160 Commerce Drive, Suite 500
Montgomeryville, PA 18936
U.S.A.
Phone: 267.421.5300
Fax: 215.701.8712
sales@panaceatech.com
www.panaceatech.com

# Asset Management: Securing and Future-Proofing the Plant Floor

***Current Landscape***

In the ever-changing manufacturing landscape, PLC and SCADA systems have become increasingly complex. The complexity can be attributed in part to advancements of technology; but it can also be tied to the evolution of the plant floor network as more and more systems can connect directly to the network rather than having to connect through third party proprietary networks. As manufacturers continue to grow, automation systems expand and obsolete systems are migrated to modern systems that plug directly into to the plant floor network as well.

This has led to manufacturing network architectures tying together numerous diverse devices that vary in functionality and purpose. Although modern control systems utilize Ethernet for the plant floor connectivity, the overall architecture may contain several ancillary and sometimes proprietary networks to communicate between the various components.

***Growing Data Requirements***

PLC systems are now tasked with far more than machine level control and are required to provide large amounts of data and connect to numerous enterprise level systems including SCADA systems, Batch Systems, MES Systems, Companywide Historians, PAT Systems, and Compliance Systems just to name a few. It has become apparent across the industry that isolating the PLC and HMI from the rest of the enterprise network is no longer an option.

As more and more data is being produced and collected, coupled with an increasing number of "Internet of Things" devices, these highly connected systems have created problems with security and asset management. Once these systems are connected to the plant wide network infrastructure, it is critical to secure and protect them from adverse interference from the external enterprise network.

***`Increased Security Concerns***

As plant landscapes evolve, so does the complexity of the software and configurations running it. The threat of unknown or undocumented changes, both inadvertent and malicious, continues to rise. This can be especially problematic as the lines of responsibility blur across the Quality, Engineering, Automation, Operations, and IT divisions within a company. The need to maintain revision control, track user actions, and provide security and backups for diverse vendor devices has never been greater.

The once tried and true method of utilizing procedural control and restricted physical access becomes nearly impossible once the plant floor network becomes accessible from the enterprise network and the internet. There have been several cases of manufacturing networks being subjected to external attacks. Regulatory agencies have issued observations on the deterioration of this control. It has become increasingly necessary and sometimes mandated to have a plan to deal with these issues.

***The Solution***

Panacea Technologies has a solution to this problem, and has been providing assistance with these issues for over 15 years. Its approach to security integrated with its well-tested solution has been successfully implemented at a number of sites. Panacea's solution solves many of the aforementioned concerns while providing clients a more secure method to access and control their manufacturing across the plant floor networks.

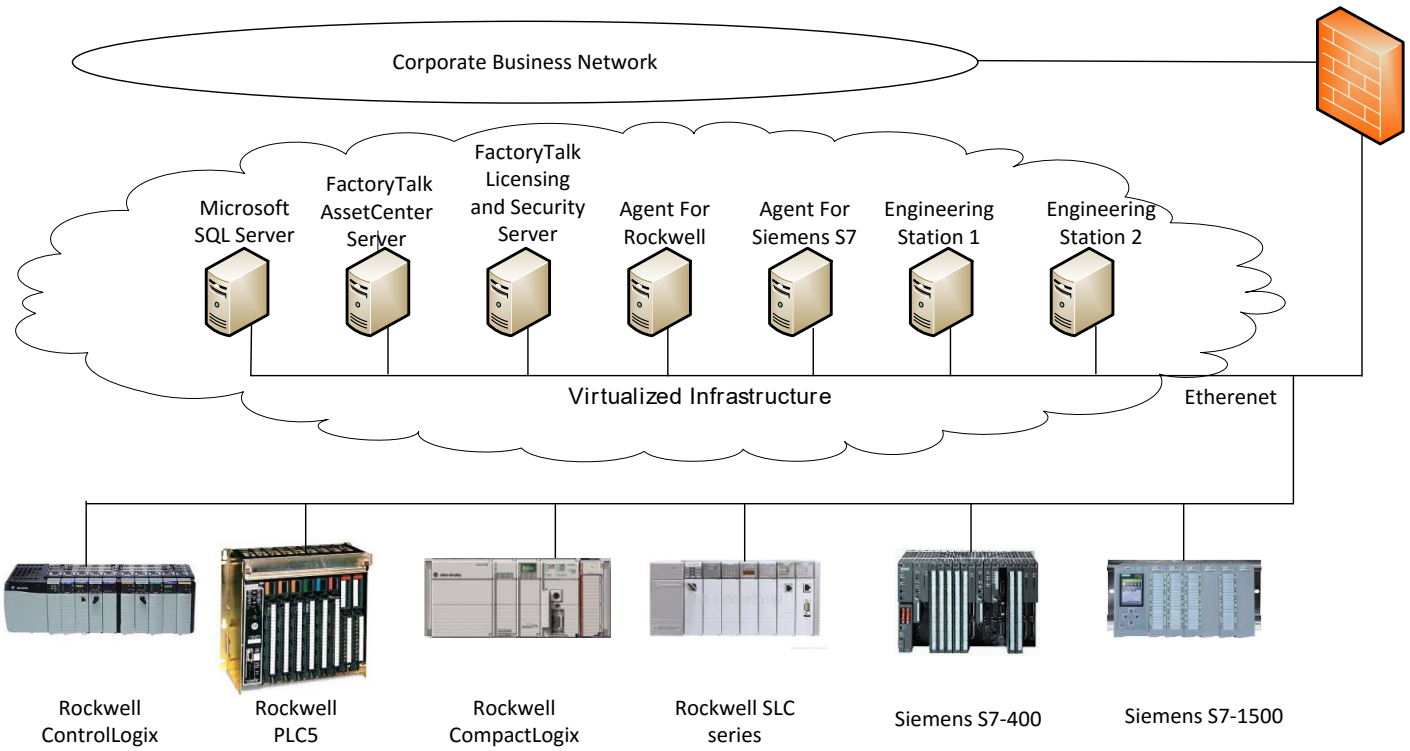
## Benefits of Implementing this Proven Solution

- A secure centralized method to provide an audit trail, facilitate change control, and provide an access management method over PLCs, I/O networks, and SCADA systems.
- Access to all previous versions of the PLC software, or other digitial file formats.
- Reports between different versions of the PLC software that identify the changes between the various versions.
- Implementation of a defense-in-depth security architecture for additional security of your control infrastructure. A controlled set of engineering terminals that are granted access to the PLC software. Simply getting to the plant floor network will not be sufficient to gain access to the PLC.
- Automatic periodic verification of the online PLC software with the controlled offline copy.
- Deployment options on either an existing or new virtual infrastructure making it extremely robust.
- Panacea can supply the .OVF (Open Virtual Format) files for all servers in our design, greatly speeding up deployment.
- Source control and difference reports for any electronic files including Microsoft Office documents, CAD files, Emerson DeltaV FHX exports, etc.
- Automatic version control and disaster recovery capabilities, as well as detailed logging of any and all changes.
- Panacea has Functional Requirement Specifications, Detailed Design Specifications, and Testing Documentation that can be used as the starting point for generating your regulatory documentation greatly decreasing deployment time.

***Architecture***

Panacea's suggested architecture is shown in **Figure 1**. The architecture depicts a suggested solution deployed on a virtual infrastructure. It can be modified to fit any system containing a number of different assets, but **Figure 1** depicts a commonly seen plant floor representation.

## .Figure 1: AssetCentre Architecture




**Microsoft SQL Server** – The Microsoft SQL server stores all past configuration data.

**FactoryTalk (FT) AssetCentre server** – It contains the application that interacts with the SQL server to store configuration data, it also interacts with the FT AssetCentre clients to provide them access to current and previous versions of the configuration data. The server can also perform comparisons of two versions of PLC software, text files, or any file format that has a comparison utility. As an example it can be used to compare two DeltaV configurations using Panacea's FHX File compare for DeltaV utility.

**FT Licensing and Security Server** – The licensing server serves as the central hub for Rockwell Licenses that can then float in real time to the various other servers and engineering stations. It also is a repository for the FT Directory Server software that adds an application security layer to Rockwell software and products. It provides application and device security that controls who can have access

to Rockwell software products, the actions they can perform, the devices on which they can perform those actions and the specific computers they can perform those actions from.

**Agent for Rockwell** – This server contains FT AssetCentre Agent and FT AssetCentre Disaster Recovery for Rockwell software. FT Agents are programs that communicate with the FT AssetCentre server and perform scheduled tasks on behalf of the FT AssetCentre server. They can automatically access online PLCs and compare their software to the latest official version stored in the FT AssetCentre Server. Agents can then store or email reports of any discrepancies they find. They can also be configured to simply backup the online PLC software periodically. The Rockwell agent works with all Rockwell PLC software.

**Agent For Siemens S7** – The Siemens agent works similar to the Rockwell agent and provides automatic access to S7 controller code. Similar agents are available for Siemens S5 controllers, Fanuc, GE-IP, ABB and Yaskawa Motoman Robots.

**Engineering Stations** – The engineering stations have FT AssetCentre client and programming software such as Logix5, Logix500, Studio 5000, FT View SE, etc. Note: Licenses for these products do not need to be loaded on the engineering stations because the licenses are acquired as needed from the FT Licensing Server.

***Conclusion***

As automation assets begin to age, and networks continue to evolve asset management is a must for any plant environment, especially those that are regulated. Deploying this proven solution on a virtualized infrastructure helps secure your process from inadvertent or malicious changes as well as provides you with a centralized way to track revisions and log changes. This solution can help decrease downtime, provide storage for a variety of electronic file formats, and aid in revision control thus lowering the Total Cost of Ownership for any control system. Utilizing this strategy will provide security, control, change management, verification and recovery all in one solution.

---

***About Panacea Technologies***

Panacea Technologies Inc. is an automation systems consulting firm located in Montgomeryville, Pennsylvania. Panacea provides services encompassing various stages of projects in the field of process controls and factory automation.

Since 1996, Panacea has been serving clients in industries including pharmaceutical, biotech, oil, gas, and chemical manufacturing. Our edge has largely been due to a broad-base expertise in services and solutions ranging from feasibility studies to implementation. Services we provide include control strategy studies, system lifecycle documentation, design, configuration, startup support, and maintenance for clients in manufacturing industries. Panacea Technologies Inc. also provides validation services to the pharmaceutical industry with a particular emphasis on S-88 based system validation and 21 CFR 11.

**Panacea Technologies Inc. is a VMware® Partner, and Rockwell System Integrator Partner.**

**Contact Panacea Technologies Inc. at (267) 421-5300 x105 or at sales@panaceatech.com to request an onsite demo or signup to receive an invitation for the next web demo.**