HMI & Virtualization in Process Automation

An Introduction to Virtualization

TDOCT-B1N4_ENG

Your automation, our passion.

PEPPERL+FUCHS

Contents

Introduction

Virtualization is a technology that stems from the information technology (IT) industry and has become more and more popular in process automation. It promises to ease software management while reducing costs. This trend also has an impact on human-machine interaction in such systems. Especially in combination with thin client technology, virtualization provides an easier and more cost-efficient way to control process automation systems, even in the harshest industrial environments.

In this collection of technical white papers, we give an overview of virtualization in process automation and describe how Pepperl+Fuchs' thin client technology fits into virtualized systems.

In the first white paper, we take a closer look at virtualization technology. We focus on the back end and show how virtualization works and what benefits it offers in process automation.

The second white paper describes how thin clients work, what their general advantages are, and which role they play in virtualized process automation systems.

In the third white paper, we present VisuNet Remote Monitors, which are industrial thin client solutions that save time and money during installation and operation and offer broader functionality than other technologies.

In the final white paper, we present the benefits of using a centralized management tool for setting up and configuring thin clients.

Dr. Marc Seißler,
Product Portfolio Manager

1 What is Virtualization?

In traditional process automation systems, multiple powerful PCs, called workstations, are used to host process applications like process control, alarm and asset management, historian data, etc. One disadvantage of a workstation-based infrastructures is that applications and operation systems (OS) are tied to the workstation hardware.

The idea of virtualization is to break up the strong coupling between application software, OS, and hardware. Virtualization allows you to run multiple OSs and applications concurrently, but segregated from each other, on one physical host hardware.

Depending on the number of system components that are virtualized, different terminologies are used:

- **Server Virtualization**: Multiple servers and their OSs (e.g., Windows® 2012 R2) are consolidated on one or a few host servers. This is, for example, a common way to run a separate backup server or a test server on which new configurations can be evaluated.
- **Desktop Virtualization / Virtual Desktop Infrastructure (VDI)**: VDI is one of the newer virtualization trends where many complete desktop OSs (e.g., Windows® 7) with their applications are hosted on one host server. This can be used to consolidate multiple workstations with different applications on one centralized host server. (See Figure 1.1)
- **Application Virtualization**: A set of applications is encapsulated in sandboxes and hosted on a server. Operators can access these applications from their local machines while the applications run on the server. This setup is quite common in setups where users need access to a pool of centrally managed applications.

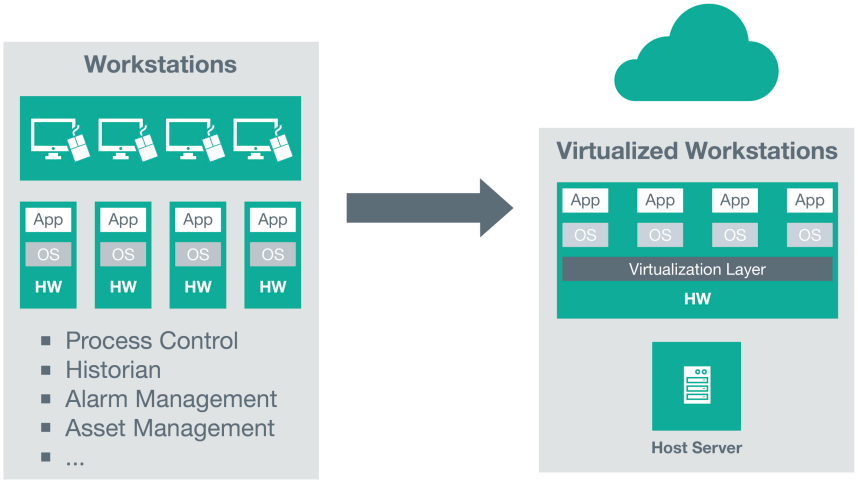

Figure 1.1: Virtualizing multiple workstations on one host server

In process automation, all three virtualization types can be seen; however, server virtualization and VDI seem to be the most prominent setups today. For manufacturing execution systems (MES), application virtualization is the most popular choice of virtualization technology.

Especially in server virtualization and VDI, an additional software layer on the host server enables the virtualization and separation of the hardware and the guest operating system and applications. This software, called a hypervisor, intercepts all operations of the guest OSs and the host server hardware. Each guest OS runs in its own virtual machine (VM) that is a pure software container. It provides a virtual hardware interface and gives the guest OS and applications the impression that they run natively on their own hardware. Each VM has an interface to the hypervisor that controls the physical hardware and assigns the resources concurrently to the VMs. (See Figure 1.2.)

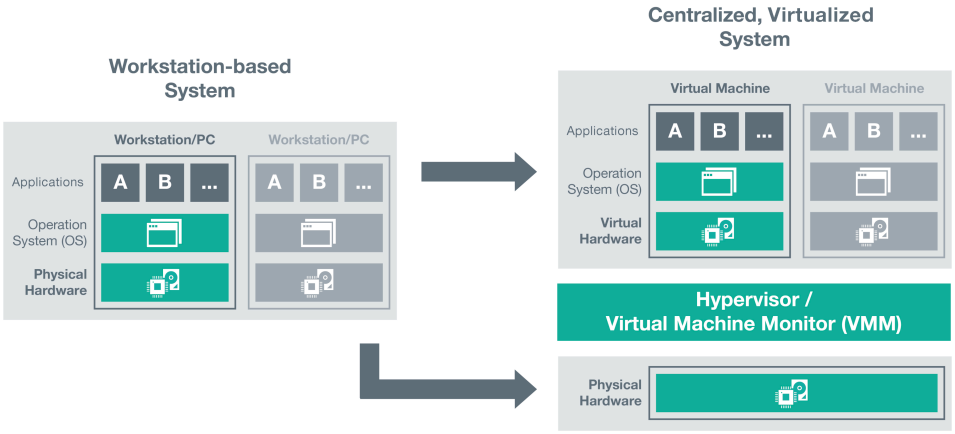

Figure 1.2: Virtualization hardware architecture

In other words, a hypervisor provides an abstraction layer that insulates the VMs from the host hardware and from each other.

In fact, a key feature of virtualization is that VMs are completely isolated from each other for operational purposes, although they can communicate with each other over normal Ethernet and data storage channels. This isolation is one major difference from standard server OSs, where multiple applications share the same OS. Running multiple applications on one OS increases the risk of conflicts between different applications since they rely on the same OS resources.

The most popular hypervisors that implement this principle, are VMWare® ESXi, Citrix® XenServer, and Microsoft® Hyper-V 2008/2012. But hypervisors are usually only one small component in a virtualized system, since virtualized environments demand additional management tools. The most popular virtualization software solutions today are VMWare® Horizon, Citrix® XenDesktop, and Microsoft® Remote Desktop Services (RDS) that also contain management suites.

Benefits

Virtualization offers several benefits. Centralized management and cost reduction due to fewer devices are the main drivers of this technology trend. But there are also other aspects that are appealing for the process automation industry.

Centralized management

One of the main benefits of virtualization is centralized management of the servers and their OS and application software. Since all applications run on only a few host servers, managing these systems becomes much easier. On the hardware side, only a very limited set of hardware components needs to be maintained. On the software side, the main benefit is that powerful tools are available that enable the management of multiple virtual machines. Some features include duplication of VMs based on master images that allow the easy deployment of software updates among multiple VMs at once.

Reduced hardware costs

Most importantly, the conversion of many physical computers (workstations and servers) into virtual machines that run on a few physical host servers allows optimizing the use of available hardware resources. The host hardware can used be more efficiently, and the hardware can be dynamically assigned to the VMs, depending on their performance demands.

Higher application flexibility

The centralized management of virtualized automation systems simplifies the roll-out of new applications and among existing systems. New software revisions need to be installed on only one master VM and then can be duplicated. Virtualization brings another benefit, since new applications can be tested offline in a separate test VM that runs isolated from the VMs that are used online in production. When all applications are tested, the test VM can be easily deployed with one click, making the applications available to the users.

Increased uptime

Process automation systems must run reliably not just for cost reasons but also to protect against equipment damage or even personnel injury. As in traditional server infrastructures, virtualized systems make it easy to set up redundant servers to increase the system robustness. For example, multiple physical host servers can be configured as a pool of resources, with VMs deployed throughout the pool based on the servers' workload and availability. If one of the physical host servers fails, the VMs can be automatically moved to an alternative physical host server.

Further, administrators can balance server loads in this manner, either locally or remotely, and equipment can be freed up for repair. All of this can be accomplished with minimal or zero downtime.

This cannot be achieved with a traditional server infrastructure, where the operating systems are strongly coupled to their physical server hardware.

Increased application longevity

Many industries struggle with the life cycle of their computing hardware and software. Eventually, users are faced with performing costly hardware and OS upgrades and revisions, or running the risk of sticking with unsupported and obsolete components and systems.

However, virtualization system providers constantly update their virtualization software to run on the latest hardware and to support a wide variety of guest OSs. Savings can be substantial as virtualization enables users to reliably keep their legacy software running for many more years, even though it is virtually deployed on newer hardware. Existing hardware with sufficient computing power can also be used for new application deployments.

Conclusion

The core principle of virtualization is to consolidate computing hardware (i.e., PCs or servers) by hosting them on one or a few centralized host servers that use a hypervisor to run these systems independently in virtual machines.

Consolidation of workstations, servers, and applications onto less computing hardware is just the beginning. There is less hardware to purchase, fewer systems to manage, and reduced power consumption due to better utilization of the hardware. More important, in many industrial applications, reliability can be greatly improved compared to a distributed infrastructure with dedicated workstations.

Virtualization provides other gains that simply cannot be realized with traditional, PC-based infrastructures. Configurations can be pretested and debugged in a sandboxed configuration. Application or even OS upgrades and migrations can be carried out in a controlled manner with little or no loss of operation. Software life cycles can be extended by years.

With virtualization on the back end, client devices are needed that enable the users to access the virtual machines on the host server. Keyboard-video-mouse (KVM) extender-based systems are no longer an option since VMs do not provide a physical PC interface that allows connection to a monitor.

For virtual environments, thin clients are the best technology to access VMs. Thin clients are small computing devices that use standard Ethernet technology and communication protocols to access virtual machines.

In the second white paper in this collection, we take a closer look at thin-client technology. We explain how thin clients work and why they are one of the best solutions to provide users access to process control and information in harsh industrial environments.

2 What is a Thin Client?

Over the last decade, thin clients have become more and more popular in process automation systems and industrial applications. Especially with the trend toward virtualized, centralized automation systems, thin clients represent a powerful and cost-efficient technology that enables users to access applications and information that run on centralized hosts.

In conventional, decentralized automation systems, all data and applications usually run on powerful PC-based workstations. In centralized automation systems, data and applications reside on the hosts that are usually servers. A thin client only runs the user interface that is required to access the applications on the host. (See Figure 2.1.)

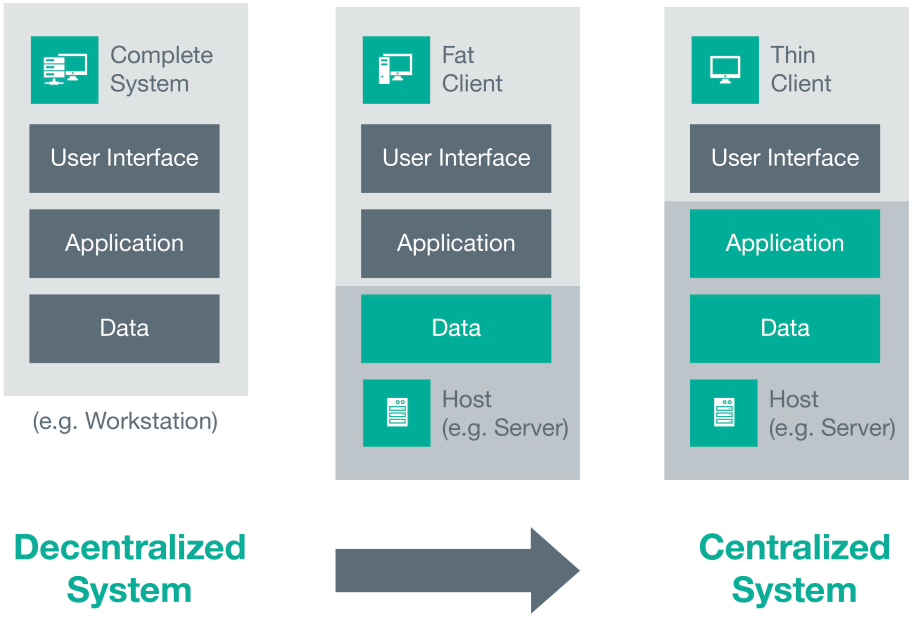

Figure 2.1: Thin clients are the first-choice technology for centralized systems

To do this, a thin client has a minimalistic, usually embedded operating system (OS) and only provides drivers for the input and output devices (e.g., mouse, keyboard, touchscreen, and monitor) that are connected to the thin client. Additionally, installed communication protocols enable the exchange of the system inputs and outputs between the thin client and host. (See Figure 2.2.)

All of these remote protocols rely on the same principle:

The host generates the user interface (e.g., GUI and sounds), which is then compressed and sent via the Ethernet-based remote protocol to the thin client. The thin client receives the compressed data, for instance, in the form of GUI pictures, decompresses them, and displays them on the screen to the user.

User inputs (via keyboard, mouse, touchscreen, etc.) are sent in the opposite direction. The thin client captures the physical user inputs and redirects them via the remote protocol to the host. The host decodes the user inputs and delegates them to the hosted operation system and applications. For the applications that run on the host, this is transparent. This means that, for the applications, it looks like user inputs occur locally on the host. Due to today's high-performance Ethernet infrastructures, the user experience of interacting with a thin client is just like sitting directly at the host system.

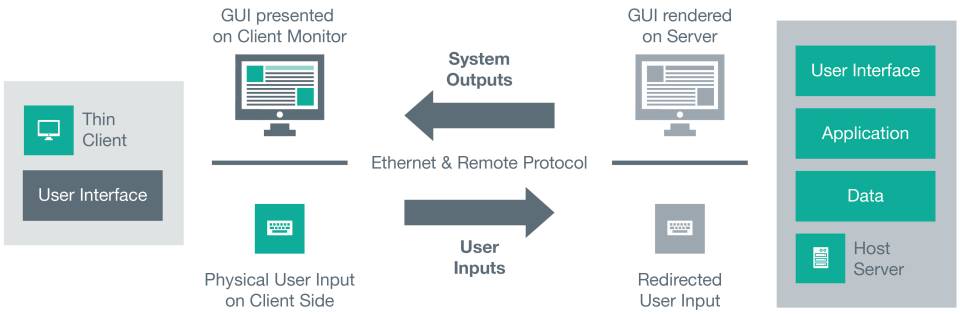

Figure 2.2: A thin client only provides the user interface to the user

Since thin clients work over Ethernet, they are also the first-choice technology for virtualized automation systems. Conventional technologies like keyboard-video-mouse (KVM) extenders are not suited for virtualized systems. This is because one or many virtual machines (VMs) usually run on host server hardware, which has no dedicated physical interfaces to connect the KVMs to. VMs can be accessed only via Ethernet and the remote protocols.

Today, multiple communication protocols exist, but there is only a small set of protocols that are relevant to cover the majority of virtualized – and even conventional, nonvirtualized – applications:

- **Microsoft® Remote Desktop Protocol (RDP)**: RDP is the most popular remote protocol for workstation-based and virtualized automation systems. While today's most recent Microsoft OS can be accessed via an integrated RDP interface (e.g., for remote administration), professional setups with multiple users require a Windows® Server OS. The server-based solution for multi-user access was formerly known as Microsoft® Terminal Services and was introduced with Windows® NT 4.0 Terminal Server Edition many years ago. With Microsoft's strategy toward virtualized infrastructures and the launch of Windows® Server 2008 R2 in 2009, Terminal Services has been extended and renamed Remote Desktop Services (RDS).
- **Virtual Network Computing (VNC®)**: VNC® is one of the older remote protocols and is still quite popular. This protocol is still used, especially in smaller, nonvirtualized automation systems, since several open-source implementations exist that allow the setup of cost-efficient solutions.
- **Citrix® Independent Computing Architecture (ICA)**: ICA is a Citrix-proprietary, platform-independent remote protocol that is used in large, professional, and virtualized infrastructures with Citrix® XenApp and XenDesktop.
- **VMWare PC-over-IP (PCoIP)**: Originally introduced by Terradici®, VMWare® integrated this protocol into their virtualized server infrastructure. Besides PCoIP, VMWare® also supports access to the hosted VMs via RDP.

Benefits

Using thin clients in a centralized automation system offers a large set of benefits. Many of the features, like centralized management, the need for fewer local computing resources, and keeping the data on the host server, contribute to a reduced total cost of ownership compared to PC-based, decentralized infrastructures.

Reduced total cost of ownership

Since the applications reside on the host systems, thin clients have fewer hardware demands compared to workstation PCs. Low-power processors are sufficient to run the different remote protocols and to encode/decode the compressed data exchanged between the thin client and the host. This has an impact on the overall hardware costs, since the thin client components are significantly cheaper than high-performance components of workstation PCs. To have the same performance in a thin client infrastructure, this demands more powerful host servers. Since centralized infrastructures allow a more efficient use of the hardware resources (for instance, due to load management), the total hardware costs sink, especially in mid-sized to large applications. (See the first technical white paper in this collection, *Virtualization*, for more information.)

Hardware & software longevity

Another benefit of thin clients is that they can have a longer life time than PCs. There are two reasons:

First, application software updates do not affect thin clients, since they only communicate with the host via a remote protocol. This allows thin clients to be used, even if the OS or applications on the host are updated.

The second reason is that the embedded OS that runs on thin clients are supported much longer than desktop operating systems (like Windows® XP Professional or Windows® 7 Professional), which usually run on PCs.

Reduced configuration effort

Thin clients are much simpler to configure. Instead of installing applications on several workstation PCs, thin clients only need to be configured. This is mostly limited to two steps: assign the thin client an IP address and specify the host server or VM name the thin client should connect to.

In large installations where multiple thin clients need to be configured, tools for centralized configuration and management help maintain whole groups of thin clients with one mouse click.

Due to the limited amount of settings that need to be made, this can be done even by personnel with limited knowledge of IT.

Increased system availability

Especially in industrial environments, systems must run reliably not only for cost reasons, but to protect process equipment and personnel. With thin clients, process reliability can be increased for several reasons:

As discussed above, thin clients have no locally stored data or applications and can be exchanged in a few minutes in case of a hardware defect. This does not affect the applications, since they are running on the host.

Since thin clients only need very limited computing power, industrial-grade components can be used for a lower price than what a powerful workstation would cost. This has a positive effect on the robustness of the thin client and allows it to be used in harsh, industrial environments where hardware has to withstand heat, shock and vibration, dust, washdowns, and explosive atmospheres, etc.

In case of a host failure, backup hosts can be used. Modern thin clients like Pepperl+Fuchs' remote monitors also allow preconfigured connections to backup hosts to which the thin client can connect automatically as soon as a host failure is detected. With this feature, highly reliable process automation systems can be set up.

Increased flexibility

Thin clients use Ethernet technology to connect to their host systems. Therefore, thin clients can connect to any host system that is located in the LAN, WAN, or even Internet.

This allows the implementation of sophisticated application scenarios, such as connecting to backup hosts in case of a failure in order to connect to and supervise different machines in a plant or to access information from different system types like a decentralized control system (DCS) and a manufacturing execution system (MES) that might run on two different hosts and networks.

Higher security

Centralized IT infrastructures also offer higher security since data and applications reside on the hosts in the data center with centralized backups, redundant servers, etc.

Thin clients in particular are further protected against manipulation with tools like enhanced write filters and USB lockdown that prevent users from installing software locally. This significantly reduces the threat of viruses being installed.

Conclusion

Thin clients are a high-performance and low-cost solution for accessing applications and information in process automation applications. Pepperl+Fuchs' remote monitors are specially tailored thin clients to withstand the harshest conditions in process automation applications.

One of the key benefits of thin clients is that no data and applications are installed locally and need to be maintained. Thin clients use industry-standard Ethernet and remote protocols to access applications and data that are located on a host system, which can be a VM in a virtualized automation system or a conventional workstation-based setup. This allows performance of the computing hardware on the thin client side to be minimized and eases system configuration.

Due to the use of standard technologies like Ethernet, users can take advantage of readily available expertise to implement their automation systems. Software tools for centralized management of thin clients further help ease the integration of thin clients, even for automation engineers without deeper knowledge of IT.

With the trend toward virtualized process automation systems, thin clients are the first-choice technology for accessing VMs. While virtualization has only a very limited effect on the thin client side, it changes different aspects on the host side.

3 What are VisuNet Remote Monitors?

For many years, Pepperl+Fuchs has offered a broad range of industrial-grade HMI systems that consist of highly robust components that withstand harsh environmental conditions like dust, high temperature ranges, washdowns, and explosive atmospheres. (See Figure 3.1.)

In the VisuNet product line, different technologies – like PC-based, KVM-based, and direct monitors – are available that offer high flexibility and address different application needs.

One of the main technologies in the VisuNet portfolio are VisuNet Remote Monitors (RMs). A core innovation of VisuNet RMs, which were introduced by Pepperl+Fuchs in 2007, is the use of thin client and standard Ethernet technology for accessing process automation systems.

Figure 3.1: VisuNet RMs are thin client solutions for demanding industrial applications

In contrast to conventional thin clients, the integrated thin clients in our RMs is based on industrial-grade hardware that has no moving parts and is rated to withstand wide temperature ranges, shock, and vibrations. They are suited for use in hazardous locations with explosive atmospheres.

Further, to fulfill the special demands of process automation applications (e.g., security and system integration), VisuNet RMs run RM Shell, a thin client software that is engineered by Pepperl+Fuchs.

With the introduction of the VisuNet RM Shell 4.0, we introduced the next generation of software that is perfectly tailored for virtualized process automation systems. (See Figure 3.2.)

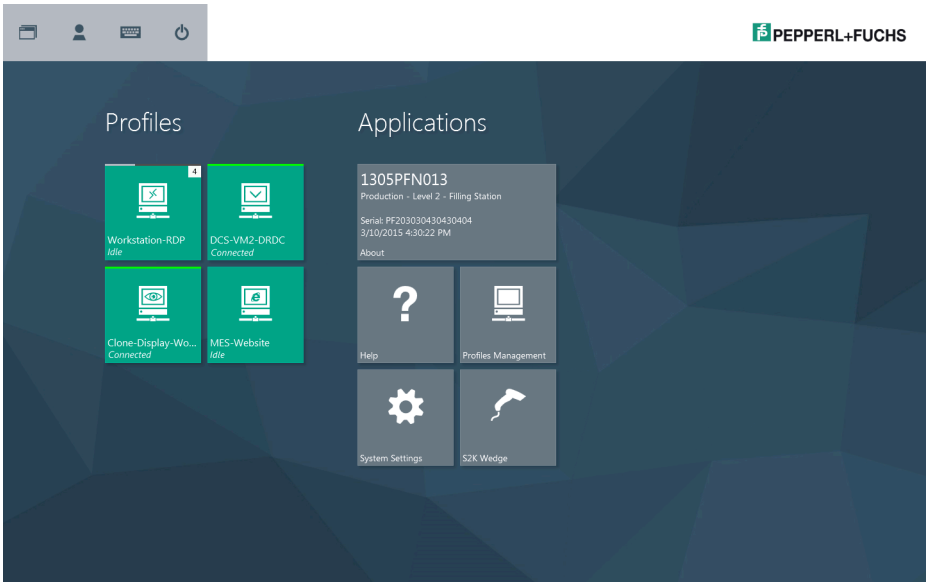

Figure 3.2: VisuNet RM Shell reduces complexity for operators and system engineers

VisuNet RM Shell reduces the complexity of the user interface to a minimum and is tailored to support the users' tasks. The system is optimized to set up remote protocols that enable the connection to the host systems in the safe area via Ethernet. One key benefit of RM Shell is that it hides the system complexity from the user and offers several features that optimize the remote connection with automatic logins, connection loss detection, backup connections, etc.

Benefits

VisuNet RMs offer many benefits compared to other HMI solutions and can help you reduce the total cost of ownership of your automation system.

Reduced integration and maintenance effort

One key benefit of VisuNet RMs is that they help reduce installation and maintenance time to a minimum. Besides the mechanical and electrical device installation, the integration of an HMI system into the process automation system poses another challenge for process engineers.

With the trend toward virtualized automation systems, which use different remote protocol types and configurations, integrating the HMI system into the process automation system demands even more IT expertise.

VisuNet RMs are optimized to support process engineers during the integration of the VisuNet RM into their virtualized process automation system. VisuNet RMs not only support the latest remote protocols that are used for connecting to virtualized systems, they also provide simplified access to the relevant system settings and information that are required for the integration of a VisuNet RM in any process automation infrastructure with the optimized RM Shell user interface.

One of the core features is a harmonized remote protocol editor that guides users through the configuration steps. (See Figure 3.3.) This simplifies setup for automation engineers with limited IT expertise.

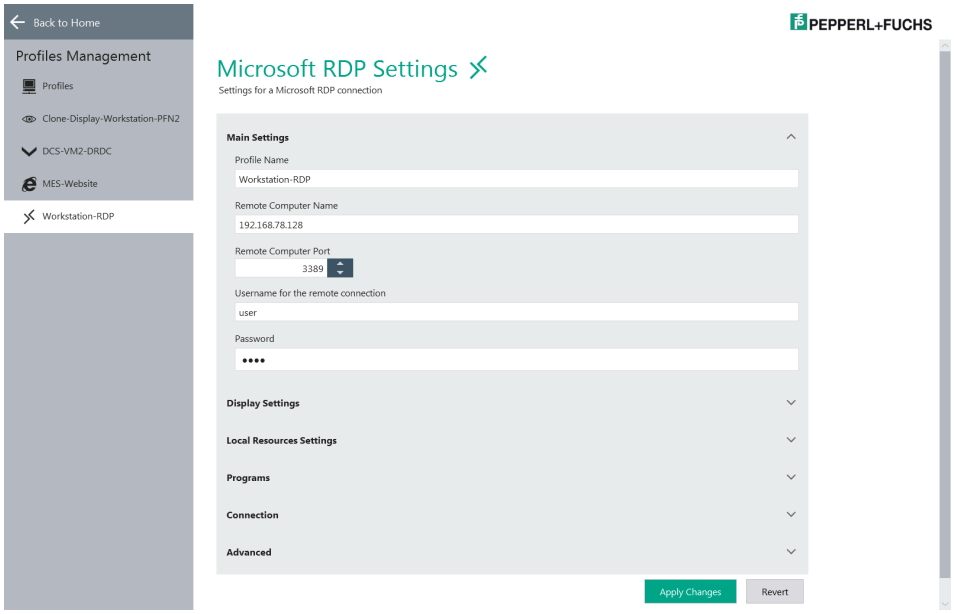

Figure 3.3: Harmonized remote protocol editor eases system integration

The support of centralized firmware updates for the VisuNet RMs further reduces maintenance effort for the process engineers.

Extended security

Besides easy HMI setup, system security plays a vital role in process automation systems. VisuNet RMs address this need with different features that make RMs one of the most secure HMI solutions in the market.

All VisuNet RMs run VisuNet RM Shell, which is based on a tailored Windows-embedded operating system (OS). The RM Shell uses different mechanisms of the OS, like the enhanced write filter (EWF) that prevent the local storage of any data or even viruses and other malware. A USB lockdown mechanism, a built-in Ethernet firewall, and password-protected VisuNet RM settings also help make the system resistant against external manipulations.

Advanced features like a built-in factory reset makes it easy to reset the system in case of a misconfiguration.

Superior performance & user experience

While the RM Shell helps process engineers integrate VisuNet RMs into the process automation system, operators also benefit from the tailored UI.

Predefined user roles (administrator, operator, and engineer) help distinguish between different information levels and provide tailored information access.

While administrators have access to all RM system information and are supported in the VisuNet RM integration process, the operator and engineer modes allow different usage scenarios to be set up.

The engineer role enables users to partially setup the RM and to start and close different, predefined remote connections. The operator mode is intended for more restricted system access. In this mode, the system can be configured to automatically connect to different, predefined host systems directly after system start. The users do not need to intervene, which helps set up a highly robust HMI system.

Features like auto-connect, connection loss detection, and backup-connection, which work for different remote protocol types, further contribute to the overall system robustness and enhance the user experience.

High flexibility

Since the RM Shell includes a broad range of integrated remote protocols, such as Microsoft® RDP, VNC®, etc., the VisuNet RMs can be easily integrated into multiple virtualized and nonvirtualized automation systems.

Further, the RM Shell uses an app concept, which allows the integration of additional third-party remote protocols and applications. This concept enables OEMs to adapt VisuNet RMs to their specific process automation infrastructure by integrating their own apps.

Conclusion

Pepperl+Fuchs' VisuNet RMs are industry-grade, thin-client solutions that are tailored for process automation systems. Due to the use of standard Ethernet technology and the latest remote-protocol technology, VisuNet RMs are suited to the latest virtualized process automation systems.

RM Shell, the tailored, simplified user interface developed by Pepperl+Fuchs, supports process engineers during system integration. Extended features like auto-connect mechanisms and backup connections further allow the setup highly robust HMI systems. Security features like enhanced write filters, USB lockdown, firewall, and password protected configuration settings make VisuNet RMs highly reliable systems.

4 What is Centralized Management?

Thin clients are computing devices that provide a user interface to the operator while the application runs on a remote host system. Ethernet technology is used in combination with software protocols to transmit the data between the thin client and the host.

To get a thin client infrastructure running, system-specific settings must be configured at the initial setup of the thin clients. On the system-hardware level, this means that keyboard language, time and local time zone, network settings, etc. need to be specified during installation. The next step is to set up the connection profiles to the host systems.

While local thin client configuration can work well in small installations, it does not scale with the size of the installation. In larger installations where multiple thin clients are used to access a host server, centralized management tools are used to set up and configure the devices via the network from one location.

These software tools are usually installed on a separate computer (or on a virtual machine) that is connected to the thin client network. (See Figure 4.1.) The tools often combine different functions that allow setup, maintenance, and monitoring of the thin clients.

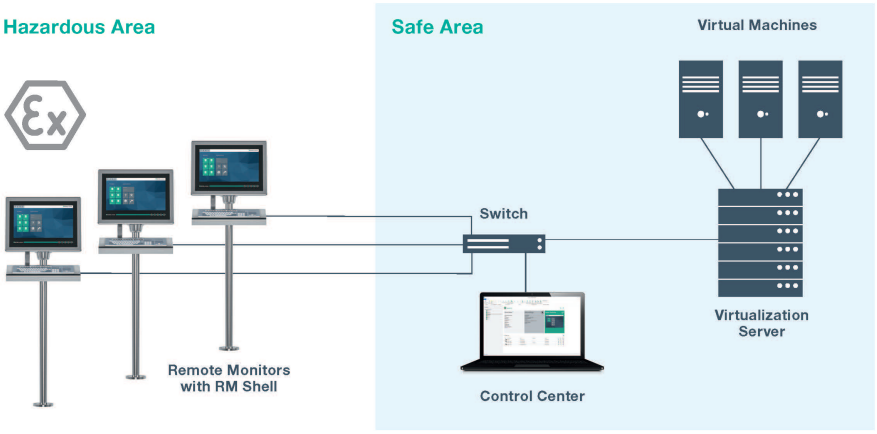

Figure 4.1: Centralized management tools like the VisuNet Control Center simplify thin client configuration.

Benefits

Using thin clients in a centralized automation system offers significant benefits. Many of the features of centralized management—such as saving local computing resources and keeping data on the host server—contribute to a reduced total cost of ownership compared to PC-based, decentralized infrastructures. The following benefits can be directly linked to centralized management of thin clients.

Easier configuration

Local configuration of thin clients takes a significant amount of time, especially in process automation, where HMIs are used throughout plants. In more challenging thin client applications, e.g., on oil rigs or in cleanrooms, entering the area where a thin client is located might entail additional restrictions or not even be possible.

Since centralized management tools allow configuration of thin-client-based HMIs via Ethernet from one location, considerable time savings are guaranteed. Depending on the network infrastructure, these tools even allow management and service of devices that are located all around the world.

Increased flexibility

More advanced tools like VisuNet Control Center offer functions that go beyond basic configuration tasks. This includes sophisticated functions that allow settings and profiles to be copied from one thin client to another. Maintenance tasks like updating the devices' firmware are also supported.

The "tile view" function of VisuNet Control Center provides a quick, live overview of remote monitors in the field. (see Figure 4.2.) Connection breaks and other errors can be seen in the Control Center as soon as they occur. In addition, the built-in "session shadowing" function makes it possible to take over control of an individual RM in order to support an operator remotely or solve an issue.

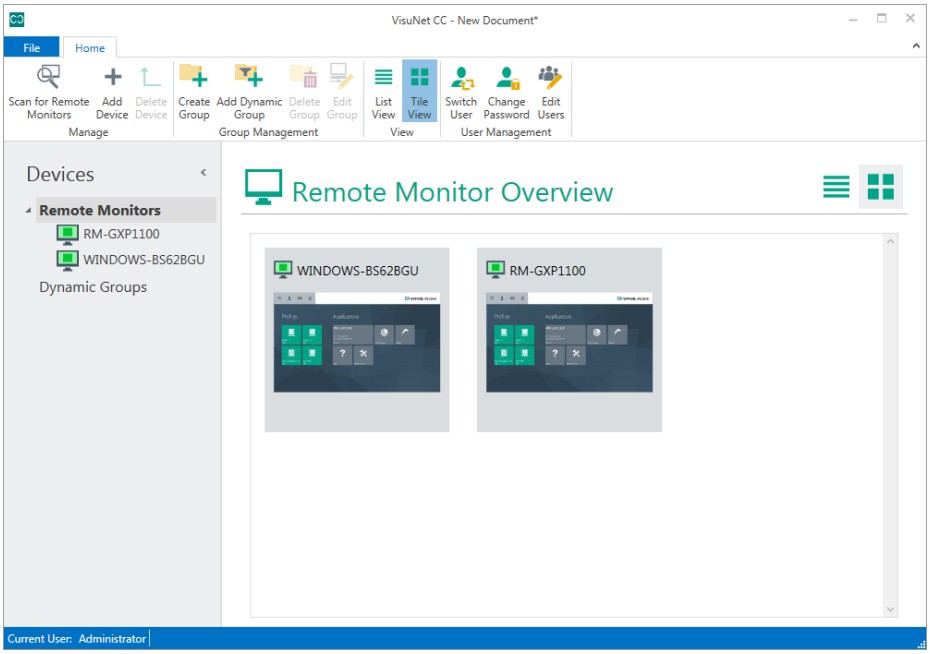

Figure 4.2: "Tile view" provides a quick, live overview of VisuNet Remote Monitor screens.

Enhanced security

Along with application flexibility, security also plays an important role when it comes to centralized management. Since management tools access thin clients via a network, the interfaces need to be locked down to protect them from external access. In VisuNet Control Center, this is achieved via a certificate-based, encrypted communication protocol between the RMs and the management tool.

Beyond security on the communication level, an advanced user management system is integrated that allows flexible assignment of rights to user roles down to even individual users. Production IT can use this feature to manage and configure the thin clients, while process engineers and supervisors can get a quick device-status overview and can directly react to problems that arise during their shifts.

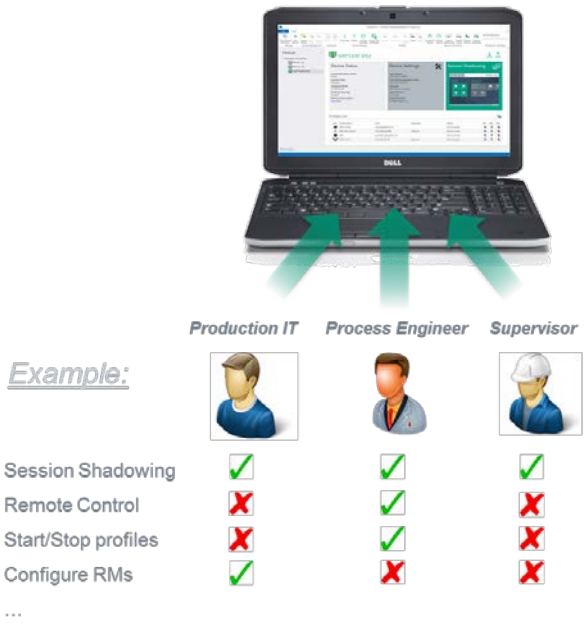

Figure 4.3: Functions can be assigned to password-protected user roles and users

Conclusion

Thin clients are a high-performance, low-cost solution for accessing applications and information in virtualized process automation systems. Pepperl+Fuchs' VisuNet Remote Monitors are thin clients that are designed to withstand the harshest conditions.

One of the key benefits of thin clients is that no data and applications are installed locally and need to be maintained. Thin clients use industry-standard Ethernet and remote protocols to access applications and data that are located on a host system, which can be a VM in a virtualized automation system or a conventional workstation-based setup. This makes system configuration easier and minimizes the burden on computing hardware on the thin client side.

Due to the use of standard technologies like Ethernet, users can take advantage of readily available expertise to implement their automation systems. Software tools for centralized management of thin clients further simplify the integration of thin clients, even for automation engineers without deep IT expertise.

Notes

Your automation, our passion.

Explosion Protection

- Intrinsically Safe Barriers
- Signal Conditioners
- Fieldbus Infrastructure
- Remote I/O Systems
- HART Interface Solutions
- Wireless Solutions
- Level Measurement
- Purge and Pressurization Systems
- Industrial Monitors and HMI Solutions
- Electrical Explosion Protection Equipment
- Solutions for Explosion Protection

Industrial Sensors

- Proximity Sensors
- Photoelectric Sensors
- Industrial Vision
- Ultrasonic Sensors
- Rotary Encoders
- Positioning Systems
- Inclination and Acceleration Sensors
- Fieldbus Modules
- AS-Interface
- Identification Systems
- Displays and Signal Processing
- Connectivity

PEPPERL+FUCHS

www.pepperl-fuchs.com

Printed in USA · DOCT-B1N4 08/17