

Control System Design and Reliability

Reliability by Design

A reliable and robust industrial control system is comprised of two major components: physical hardware (control panels, sensors) and software (control programs, the operator interface). To be reliable and robust, the system must include carefully designed and deployed hardware and software. Industrial control applications differ greatly from other computing tasks such as HVAC environmental control and office applications (accounting, word processing) – because an industrial control system malfunction can be very costly in terms of product loss, safety, and liability.

In addition to being robust and rugged, industrial control **hardware** must be 1) “fault tolerant” (able to withstand and recover from the abuses of an industrial environment), 2) deployed at the point of use to reduce installation costs, 3) autonomous to allow local operation in the event of communications malfunction, and 4) purpose-built (designed and built specifically for industrial control - not adapted from a lightweight commercial or office-grade design).

Industrial control **software** must be developed specifically for industrial control systems, not adapted from simple HVAC or office application. Like hardware, industrial control software must be robust, fault tolerant, and capable of reliable operation under abnormal circumstances.

Control System Architecture

Methods for implementing an industrial control system generally fall into one of three categories:

1. *Distributed Industrial Control System.* Typically comprised of a network of powerful industrial control panels interacting with one another. One or more PCs are deployed as operator interface stations but are not critical to the operation of the actual control system. Control systems of this type are the most reliable and powerful but are also the most complicated to design.
2. *PC-based Control System.* Typically a single PC controls the entire facility as well as serves as an operator interface. This type of control system is the simplest to design, but suffers from many reliability issues.
3. *PLC (Programmable Logic Controller) based Control System.* Typically comprised of a network of PLCs with an PC operator interface. This type of control system can be reliable, but is the most difficult to design and suffers from very simplistic control

strategies. Some vendors deploy a hybrid PC/PLC system that significantly degrades control system reliability.

So Why Not a PC-Based Control System?

PCs are widely available, have powerful processors, are an inexpensive commodity, are highly connected via corporate networks and the internet, and have legions of programmers writing software for them. It is no wonder that PCs are often considered as the basis for a control system.

However, PCs suffer from numerous disadvantages when used in an industrial environment because they:

- are designed and programmed for office tasks (spreadsheets, word processing, internet access),
- are dependent on numerous mechanical devices with limited life spans (hard drives, cooling fans etc.),
- are subject to constant attacks by viruses and hackers, and are vulnerable to lock-up at the most inopportune time,
- become quickly obsolete and are only repairable for several years at most,
- are not designed to respond in “real time” (for example, a PC may halt operation while waiting for a printer), and
- require ample ventilation in a relatively clean office-type environment (realistically, an operator PC needs to be placed where it can be easily accessed by plant personnel - often a dusty maintenance building).

A PC also lacks a “fail-safe” hardware mechanism (known as a watchdog timer) that will force the system into a safe condition if PC hardware or software malfunctions. PCs are also easily disabled by common mishaps such as spilled coffee. All these things tend to make PCs unreliable, especially in an industrial setting.

What about “Industrial” PCs?

An industrial PC is basically a standard PC installed in a protective enclosure that make it tolerant of dusty environments and careless coffee drinkers. It still possesses most of the weaknesses of an office grade PC.

The Single “Egg Basket” Risk

A PC-based control system combines nearly the entire control system’s functionality into a single PC. This is analogous to “putting all your eggs in one basket”: a single event can have catastrophic results. A PC-based control system “basket” contains the following:

- All system software programs and functions that control equipment, monitor safety levels, track product quality, and so forth.
- All control system settings such as operational and safety setpoints specific to facility operation.
- All historical data vital for safety and product quality assurance.
- Plant Operator Interface, such as the menus and screens that the operator interacts with to monitor and modify control system behavior.
- Remote Operator Interface, shared with the onsite Operator Interface via a dial-in Modem and “pcAnywhere™” type software.
- Alarm Annunciation to alert an operator, either on-site or off-site, of an equipment malfunction or unsafe operating condition.

Combining all these critical functions into an unreliable PC-based control system makes your business vulnerable to many likely modes of failure, most of which can result in entire plant shutdown, unsafe operating conditions, and loss of data. This is a significant, probable risk for any business using a PC-based control system - a risk you can easily avoid by selecting a reliable control system architecture designed by a reputable company.

Should a PC Never be Used in a Control System?

One might ask, “if PCs are so unreliable, why would you use one?” It’s true, PCs do have valuable uses - the ones they were designed for: data analysis, report generation and operator interface that simply displays current operational information gathered from an independent, dedicated control system. In this scenario, one or more robust, dedicated industrial microprocessor controllers (non-PC) control the facility’s operation. When PCs are properly limited to these functions, their sole tasks are then to allow the operator to *interact* with the control system to view status, adjust settings, analyze and correct operating trends, and so forth. *The failure or theft of a PC in this configuration will prevent operator access to the control system but will not prevent control system operation.* Deployment of multiple independent PCs will greatly mitigate this risk as an operator can use an alternate PC if the primary PC is not available.

What About a PLC System with a PC Operator Interface?

PLCs (Programmable Logic Controllers) are well suited for simple tasks such as mimicking mechanical controls such as thermostats and pressure switches. However, PLCs lack the powerful high level programming languages required to deploy effective energy efficient control systems.

Without sophisticated programming tools in the hands of a skilled control system programmer, a PLC control system vendor is unable to provide anything much more substantial than that of a simple mechanical control system. This lack of sophisticated programmability is why a control system vendor may be more inclined to deploy a PC-based control system than a PLC-based system.

How Does Logix Address These Issues?

Logix has designed and deployed true industrial control systems for over 20 years. A Logix System is comprised of a distributed network of independent industrial control panels deployed at their point of use. The control system is independently accessible from multiple networked PCs, dial-up Modem and internet connections. A Logix Control System is:

- *Robust* - Control is distributed throughout the facility in powerful independent panels at the point of control. Logix Control System software is specifically designed and implemented by Logix for industrial automation.
- *Fail-Safe* - Each Logix control panel features a hardware “watchdog timer” that will force all control points to a safe condition in the unlikely event of an unrecoverable malfunction.
- *Reliable* - Logix control panels contain *no* moving parts and *no* office-grade software such as the Windows® operating system. PCs are deployed as Operator Interface Stations only. A PC failure/virus/malfunction will not affect the operation of the facility. Logix Control Systems deployed 20 years ago are currently in operation.
- *Accessible* - Multiple, completely independent, operator-access networks (PC Network, Dial-up Modem, Internet, Interactive Voice) ensure the control system can be accessed in the event of an onsite PC malfunction. Because Logix does not utilize remote PC access software such as “pcAnywhere™”, a Logix Control System is always accessible even if the on-site PC is disabled.
- *Expandable* - Additional Logix Control Panels and PCs can be easily added to the control system as your facility grows. Corporate network access (LAN) allows multiple client PCs to independently access the control system, including access over the internet.
- *Secure* - Because the Modem is not connected to an on-site PC, the Logix Control System acts as a firewall between a dial-up Modem connection and the facility PC network. The control system itself is not subject to virus attacks and other security



breaches because it is not PC based and is not using Windows® OS or any other public interface.

- *Data Redundant* - Historical Data is stored on *each* connected PC as well as buffered on the control panel itself. This insures historical data is not lost if a PC should malfunction.
- *Designed with an **Open Architecture*** - An open, industrial standard interconnection bus is used in Logix Control Systems allowing for expansion with literally hundreds of devices from numerous independent vendors. Open protocol interfaces such as MODBUS, ODBC and OPC DA are available to integrate a Logix Control System and its data with an enterprise-wide system.
- *Interconnected* - A Logix Control System has the ability to monitor and control any device from any vendor with communications capability. Not only is the Logix Control System information available on-site and off-site, but information from other vendors' equipment is available as well. A Logix Control System can also be accessed over a corporate network and the internet. This comprehensive access to information allows accurate and rapid troubleshooting (both on-site and off-site), minimizes downtime and reduces service and overtime costs.
- *Durable* - Logix Control Systems deployed 20 years ago are currently in operation and are far from obsolete, still having a forward migration path for future expansion.
- *Cost-Effective* - The powerful energy efficient control strategies deployed in a Logix control system reduce operating costs and improve product quality year after year, making their Return On Investment (ROI) very competitive with alternative business investments available.

So Why Would a Control Vendor Deploy a PC Based Control System?

People naturally tend to use tools they are most familiar with and programmers are no exception. It is much simpler and cheaper to adapt an existing technology (such as an office PC) to a use it was not designed for than to go to the considerable effort and expense of designing a purpose-built control system specifically for industrial automation. Most control system vendors are not manufacturers but rather system integrators, cobbling together various components from various manufacturers.

So the question is really, **"Why use a control system that's advantageous to the control system vendor and disadvantageous to your business?"**

Your Business is Serious - Our Control Systems are Serious

