppage, how long will it impact other research, production or shipments?
- What is the financial impact of losing product or research specimens?
- Can you define downtime cost either by time, lost production, blemish to reputation or other stakeholder pain?
- Can you identify single points of failure and ways to reduce them?
- Does it cost more to recover from equipment failure, product loss, internal and external reviews and other unplanned interruptions than it would to invest in continuous operation?

For assistance in answering these questions, click here to apply for an evaluation of total costs-of-ownership for the continuous monitoring systems currently in your pharmaceutical plants and warehouses.

Sources

- http://standards.ieee.org

- http://www.veriteq.com/chart-recorders

- Part 11 US CFRs, EU GMPs, ICH Guidelines

- http://en.wikipedia.org/wiki/Power_over_Ethernet

- http://en.wikipedia.org/wiki/Wireless_security

# # # # #

About Veriteq, a Vaisala company

Veriteq is a part of Vaisala, global leader in environmental and industrial measurement. With solutions that deliver fail-safe records for temperature, humidity and other parameters, we provide high performance solutions for validating and monitoring strictly-regulated and other controlled environments. Vaisala acquired Veriteq in April, 2010, building on more than 70 years of reliability in measuring critical environments. Headquartered in Finland, Vaisala is listed on the NASDAQ OMX Helsinki. www.vaisala.com

www.vaisala.com/veriteq