

## Facility Monitoring System Design Recommendations

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. It is assumed the reader already understands what a monitoring system is, its components, and how it is applied.

When designing or specifying a monitoring system there are many factors that must be taken into consideration. The right questions to ask are nearly always at the beginning of a project, asking them once irreversible decisions have been taken will be too late. Some of the many questions that need to be considered when proposing and designing a system are detailed below.

---

### Monitoring System Questions

#### General Monitoring System Networking

- Where will the end user want to see the FMS data?
- Will the monitoring system be a closed system, i.e., not operating on the end user's local area network (LAN)?
- Will the FMS data need to be viewed and archived across the end user's LAN?
- Can the monitoring system be a closed system *and* operate across the end user's LAN at the same time?
- Do you need cooperation from the end user's IT department?
- Can you install sensors on the end user's LAN, if so what are the risks?
- Can you install FMS Clients on the end user's LAN?



## Databases

- What are the end user needs or policies regarding data storage and back-up or archiving?
- Can you use a SQL database?
- If you use a SQL database are there any system design constraints?
- Where is the best location to put the standard SQL database?
- How do you configure a Mirror SQL database and where is the best place to put it?
- How do I implement a SQL database with multiple Monitors and Buddy Monitors?

## Buddy Monitor

- What is the end users appetite for risk, is real time hot standby monitoring system needed?
- What is the best way to implement a Buddy Monitor on a Monitoring System?
- Can you implement Buddies with multiple Monitors and multiple Clients?

## Alarms

- How will the end user immediately inform their operators when an action or alert limit is breached?
- Do alarms need to be remotely accessible, SMS text, or phone dial out?
- Is it important to see the monitoring system data in the critical areas via local alarm panel displays?

## Remote Access

- Does the end user need to access the data from home or off site?
- What is the best way to view the Monitor remotely (off-site)?
- Will an FMS Client run on a Virtual Private Network VPN?
- Can I view data from a Monitor or Client on an iPad® or iPhone®?

## Operating System Platforms

- Can I run the Monitor on a virtual server?
- What operating systems are supported?

## Sensor Integration

- How many TSI Remotes can I connect to the system network?
- How do I integrate TSI remotes into the system network?
- How do I integrate environmental sensors into the system network?
- What is the best way to connect alarm beacons into the system network?
- What is the maximum number of sample points or sensors supported by the Monitor and Client?
- What is the minimum sample interval? Short sample intervals lead to greater storage requirements.

As a prerequisite to reading this document, TSI recommends that you have a solid understanding of TCP/IP networks and data bases. This understanding will *significantly* assist you to design, install, troubleshoot, and support a Facility Monitoring System. It is not the objective of this document to train you these disciplines.

This application note will address system network and sensor connection design considerations. It will not cover sensor positioning, sensor selection, sensor enclosure design, or remote vacuum system design.

The next section covers Facility Monitoring System (FMS) software architecture. You will need a fundamental appreciation of this before you can start to ask the right monitoring system design questions.

#### NOTE

TSI strongly recommends installing a monitoring system with FMS on a single standalone computer as this is the simplest configuration. Most technicians possess adequate knowledge to be able to perform this work with minimal training or difficulty. This is straightforward.

Installing a distributed monitoring system across a customer's network with FMS Clients, mirror databases and FMS Buddies is a completely different proposition. This can be complex. It should not be attempted without seriously reviewing your technical capabilities and without thorough training. Familiarity with the use of network analysis tools is strongly recommended. TSI wants to ensure you clearly understand the complexities of distributed networked systems, and that your technicians receive appropriate training. This will enable you to deliver robust and reliable monitoring systems to your customers.

*(continued on next page)*

## Facility Monitoring System 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 may cause confusion. For consistency this application note will use the simplified terms as detailed in the table below:

Program Name	Alternative Names	Simplified Term	Definition
<b>The Monitoring Engine Server</b>	Node, monitoring node, Instance of monitoring, monitoring engine, monitoring task, monitoring server, FMS server, FMS monitoring Server	<b>Monitor</b>	Controls equipment, collects data from the equipment, stores the results in a database, and detects alarm conditions. It performs various actions in response to a range of events.
<b>The User Interface</b>	Client, FMS Client	<b>Client</b>	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.
<b>A SQL Database Server</b>	Database	<b>SQL Database</b>	The SQL server is the application that stores the collected data. There are several types of SQL server. FMS has been tested using MySQL <sup>®</sup> and Microsoft <sup>®</sup> SQL software. 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, only the Client has a user interface. The other applications are run in the background without needing to display any data. 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.

---

MySQL is a registered trademark of MySQL AB in the United States, the European Union and other countries.

A single SQL Database server can be shared with many Monitors; each Monitor will have its own discrete database within a single SQL Database server.

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

Many possibilities and many permutations can be implemented. This can become very confusing, so it is important to understand the end user's needs and work with TSI to optimize the application of the FMS software.

To help you, this application note will work through three levels of monitoring system complexity.

- Simple System
- Simple Distributed
- Complex Distributed

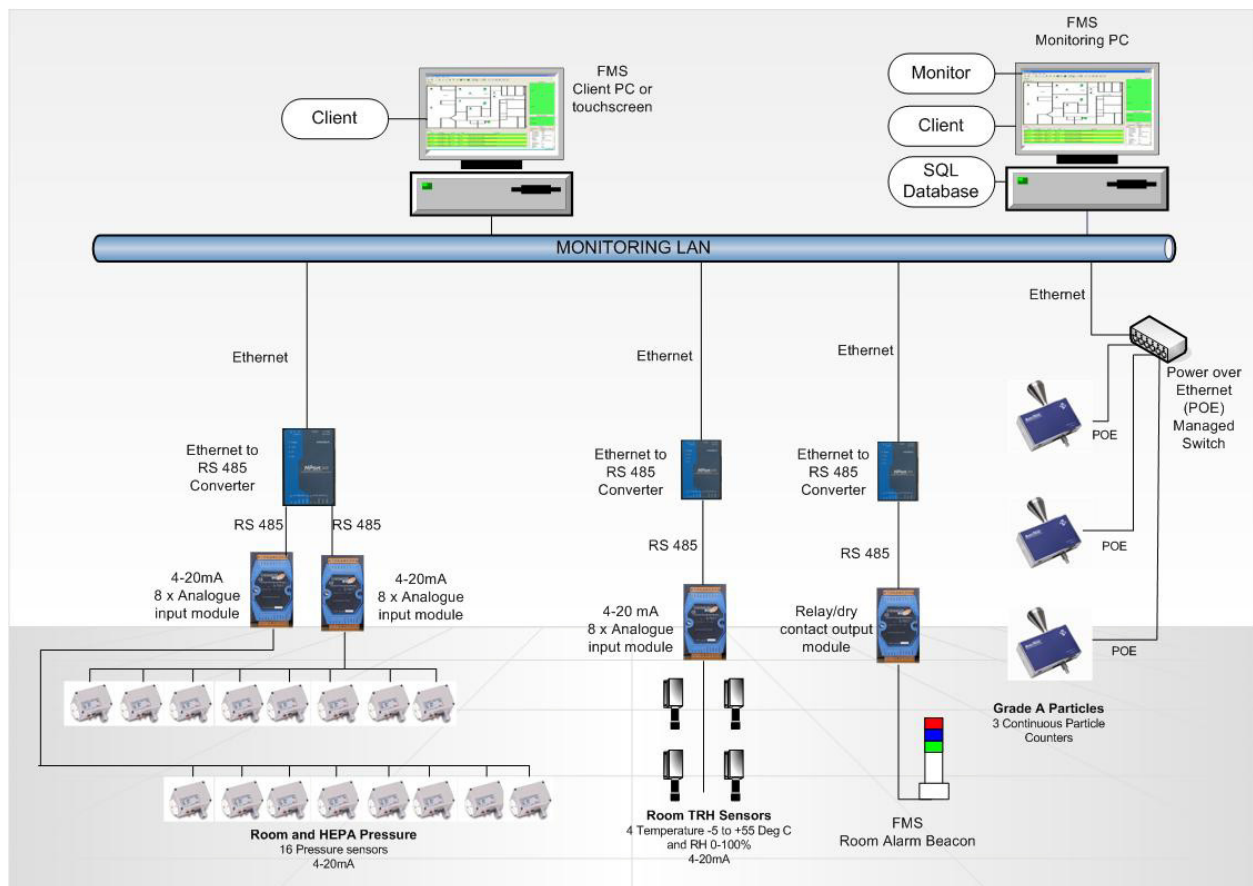
We will suggest typical system layouts or designs, sometimes called topologies, to guide you towards a system design that is well understood and is known to function reliably. The design principles applied to the simple system are a good foundation on which to build more complex systems, hence there is a lot of detailed information in the Simple System description.

**Note:** The complex system covers alarm SMS outputs and Autodialer functionality to inform the end user of an Action limit breach, off site. This functionality can be easily implemented into the Simple and Simple Distributed system examples; it is not exclusive to complex systems.

*(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.



*Simple system schematic*

The single computer with the FMS Monitor, Client and SQL database installed on it is the simplest monitoring system to implement.

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, the Monitor, and the 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 MYSQL database recommended for use with FMS.
- Additional Clients may be installed on dedicated computers or a touch panel/screen computers on this closed network.

## Sensors

An important principle is introduced here; keep 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 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 and lead in certain circumstances:
  - Putting critical data collection at risk.
  - The network performance deteriorating.
  - The network performing unpredictably.

If the monitoring sensing hardware is installed on a separate LAN then you retain control over any network traffic and changes made to that network.

## Computers

Below are some recommended requirements for the FMS monitoring computer. Poor selection of this computer can lead to poor system performance and reliability issues. Purchasing a low cost computer can save money upfront but could cost you very dearly later.

Minimum Computer specification for a Single Monitoring computer:

- 2 GB Memory
- CPU better than Pentium® processor
- Hard drive requirements recommended 80 GB
- Reputable computer brand—this can vary across global geographies
- Operating System: Windows® XP SP 3, Server 2003 (32-bit), Windows 7 (32-bit)—Ultimate and Enterprise
- Min Screen Resolution should be at least 1152 by 864 to view all Client dialogs

---

Pentium is a trademark of Intel Corporation in the U.S. and/or other countries.

Windows is a registered trademark of Microsoft Corporation in the U.S. and/or other countries.

## Networks

The network cabling and computer network configuration 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.
- Use managed switches as these provide intelligent routing capabilities and manage power distribution to the POE powered TSI Remotes—CISCO® is recommended.
- 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.
- Ensure that high quality network cabling (Cat5e or better) and appropriate RJ45 connectors are specified. Ensure that cable preparation, routing and termination follow best practices.
- It is strongly recommended that all network cabling is tested using a "Qualification" cable tester available from Fluke and other manufacturers, the cabling should be qualified to "Fast Ethernet (100BASE-TX)" requirements.

## Configuring a Monitoring System

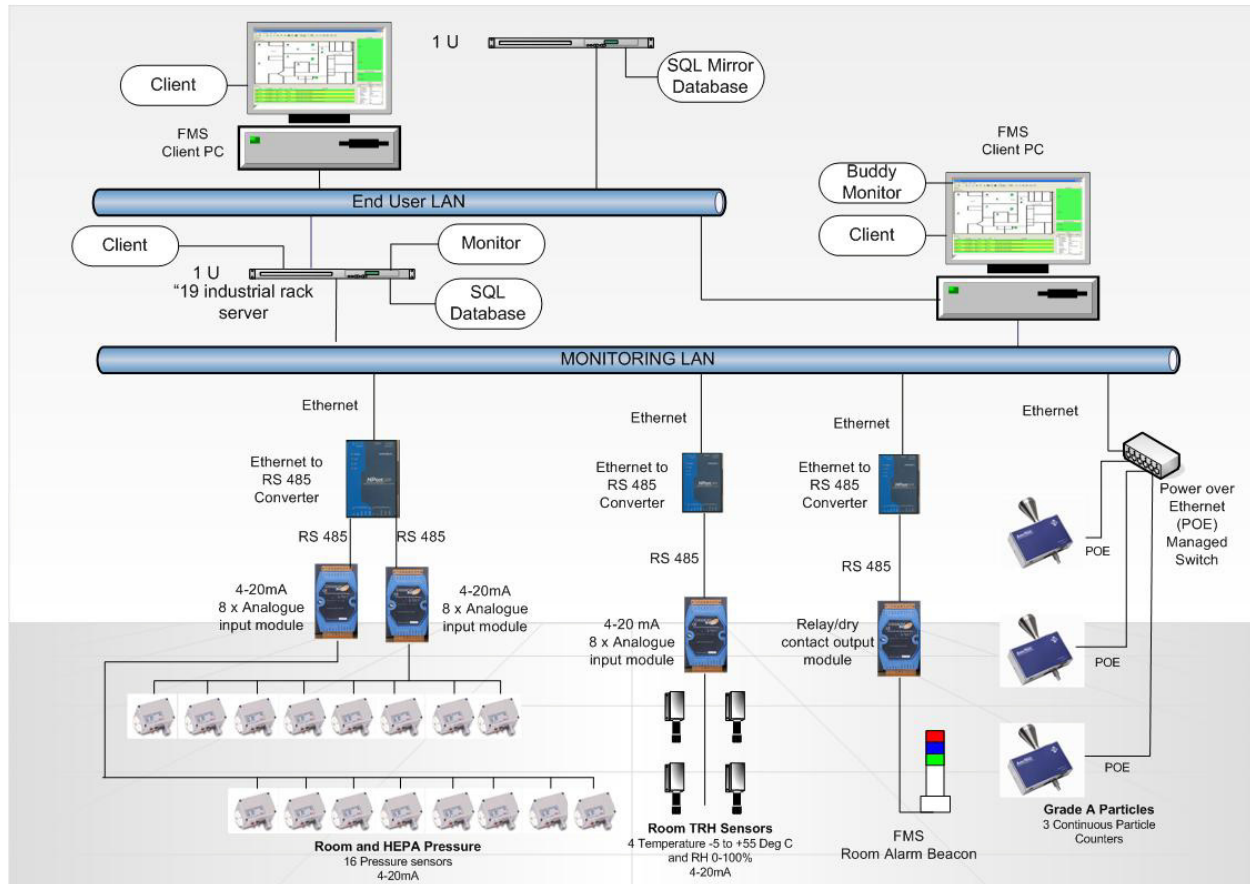
- Maximum sample points per node is dependent on a number of factors (sample interval etc), a maximum of 100 is advised but is not mandated. One factor influencing the number of sample points is the display size and resolution. For large numbers of sample points it good practice to consider dividing 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 generate reports across separate monitoring systems.
- 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 m<sup>3</sup> data simultaneously. In order to accomplish this FMS collects ~36 x 1 minute samples (= 1m<sup>3</sup>), then posts a counts per m<sup>3</sup> 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 m<sup>3</sup> result is then updated. This is commonly known as the "Rolling m<sup>3</sup> buffer", this functionality exists within FMS. Importantly, in order to collect counts per cuft and rolling m<sup>3</sup> data simultaneously you will need to ensure you have allowed 2 sample points per TSI remote particle counter.

## Simple Distributed System

Commonly used in medium sized pharmaceutical or life science facilities where system up time is a priority and data loss cannot be tolerated. 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 three monitors
- SQL Mirror database—Real time data archiving

The requirements as detailed for the simple system are followed; however, there are some additional considerations:

- It is recommended when implementing a Buddy Monitor to only have a single SQL Database server. The Monitor and the Buddy Monitor should be pointed at the same SQL Database server. Utilizing two SQL Databases on different computers adds unnecessary complexity and additional maintenance overheads to the monitoring system.
- Common programs such as the SQL Database, Monitor and Buddy Monitor must be available to the Monitoring LAN and the End User LAN. For this reason these programs must be installed on computers with Dual Network Interface Cards.

- 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, isolated from the DNS. All Ethernet to RS 485 converters and particle counters will have static IP addresses.
- The mirror SQL database is installed on an end user computer, typically their main data server. This mirror database will then be backed up as part of the end users data archiving/ management policies.
- Windows operating system updates must be turned off and implemented in a controlled way.
- Ensure any virus checking software if installed, has the appropriate exceptions configured.
- 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

It strongly recommended that an industrial server grade computer is used for the Monitor. Again, it cannot be over emphasized that poor selection of system computers can lead to poor system performance and reliability issues. Purchasing a low cost computer can save money up front but are likely to cause reliability and performance issues later.

Minimum Computer specification for a Server grade monitoring computer:

- 4 GB Memory
- CPU better than Pentium processor
- Hard drive requirements recommended 80 GB
- Reputable computer brand—this can vary across global geographies
- Operating System: Windows Server 2003 (32-bit), Windows 7 (32-bit)—Ultimate and Enterprise
- It is helpful if Keyboard Video, Mouse (KVM) connectivity is local to server computer
- It is helpful to install a Client on the server computer

## Networks

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

- Network routing policies; the configuration of communication routing between the monitoring system computers should be optimized.
- The MYSQL databases should be installed on a server grade computer, poor MYSQL Data base computer performance will cause the system reporting functionality to be impeded.
- Ensure any Static IP addresses used fall outside the DHCP and DNS address range.
- If using MS SQL database, configuration must allow for FMS functionality, e.g., multiple simultaneous connections. MySQL 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.

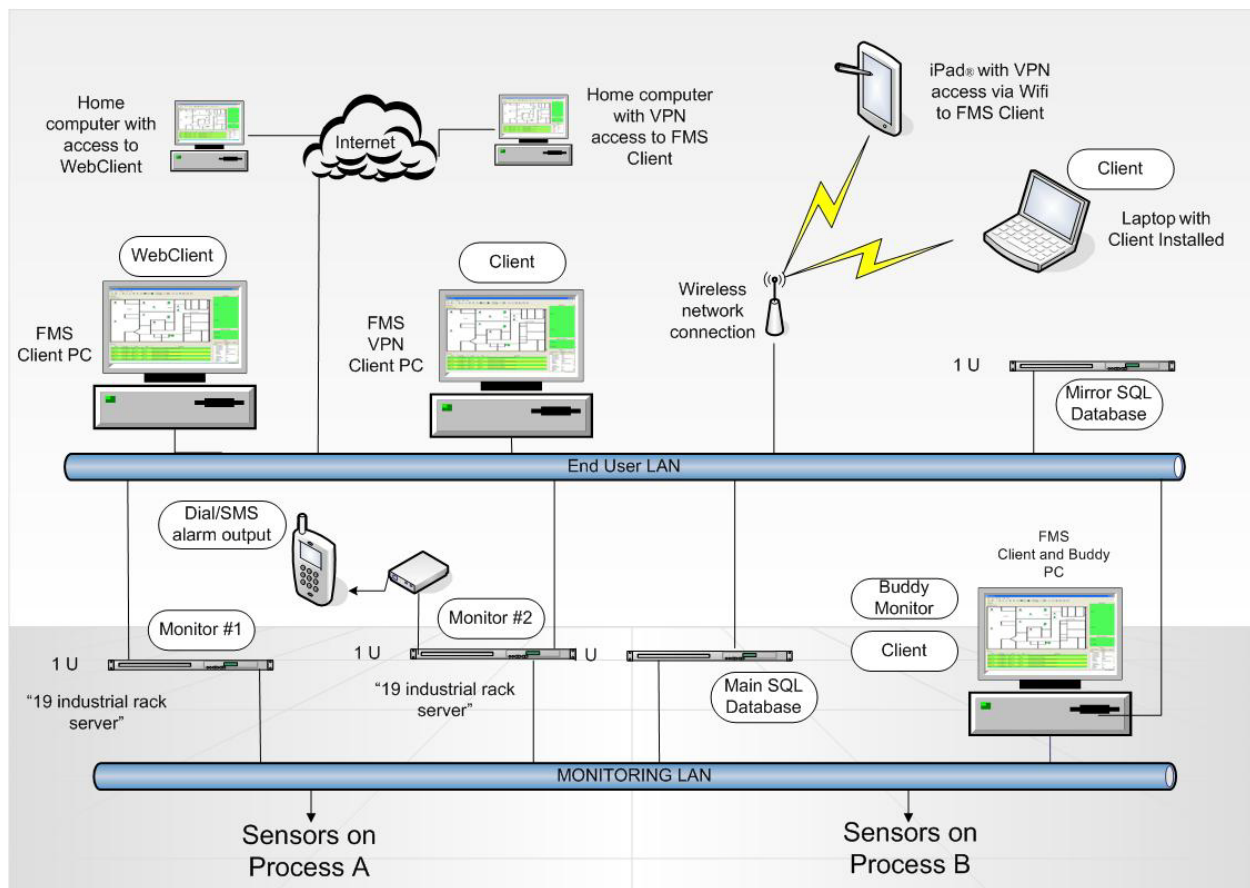
## Configuring a System

- 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 to support you 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 to support you in establishing a simple script to facilitate this activity.

---

## 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 this 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 generate a single report that includes data from Process A and Process B 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 (hardwired) installed on end user computers. Tablet computers are also being used via wireless connectivity in this facility in conjunction with a VPN connection for end users to view a Client on the move, a Client is installed on a VPN server to facilitate this functionality.

VPN connectivity is used to facilitate remote access to a Client (from home) for full system access and control. The FMS WebClient 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. Contact TSI to determine which brands of SMS modem are 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

The requirements as detailed for the simple system and the simple distributed system are the same and should be followed.

Minimum Computer specification for a Server grade monitoring computer

- 4 GB Memory
- CPU better than Pentium processor
- Hard drive requirements: recommended 80 GB
- Reputable computer brand—this can vary across global geographies
- Operating System: Windows Server 2003 (32-bit), Windows 7 (32-bit) Ultimate and Enterprise
- It is helpful if Keyboard Video, Mouse (KVM) connectivity is local to server computer

## 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, then user logon policies should be well understood as this can lead to unreliable access to FMS. FMS does not allow passwords any shorter than six characters; ensure you understand the end users site wide user name and password policies.
- It is good practice to refer to location of a SQL database by IP address and not by host name.
- It is good practice to refer to the location of a computer used by an FMS component by IP address and not by host name.
- Ensure all computers on which all monitoring system software components are installed are using the same time server.
- Poor quality or low cost Ethernet switches will cause data bottlenecks in the system.

## 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.
- Avoid complex FMS login usernames, avoid using non text characters.
- The Autodialer functionality is initiated by an FMS alarm relay output. The dial out configuration is contained within the Autodialer itself.

---

## Summary

These examples are intended to help you understand robust monitoring system design. No two systems are the same and so your system may end up being a combination of the examples detailed in this document. Whatever the final design, you now have enough information to ensure you establish a robust and reliable monitoring system that meets the end users needs.

The TSI team is available to support and answer any questions you may have during your system design process, please do not hesitate to contact us, no question is too small.

---

**TSI Incorporated** – 500 Cardigan Road, Shoreview, MN 55126 U.S.A

<b>USA</b>	Tel: +1 800 874 2811	E-mail: <a href="mailto:answers@tsi.com">answers@tsi.com</a>	Website: <a href="http://www.tsi.com">www.tsi.com</a>
<b>UK</b>	Tel: +44 149 4 459200	E-mail: <a href="mailto:tsiuk@tsi.com">tsiuk@tsi.com</a>	Website: <a href="http://www.tsiinc.co.uk">www.tsiinc.co.uk</a>
<b>France</b>	Tel: +33 491 11 87 64	E-mail: <a href="mailto:tsifrance@tsi.com">tsifrance@tsi.com</a>	Website: <a href="http://www.tsiinc.fr">www.tsiinc.fr</a>
<b>Germany</b>	Tel: +49 241 523030	E-mail: <a href="mailto:tsigmbh@tsi.com">tsigmbh@tsi.com</a>	Website: <a href="http://www.tsiinc.de">www.tsiinc.de</a>
<b>India</b>	Tel: +91 80 41132470	E-mail: <a href="mailto:tsi-india@tsi.com">tsi-india@tsi.com</a>	
<b>China</b>	Tel: +86 10 8251 6588	E-mail: <a href="mailto:tsibeijing@tsi.com">tsibeijing@tsi.com</a>	
<b>Singapore</b>	Tel: +65 6595 6388	E-mail: <a href="mailto:tsi-singapore@tsi.com">tsi-singapore@tsi.com</a>	



TRUST. SCIENCE. INNOVATION.

Contact your local TSI Distributor or visit our website [www.tsi.com](http://www.tsi.com) for more detailed specifications.