The Protected Plant

How a modern process automation system mitigates risks to operational integrity

by Mike Chmilewski, Alain Ginguene and Grant Le Sueur

Executive summary

This is second of a three-part series exploring how today's most advanced process automation systems deliver new functionality to the process-driven business. Leading off, "The Future-Proof Plant" described how the modern automation system has evolved to offer real solutions to three critical obsolescence challenges facing industrial process operations. This second paper, "The Protected Plant," focuses on the process-connected aspects of a system that impact business continuity by mitigating risks to operational integrity. The third paper, "The Enlightened Plant," explains the new operational insight that can be delivered to plant operations once basic needs for reliable, secure performance are met.

Foxboro®

by Schneider Electric

Introduction

As the power of automation systems to create effective industrial process operations has grown, threats to that effective operation have also increased. What are those threats? Can a next-generation automation system deal with them successfully? And perhaps most importantly, what protective qualities must such a system possess?

The threats in brief

Key issues are those that can impact operational integrity. This may be defined as the capacity of the process system or plant to maintain its whole or unified state. It's the unhindered ability of the system and plant to remain sound, to conduct productive operations on a routine basis, regardless of threat — meeting or exceeding production goals and remaining competitive in a given marketplace. We define operation integrity as: reducing risk to ensure continuous production, business continuity, safety and security.

The following are potential threats to this necessary operational integrity:

- Increasing speed and volume of business, plus non-strategic proliferation of data that can bring a system to its knees
- Cyber terrorism or other unfriendly attacks
- Natural disasters, such as floods or earthquakes
- Industrial accidents
- Advances in new technology, which demand greater processing power
- Poor planning

The system in general

In the face of the above threats, regardless of how advanced and capable your process automatio system is, it does little good if it is not running on the most robust, powerful and resilient technology platform available. In addition to being capable of handling increased processing demands that the future may bring, a future-proof system must have added reliability; protection from external forces; and a means of fast, economical recovery if things do break down.

To best reduce risks to the integrity that plants need for the next generation of industrial operations, we believe automation systems must possess at least the following characteristics:

- High-performance, highly scalable processors
- Multi-tiered historian
- Redundancy at the workstation level
- Redundancy at the emergency shutdown level
- Redundancy at the system level and fault tolerance
- Cyber hardening
- Proven expertise
- Controlled obsolescence
- Backup control room/remote operations

Each requirement is explored in more detail below.

High-performance, highly scalable control processors

One key consequence of the increased volume and speed of business is the amount of raw data that materializes in its wake. The third paper in this series describes some practices that can be used to reduce and manage the flow of that information. But even the most strategically run plants will be contending with more and more data, and computing requirements must increase accordingly. All indications are that Big Data is coming — and getting Bigger every day.

To avoid becoming overwhelmed, a modern process automation system must be designed accordingly. For instance, to ensure that users of the Foxboro Evo process automation system have processing power that will servethem well in this Big Data future, the system incorporates the Foxboro FCP 280 controller. It has twice the processing power of its predecessor. It also has four ports instead of one, and accepts input in the front instead of the back, making it easy for customers to mix and match I/O.

I/O mixing/matching capabilities help preserve operational integrity by providing the flexibility to add processing power on the fly, as required, without needing to invest in a major system replacement. If, for example, a plant were running both Foxboro and Honeywell TDC 2000 control systems, plant engineers could use a Foxboro competitive migration plug-in card in one port to connect to devices previously controlled by the Honeywell system. They could use another port to hold the Foxboro 100 I/O card, connecting to devices that may not require maximum baud rate to the Foxboro Evo system, and use the remaining ports to connect the balance of the system. This flexibility provides maximum performance while also protecting asset investments.

Multi-tiered historian

In addition to being able to process high volumes of data, modern industrial plants' systems must have a way to store and access it. Efficient processing requires a single point of access to all historical data. However, plants with multiple locations or plants running more than one brand of control system might well be operating different historians. Accessing all of this information puts a strain on both system and operating personnel.

Look for a system with a multi-tiered historian, which can aggregate data from multiple historians up to a common parent historian. When such an historian is SQL Server compatible, it can receive information from a wide variety of sources, including Excel spreadsheets. And where traditional historians may support up to 500,000 data points, models such as the state-of-the-art historian developed for the Foxboro Evo system supports up to two million points in a single instance, or many more in multiple configurations.

Redundancy at the workstation level

In traditional configurations, workstation users interact with data via an HMI, which sends requests to a server — which then fetches information from the controller and displays it to the user. While quite efficient for PLC-driven implementations, this arrangement introduces a temporary loss of view considered unacceptable by many companies wishing to implement more complex control strategies.

A well-designed process automation system addresses this by configuring each workstation to fetch data directly from the controller. In this model, the user distributes 1-n HMIs around the plant, or the globe. If one workstation goes down, the user can still access needed data from another. This kind of resilience is useful in many applications, ranging from immediate troubleshooting to identify problems that may have caused the workstation to go down in the first place, to disaster recovery issues that may have impacted workstations at all locations. The key point: you avoid any temporary loss of view — and eliminate the server as a single point of failure that could otherwise halt the process.

Redundancy at the emergency shutdown level

Emergency shutdown applications are one area where PLCs do need high redundancy. A bad or lost signal to shut a valve feeding a dangerous chemical into a processing unit, for example, could result in hazardous effluent conditions or worse, jeopardizing people in the plant and in surrounding areas. Triple modular redundancy has proven the most effective architecture for avoiding failure on demand.

Among modern process automation systems, the Foxboro Evo system ensures this critical capability by providing a common interface to the Triconex Safety Instrumented system. This Triconex offering was the industry's first Triple Modular Redundant (TMR) safety system, and remains the most popular safety system in the world. The technology has been in use for 30 years without a single failure on demand.

Integration is accomplished via an advanced communications module, which brings data from the safety system to the same HMI and historian shared by the controller. However, it uses an asynchronous communications mode, keeping the safety system functionally isolated. The system is designed to allow users to integrate as tightly as their policies require, and also may be implemented in the context of Invensys tools and consulting services, which can help establish polices based on a more accurate profile of risk.

Redundancy at the system level

The imminence of large-scale disasters such as hurricanes, earthquakes and floods requires redundancy at the system level as well. In state-of-the-art systems, mirroring the operation of control logic in remote backup locations such as virtual servers eliminates dependencies between the physical hardware and software, providing end users with more capability to manage the availability of their applications, servers and equipment. Because the CPU, operating system and communications are relatively contained, it is much easier to move virtual machines between host computers. This enables implementation of a variety of fail-safe scenarios, each of which provides options for different levels of redundancy. So systems are more resilient and less prone to equipment failure and site failure, as well as simpler to upgrade.

In the event of a system failure in one plant location, such a system could fail over to a backup disaster recovery system mirrored on the other side of the world, or in the cloud. Such failover can take place in minutes or even seconds, getting a plant up and running with minimal service interruption.

Cyber hardening

Although some managers may feel that their standalone legacy plant systems are more cyber secure than more modern, more open systems, this does not take into account how much new technology may have been added over time. Cyber security considerations must be designed into the system from the start; they are not something that can effectively be added at the end. Microsoft, Symantec, and a number of standards and regulatory agencies have been cooperating on these issues, providing guidance that defines the essential requirements for cyber hardening.

Such a system should be systematically hardened according to these evolving guidelines. It should include state-ofthe-art capabilities for creating stronger passwords, for example, by mixing types of characters plus controlling length, managing failed password attempts and dealing with password aging. The new system should also avoid unused programs, services and ports, which can contribute to vulnerability in aging systems. And third-party validation, such as the Achilles Certification from Wurldtech, can be a useful recommendation, if not a requirement; it indicates that a given system surpasses the industry benchmark for the deployment of secure industrial control devices.

Rock-solid implementation

Ensuring operation integrity begins at implementation. Whether building a new plant from the ground up or expanding existing capacity, schedule delays, change orders and the lack of availability of key players threaten the long-term integrity of the system. Also, budget constraints sometimes require substituting good decisions for optimal decisions.

Proper system design can have a major positive impact on such implementation woes. Case in point: the Foxboro Evo system improves integrity at the implementation level by combining server virtualization and Foxboro Intelligent Marshalling.

Virtualization can speed up the process by eliminating a significant bottleneck early on. Bottlenecks occur because good practice dictates not procuring workstations until the control system is fully designed, which can be as much as threequarters of the way through the overall schedule. In many cases, configuring the workstations to run the new system can't begin until the workstations have arrived — but they could already be out of date by the time the system is delivered. By enabling configuration of automation on a virtual server instead of physical servers, the Foxboro Evo system makes it possible to have the system configured before selecting workstations. This can compress the delivery schedule by months, and allow process engineers to devote maximum attention to quality control procedures.

The same is true of I/O. Characterizing wiring connections to field devices is among the most labor-intensive parts of control system installation. Traditionally, one can't begin until there is a finalized plant design and instrument schedule, even though you may not actually be ready to make that choice until later in your design process. Using Foxboro Intelligent Marshalling universal I/O technology, however, decouples the design of the cabinets and wired processes from the field device type. This compresses the delivery schedule significantly, by creating standard cabinets early and programming them later for whichever field device types are chosen. If the I/O is software-configurable, characterization can even be done remotely, adding greater flexibility and efficiency.

In addition to enabling remote I/O configuration, virtualization reduces risk at the implementation stage by simplifying global collaboration on all aspects of the system design and I/O characterization. In the Foxboro Evo system, this is accomplished via implementation of the Foxboro Intelligent Engineering Workbench. This enables engineers located anywhere in the world to work together in real time to design, test and debug their system in a fraction of the time that might otherwise be needed. Individuals with specialized talent can now apply their skills to system engineering no matter where they are located, even thousands of miles away from the hardware. Moreover, if multiple process designers or contractors are involved, testing and validating can be done concurrently at several locations instead of solely at the equipment site.

Controlled obsolescence

The best way to avoid obsolescence is to swap out parts as they near the end of their useful lives, but before they actually fail. Large building complexes, for example, have found what they call “group lamping” to be more cost-effective than replacing bulbs one at a time as they fail. Lamps are replaced wholesale according to intervals based on expected lifecycles. Some useful life is lost, but because replacement can be done during off-hours, for example, the benefits in business continuity far outweigh the costs.

The component object architecture delineated in the first paper of this series makes this approach applicable to the process automation world as well. In a final example, Invensys delivers Foxboro Evo as part of its planned upgrade program, which provides customers with a detailed roadmap to the lifecycle of each component so they can know exactly when a particular component will reach the end of its useful life. Thus customers can avoid the consequences of aging systems, and greatly reduce the risk of unplanned shutdown.

This changes everyone

Ultimately, advanced process automation offerings such as the Foxboro Evo system implement such robust technology, wrapped in so many layers of protection, that they enable everyone in the plant to fulfill their roles more effectively. Those involved in the process-connected aspects of the system are better able to do their jobs. Those in the control room side of the business are able to concentrate on moving operations to new levels of effectiveness — without worrying about risks to the integrity of the system that delivers them.