

FACILITY MONITORING SYSTEM DESIGN RECOMMENDATIONS



TECHNICAL NOTE TCC-170 (US)

Introduction

A monitoring system is referred to by a number of different names, a Facility Monitoring System (FMS), a Continuous Monitoring System, an Independent Monitoring System (IMS), and an Environmental Monitoring Systems (EMS). For clarity throughout this document the simplified term of a Monitoring System will be used. When you see the term “FMS” this will be referring to the TSI FMS monitoring software.

The main purpose of a monitoring system is to collect data from many sensors distributed at critical locations throughout a manufacturing process, and are defined based on the principles of quality risk management QRM ICH Q9. These are locations where there is greatest risk of contamination or adverse environmental conditions impacting product quality, and in life science applications patient health. Collecting the data and ensuring its integrity is the first step; the data must then be presented as useful information to the end user. Trend reports and immediate notification of a loss of process control or an adverse trend or event all lead to enhanced process understanding and improved product quality.

To this end, it is critical that a monitoring system operates in a reliable and stable manner. Uninterrupted data collection must be the number one priority in any Monitoring System design philosophy.

Scope

The purpose of this technical note is to define monitoring system layout and designs (topologies) that are known to work reliably and have minimal installation or integration overhead.

This document will not cover sensor positioning, sensor selection, sensor enclosure design or remote vacuum system design.

It is a prerequisite that any system integrator to be confident and familiar in:

- TCP/IP network installation
- TCP/IP network maintenance
- TCP/IP network troubleshooting
- SQL database installation and maintenance



Objective

Having read this document the reader will have an understanding of the following:

- FMS software architecture fundamentals
- Software components that can be used to build and design a reliable and robust Monitoring System
- FMS topologies that are supported by TSI and are known to work well and reliably
- The risks associated with the use of non-standard components and system topologies
- The minimum technical skill level required to design, install and commission the different system topologies covered in this document

FMS Software Architecture Fundamentals

FMS is a client server application. There are different programs that communicate with each other over TCP/IP networks. There are three main programs. Please be aware that these programs can be referenced by many different names, especially the Monitoring Engine Server which can cause confusion. For consistency this technical note will use the simplified terms as detailed in the table below:

Program Name	Alternative Names	Simplified Term	Definition
The Monitoring Engine Server	Node, monitoring node, Instance of monitoring, monitoring engine, monitoring task, monitoring server, FMS server, FMS monitoring Server	Monitor	Basic control of monitoring system equipment such as digital and analog IO modules and particle counters. Collects data from sensors, stores the results in a database, and detects alarm conditions. It performs various actions in response to a range of events.
The User Interface	Client, FMS Client	Client	Main user interface with FMS, this application displays the status of the system, the configuration of monitoring servers can be controlled and alarms acknowledged. Reports can be generated from the data stored on the SQL database.
An SQL Database Server	Database	SQL Database	The SQL database server is the application that stores the collected data. There are several types of SQL server. FMS standard database is PostgreSQL. Applications other than FMS can also access a SQL server to generate reports. SQL servers usually have comprehensive security features to control access and can include encryption.

Although there are several different programs, the only user interface a system operator uses on a regular basis is the Client. The other applications run in the background. (The database has a user interface; however this is only periodically accessed for setup and maintenance purposes by database administrators). This means a whole system can run on just one computer. However, it is possible for each program to run on a different computer. There are advantages to running the SQL Database on a different computer, especially in distributed system designs when robust monitoring is required.

It is possible to have more than one Monitor running. This can be on one or more computers. For example, you might have one Monitor collecting data from Process A and a second Monitor collecting data from Process B. The advantage is that you can segregate all validation and support activities for these processes.

A single SQL Database server can be shared with multiple Monitors; each Monitor will have its own separate database within a single SQL Database server. On a single subnet up to four concurrent Monitors including watchdog monitor (Buddy) are supported. Up to six Clients connected to a single monitor are also supported. Contact TSI if you are looking to implement more than clients on a subnet than this.

Each client can see all monitoring servers on a network. It is possible to partition the network to limit Monitor visibility if desired.

In summary the distributed nature of the FMS software components means there are many system software component topologies that can be implemented. We will not detail them all; however, we will recommend topologies that are known to be robust and function reliably.

TSI cannot anticipate risk scenarios associated with pursuing topologies not detailed within this technical note. The end user and system integrator are responsible for managing technical and commercial risk using the principles of quality risk management. Contact TSI to discuss the technical topology and software issues involved with potential alternate topologies.

Standard Components

Please see technical note *Authorized Components for FMS Software TCC-168*. This technical note details recommended hardware and software components that are supported as standard by TSI. Hardware includes particle counters, analog input devices, digital input and digital output devices. The importance of this information cannot be overstated. The commercial risks associated with using non-standard hardware or software may result in some or all of the following:

- A non-functioning system
- On-going system maintenance and reliability issues throughout the system lifecycle
- Late delivery
- Increased delivery costs
- Lengthy site commissioning activities
- Additional, fee-based support from TSI

Design Constraints

TSI alerts system integrators to the following system software design constraints:

Virtual Machine (VM) Implementation

Briefly, VMs emulate a physical computing environment. Because VM environments work by time-sharing host physical hardware, they cannot exactly duplicate the timing activity of physical machines.

FMS is a real-time monitoring system that relies on the underlying operating systems ability to keep accurate time. If the operating system is unable to do so, it can hinder FMSs functionality.

On an operating system that is unable to keep accurate time, if the IT department syncs the time often enough, FMS will be able to function normally. However, TSI cannot make a recommendation i.e. “sync your clock every x hours,” because the severity of the clock drift will vary from site to site. Some sites may only need to sync the clock daily other sites may need to do it hourly. When the underlying operating system updates the clock, if Monitor detects a clock update of more than 100 seconds forward (a slow clock), or more than 1 second backwards (a fast clock), Monitor will restart.

In summary, TSI only recommends running any FMS software components in VM environments at facilities where their IT department is capable to *internally* manage clock drift.

Integrators should also be aware that an instance of Client must be running for scheduled reports to function.

Remote Desktop or Terminal Emulation

There are many applications on the market today which can enable access to a single Client from remote desktop sessions on multiple remote computers. End user should be made aware Computers can be exposed to external environments and time synchronisation can occur during a remote desktop session.

TSI has not formally tested FMS Client functionality via remote desktop sharing software and cannot guarantee functionality.

Virtual Private Networks (VPN)

Enables a computer to send and receive data across a public network such as the Internet as if it is directly connected to a private network.

This is typically used to enable employees to access a company’s network when travelling outside the office or working from home. TSI has not tested the Monitor, Client or SQL server via VPN and cannot guarantee functionality.

TSI does not recommend that the Monitor and SQL database communicate with each other over VPN. There are known issues with database periodic spooling or clock skew errors occurring which could result in the monitor stopping.

Databases

TSI does not recommend that system integrators assume the role of database administrators for the FMS system once installed.

PostgreSQL is the standard database supported by TSI with FMS. SQL databases are widely used and well understood by end user IT departments worldwide. For SQL database backup/restore, master/slave databases or database replication we strongly recommend involving the end user IT department and database administrators. They will have specific site disaster recovery policies and approaches they will want to adopt.

System Topologies

FMS has distributed architecture. This is a key differentiating feature of FMS and is a powerful advantage. But, there are too many permutations for TSI to test, and that TSI will support as standard.

TSI recommends standard system design topologies as a control measure and a risk reduction strategy to reduce the probability of the following risk scenarios occurring:

- A non-functioning system
- On-going system maintenance and reliability issues throughout the system lifecycle
- Late delivery
- Increased delivery costs
- Lengthy site commissioning activities
- Additional, fee-based support from TSI

This technical note covers three system topologies, starting with the easiest first and most difficult last.

1. Simple System
2. Simple Distributed
3. Complex Distributed

NOTE

SMS outputs and AutoDialer functionality are not exclusive to complex distributed systems. This functionality can easily be implemented into the Simple and Simple Distributed system examples.

(continued on next page)

Simple System

Commonly used for small to medium sized monitoring systems; hospital pharmacies for example. The end user's LAN is not used.

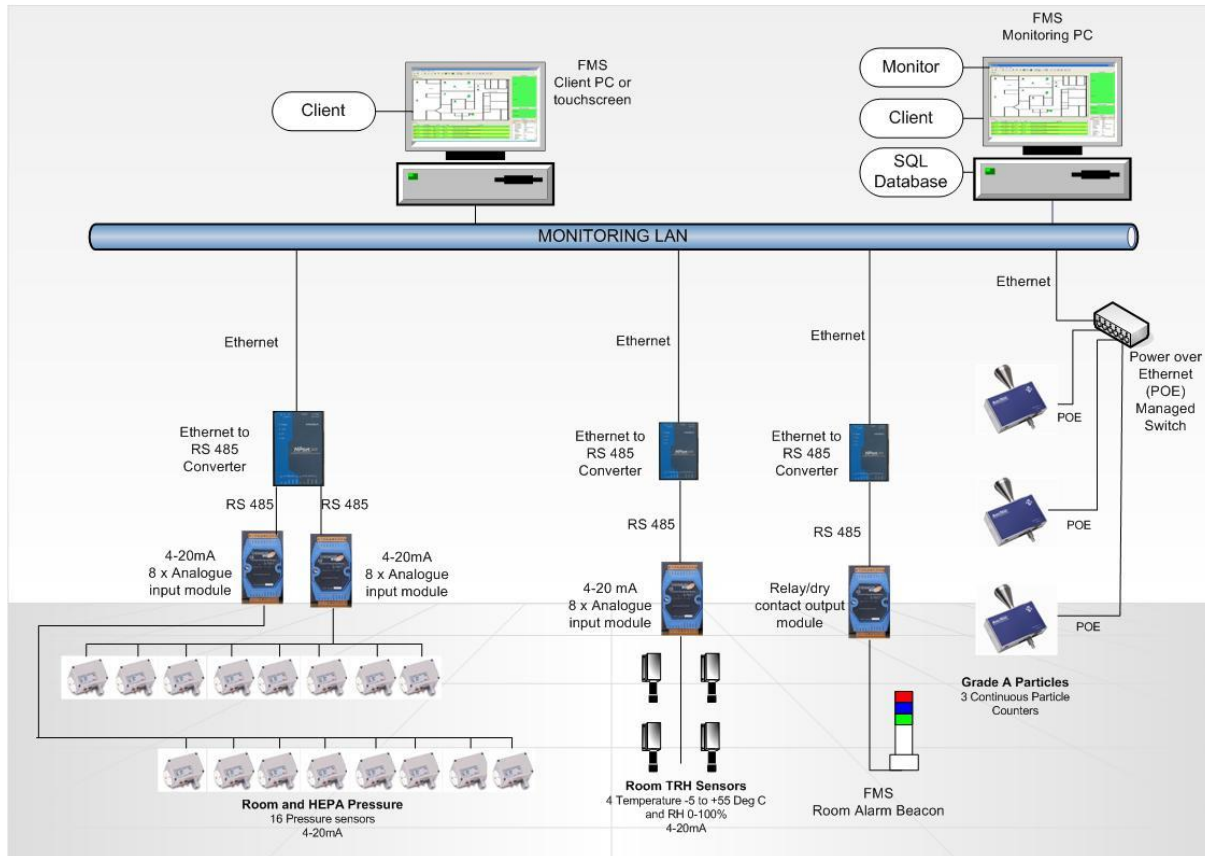


Figure 1: Simple system schematic: ICP CON Input/ Output I/O devices are shown; PhoenixContact I/O devices can also be deployed

The simplest monitoring system implementation is to have FMS Monitor, Client, and SQL database reside on a single computer.

The schematic shows an additional computer with a Client installed to allow the Monitor to be accessed at a second location in the facility. Other key points to note:

- There is only one network; all the system sensors are connected to this network. This is called the Monitoring Network or Monitoring LAN (Local Area Network).
- All sensors are communicating to the Monitor program via Ethernet.
- The Client, Monitor, and SQL database are installed together on a single FMS Monitoring computer.
- The FMS monitoring computer is **NOT** connected to the end users network or LAN.
- The SQL Database is the standard PostgreSQL database recommended for use with FMS.
- Additional Clients may be installed on dedicated computers or a touch panel/screen computers on this closed network. Note: we would not recommend configuring FMS from a touch screen interface as the onscreen keyboard will need to be used.

Sensors

An important principle is introduced here; TSI recommends keeping all sensing hardware on a closed separate Monitoring LAN. It is possible to install sensors on the customer's LAN; however, it is important to remember that this is a critical monitoring system, all stakeholders must fully understand the risks of installing sensors on the company-wide LAN from the beginning. The following must be taken into account:

- Fixed IP address will be used for all the monitoring hardware.
- The customer may have varying levels of control over their LAN (this control is sometimes outsourced).
- IP addresses may be introduced at a later time by the IT department that will unknowingly clash with one of the monitoring system IP addresses.
- Other changes may be made to the end user's LAN that could increase network broadcast traffic, which can lead to:
 - Putting critical data collection at risk
 - The network performance deteriorating
 - The network performing unpredictably

By having the monitoring sensing hardware installed on a separate LAN, it allows you to retain control over any network traffic and changes made to that network.

Computers

For minimum computer specifications, please see TSI Technical Note TCC-169, *Minimum Computer Requirements for FMS Software*.

Poor selection of a computer can lead to poor system performance and reliability issues.

TSI strongly recommends that stable computers are sourced. These computers should be built with quality components that are known to work with each other. The computer vendor will have tested the computer prior to delivery and must provide supporting documented test evidence.

Often, buying a computer from a vendor will come with pre-loaded programs. TSI recommends that the computer has a clean installation of the operating system, i.e., no preloaded programs on the computer, and the computers sole purpose is FMS. Keeping additional programs to a minimum is important.

Networks

The network cabling and computer network configurations are very important. Cutting corners here could lead to system problems that will be very difficult to diagnose and resolve once installed.

- Minimum network speed needs to be 100BASE-T.
- Configure Firewall exceptions for broadcast request and database ports—this information is in the FMS installation instructions and is **VERY** important as the Monitor, SQL Database, and Clients all communicate via TCP /IP and will be blocked or may behave in an unpredictable way if the firewall is incorrectly configured.
- Managed Switches are recommended when the FMS Monitoring network needs routing or segregating
- A minimum specification of Cat5e data cabling should be used. Ensure that cable routing and labeling follow end user site best practice requirements.
- Most importantly, TSI strongly recommends that each network cable is bandwidth tested using a "Qualification" cable tester. (CableIQ from Fluke or similar). All network cabling should be qualified to "Fast Ethernet (100BASE-TX)" requirements.

Configuring a Monitoring System

Maximum sample points per monitor of 150 is advised but is not mandated. For systems requiring more than 150 sample points per monitor please consult the factory.

One factor influencing the number of sample points is the display size and resolution. For large numbers of sample points it good practice to consider dividing the system into smaller discrete monitoring systems. This makes the overall system easier to support and maintain. Be aware that it is not possible to include sample point data from multiple monitoring systems into one report.

Consider use of languages, ensure regional settings and database are configured to allow the required character set.

Remote Particle Counters—Additional System Design Considerations

It is well understood and widely accepted in life science applications that 1 cuft (1 minute) samples are collected by remote particle counters, so that alarms may be generated based on a contamination event. It is often the case that the customer will want to also collect the counts per m³ data simultaneously. In order to accomplish this FMS collects ~36 x 1 minute samples (= 1m³) then posts a counts per m³ result. FMS then discards the first one minute sample collected and then adds on to the end of this 36 min window a new result, the counts per m³ result is then updated. This is commonly known as the “Rolling m³ buffer”, and this functionality exists within FMS. Importantly, in order to collect counts per cuft and rolling m³ data simultaneously you will need to ensure you have allowed 2 sample points per TSI remote particle counter.

Database Considerations

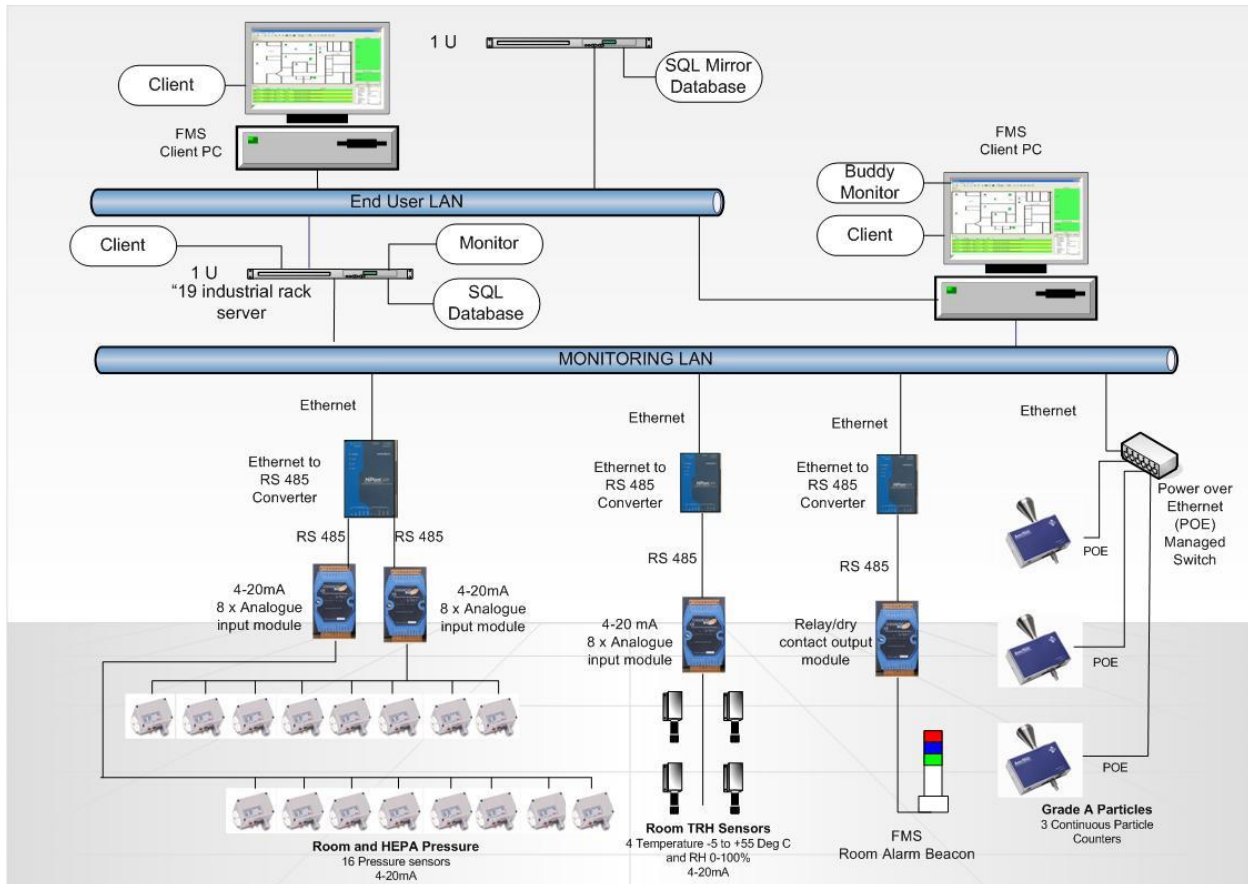
TSI recommends integrators are familiar in SQL database installation and maintenance.

TSI does not recommend that system integrators assume the role of database administrators for the FMS system once installed. For SQL database backup/restore, master/slave databases or database replication we would strongly recommend involving the local end user IT department or database administrators. They will have specific site disaster recovery and data archiving policies they will want to adopt.

(continued on next page)

Simple Distributed System

This topology is commonly used in medium sized pharmaceutical or life science facilities. This design utilizes the FMS Buddy automatic hot standby in the event of a monitoring computer failure. The end user's LAN is used to make system data available to users and archive the FMS data in real time.



Simple distributed system schematic

This is the SAME monitoring system as the Simple System; the same physical parameters are being monitored. The main difference here is that the robustness features of the FMS software are being implemented.

These are:

- Buddy Monitor—Hot automatic standby monitoring system—**Note:** This will support up to three monitors. The buddy is a watchdog; it watches an instance of Monitor and should it fail, will automatically launch a copy of the Monitor it is watching. **Note:** Buddy is only supplied with a single sample point license. If the end user needs to view the Monitor on the Buddy computer, an additional unlimited sample point Client license will need to be purchased.
- SQL Mirror (second) database—This is real-time writing of data to a second (mirror) SQL database. **Note:** The mirror database does not synchronize data with the main database. FMS is simply writing data to two separate databases at the same time.

The requirements detailed previously with the simple system still holds; however, there are some additional considerations when implementing a simple distributed system:

- For a robust monitoring environment it is required that all Monitors, Clients, SQL databases, mirror SQL databases, and Buddy Monitors will have static IP addresses. All Ethernet to RS-485 converters, Ethernet I/O devices and particle counters will have static IP addresses.
- Windows® operating system updates must be turned off and implemented in a controlled way. **Note:** *At each FMS release, TSI will detail any known issues with Windows updates.*
- Ensure any virus checking software if installed, has the appropriate exceptions configured.
- TSI strongly recommends designing a monitoring system to allowing remote access to facilitate remote support. Typically remote access is enabled and disabled by the end user as needed.

Computers

For minimum computer specifications, please see TSI Technical Note TCC-169, *Minimum Computer Requirements for FMS Software*.

Same as Simple System, plus:

- Common programs such as the SQL Database, Monitor and Buddy Monitor must be available to the Monitoring LAN and the End User LAN. Since the computer with these programs installed on it requires a connection to two networks simultaneously, the computer needs to have either two network interface cards or a dual network interface card.
- Data integrity consideration should be given to installing dual hard drives that are mirrored (RAID 1) on the computer where the database resides.

Networks

The same requirements as detailed in the Simple System section apply with some additions detailed below:

- The PostgreSQL databases should be installed on a stable computer as defined in the Computers section, poor PostgreSQL database computer performance may cause system reporting and data integrity to be impacted.
- If using MS SQL database, the database configuration must allow for FMS functionality, e.g., multiple simultaneous connections. PostgreSQL databases are auto-configured by the FMS installer and will have optimum configuration automatically set.
- Ensure all computers on which all monitoring system software components are installed are using the same time server and time zone.
- TSI Recommends disabling daylight savings on the operating system on all computers, to avoid gaps and overlapping data.

Configuring a System

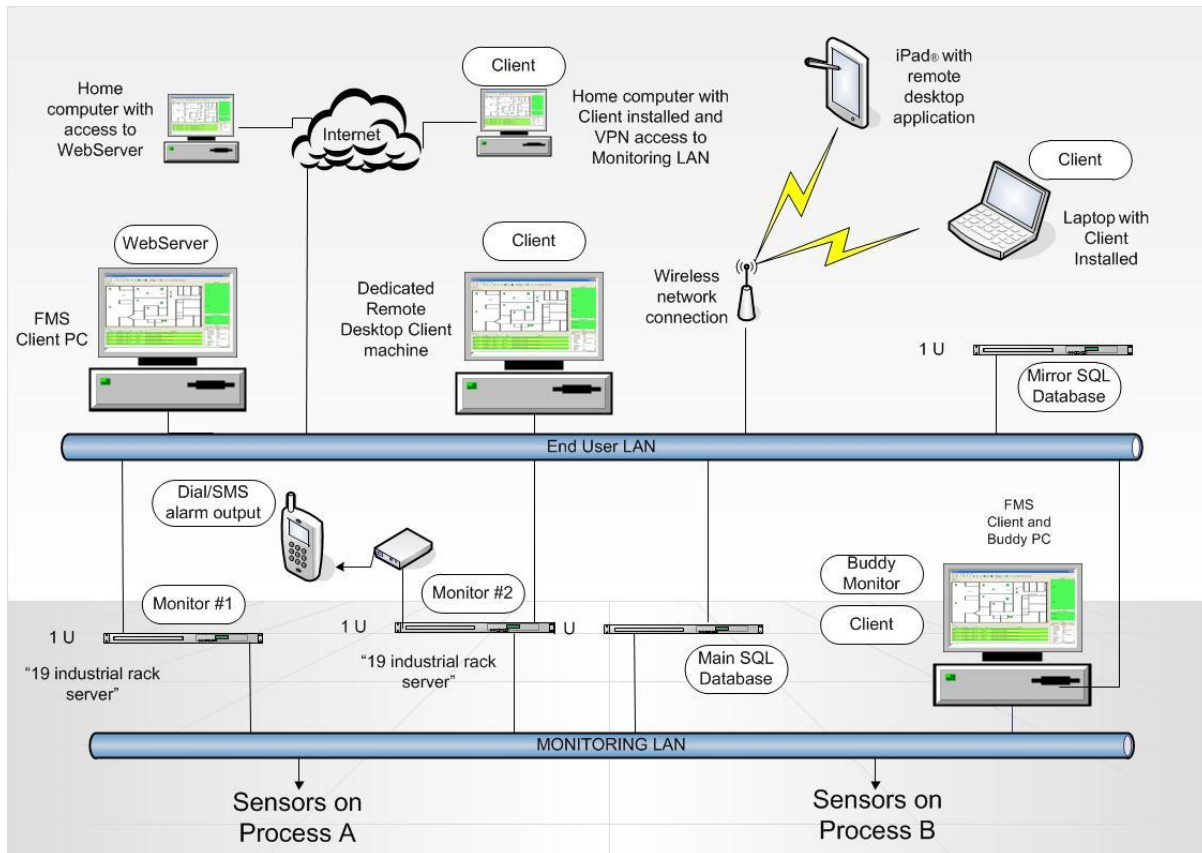
- It is strongly recommended that the Buddy Monitor configuration is regularly (at least every day) synchronized to that of the Main Monitor configuration. This is not done automatically. Contact TSI for support in establishing a simple script to facilitate this activity.
- It is also strongly recommended that the Buddy password file is synchronized regularly (daily). This is not done automatically. Contact TSI for support in establishing a simple script to facilitate this activity.

Databases

It is recommended when implementing a Buddy Monitor that the Monitor and the Buddy Monitor should be pointed at the same SQL Database server. TSI does not recommend utilizing two SQL Databases on different computers as this will add unnecessary complexity and additional maintenance overhead to the monitoring system.

Complex Distributed System

Commonly used by large pharmaceutical facilities where there are a number of manufacturing processes, typically these processes are on the same site but in different buildings. The end user's LAN is relied upon to facilitate system access and control.



Complex distributed system schematic

This is called a complex distributed system as all the components of the system software are distributed across the end users LAN and the monitoring LAN, they are also installed on different computers.

This is the SAME monitoring system as the Simple System with the same physical parameters being monitored. In this example we are introducing an important concept of multiple monitoring systems. In this example, we see Monitor #1 and Monitor #2. This enables the end user to segregate their sensors; Monitor #1 collects data from the sensors on Process A, and Monitor #2 collects the data from sensors on a Process B, these processes are often in separate buildings. When the end user expands their manufacturing to Process C for example, it allows them to expand the monitoring system, without impacting existing data collection from Processes A and B. Importantly they will not have to revalidate the entire system. Remember, the end user will not be able to include data from Process A and Process B into one report using the FMS report generator, the data collected is segregated into separate databases within the SQL database server.

In this example the monitoring system is accessible to the end user from home via the internet utilizing VPN connection provided by the end user. The monitoring system is available internally within the end users facility via Clients installed on the end users LAN and the Monitoring LAN. Tablet computers are also being used via wireless connectivity in this facility to allow end users to interact with a Client via remote desktop software, a Client is installed on a dedicated remote desktop machine to facilitate this functionality.

VPN connectivity is used to facilitate remote access to the monitoring LAN from a Client installed on a computer at home, for full system access and control. Typically, when you VPN into a network, it will assign different IP address on each connection. Modifying which IP addresses that are allowed to connect to a database should be taken into consideration, or some thought should be given to allow all IP addresses on a specific subnet to have access to the Database.

The FMS WebServer enables the viewing of data only via a web browser remotely; no control or interaction with the system is possible.

Alarms are communicated to end users off site via SMS modems and Autodialer land line hardware. Please contact TSI for the model of SMS modem currently supported by FMS software.

TSI recommends allowing remote access to the monitoring system to facilitate remote support. Typically remote access is enabled and disabled by the end user as needed.

Computers

For minimum computer specifications, please see TSI Technical Note TCC-169, *Minimum Computer Requirements for FMS Software*.

Common programs such as the SQL Database, Monitor and Buddy Monitor must be available to the Monitoring LAN and the End User LAN. Since the computer with these programs installed on it requires a connection to two networks simultaneously, the computer needs to have either two network interface cards or a dual network interface card.

The requirements for sourcing stable computers as detailed for the simple system and the simple distributed system still applies. Additional consideration should be given to installing the Monitor and SQL database on computers with better quality components.

Networks

The same requirements as detailed in the previous sections apply with some additions detailed below:

- If Windows domain user names and passwords are to be used, user logon policies should be well understood as this can lead to unreliable access to FMS. One reason is that FMS does not allow passwords any shorter than six characters and cannot work with nonstandard characters such as “-“, “”“, “%” and “.” i.e., characters that are not integers or in the alphabet.
- It is recommended that all components of an FMS installation use static IP addresses. FMS should also reside on an isolated network, separate from the end users DHCP and DNS servers. This will reduce unnecessary network traffic.
- Refer to the location of an SQL database by IP address and not by host name.
- Refer to the location of a computer used by an FMS component by IP address and not by host name.
- FMS requires having a stable connection with each of its components, failure to do so can cause interruption in sampling. High networking traffic, unstable Ethernet switches, and/or faulty wiring can cause packets to be delayed or even lost over the network, which ultimately results in loss of data.

Configuring a System

The same requirements as detailed in the previous sections apply with some additions detailed below:

- Ensure that any SMS modems used for alarm outputs have enough credit on the SIM card in order to function.
- The AutoDialer functionality is initiated by an FMS alarm relay output. The dial out configuration is contained within the AutoDialer itself.

Summary

Readers are strongly encouraged to note any TSI recommendations made in this technical note.

The topologies described are designed to aid understanding and enable development of monitoring system designs known to be reliable and robust. No two systems are the same and the system may culminate in a combination of the examples detailed.

The TSI team is available to support and answer any questions you may have during your system design process, particularly related to the capabilities of FMS Software. However, end users and system integrators understand the risks associated with your specific project. Please contact TSI for support.



UNDERSTANDING, ACCELERATED

TSI Incorporated – Visit our website www.tsi.com for more information.

USA	Tel: +1 800 680-1220	India	Tel: +91 80 67877200
UK	Tel: +44 149 4 459200	China	Tel: +86 10 8219 7688
France	Tel: +33 1 41 19 21 99	Singapore	Tel: +65 6595 6388
Germany	Tel: +49 241 523030		