Cyber Automation & Autonomous Systems | PISIQ

Cyber Automation in a nutshell

Many of today's control systems use the same PC hardware, operating system and communications as corporate office and administrative networks. So automation systems security is an urgent issue, perhaps even a critical one.

This is where Cyber Automation comes into play.

Automation & IT systems are different

The use of common technologies – Intel PC-based computers, Microsoft Windows and Ethernet/TCP/IP – means that vital production and process control systems can be exposed to the same spam, virus and security threats that corporate IT departments have been facing for several years. It's tempting to suggest that, because they have the immediate knowledge and experience, corporate IT people should be responsible for total network security, including that of the automation and control systems. But this is wrong. The problems are quite different, and the urge to delegate the responsibility is misleading.

With automation systems there are definite differences of goals, objectives and assumptions of what needs to be protected. It's important to understand what "real time performance" and "continuous operation" really mean and recognize how well-intentioned software-based security solutions can interfere with automatic control systems.

Beyond the common architectures, many business networks are now connected with process networks. This has opened the door for hackers and viruses to enter the production and process environments. If ignored, or under-managed, this can lead to serious problems.

Many legacy process automation systems were designed for functionality and performance not security. They were largely proprietary and specialized knowledge was needed to work with them. System components were purchased as black boxes considering only their end-to-end function and there was little or no concern with interconnectivity with other systems. Control systems operated in isolation from the rest of the company, both technically and physically, assuming an environment of implicit trust. And so, when included in common networks, they are often the weak point in total network security.

It’s important to have separate networks where access to automation and control systems is strictly limited by routers and firewalls. Users and applications on control networks should be limited to those specifically required for the process—no email, no games, no Internet browsing. Control rooms may also need a business network for email and business applications, and budget-conscious administrators may suggest network commonality. But that’s short-sighted, and simply exposes the automation systems network to a plethora of problems. Parallel installation of different networks is not a luxury – it should be mandated.

Accidental or Deliberate

There are two general categories of control network problems: accidental and deliberate. Accidental problems are typically caused by cabling or configuration errors, or by faulty network devices. Many errors may be caused unintentionally (example, installation of anti-virus software may limit real-time functionality). A common problem is a computer-savvy employee inadvertently changing the configuration of a device, causing process disruption. These days unauthorized tampering with networks by well-meaning employees is becoming more common because people are more computer literate and control systems are increasingly PC-based.

Deliberate problems are caused by individuals with malicious intent, such as disgruntled employees or ex-employees who may be involved in theft and retaliation. And there are “hackers” who may do it just for the thrill, plus vandals and opportunistic criminals (including terrorists). Passwords usually provide only limited protection against hacking because most production and process control groups use easy-to-remember (and easy-to-guess) passwords on their systems and typically don’t change them regularly.

Accidental errors typically outnumber deliberate attacks in industrial environments. But the proliferation of viruses and the increase in PC-based control systems is causing a significant increase in deliberate system intrusions.

Deliberate attacks on automation control networks fall into one of these two categories:

• Viral Infection. Worms and trojans usually enter through mainstream software – Microsoft Windows, Internet Explorer and Outlook email on Intel-based computers. The chances of infection have increased in the automation environment because these technologies are being used more and more in control systems due to low cost and interoperability. A not uncommon problem is vulnerability to what is called “sneaker net” – the use of portable memory like floppy-disks, CDROMs or USB memory sticks to transfer data or programs. These could insert a virus or worm intentionally or unintentionally. Security policies must include both network protection (firewalls) and physical protection (making the server inaccessible).

• External Intrusion. Hacking of automation and control networks is increasing rapidly during recent years, as more plants and factories are connected to the Internet, or to corporate Intranets. Typically a hacker will get access to the business network, and then attempt to invade other computers or networked servers. Intranet web servers are a weak point in many industrial installations. They are used commonly as an effective data distribution tool; because they may not be directly exposed to the Internet, they are not usually maintained with the latest updates and security patches.

Hacking into a control system

PISIQ's Cyber security threats against automation networks can take different forms – the most publicized being worms and viruses. Many threats are indiscriminate, but all carry potentially destructive results. Here are some examples:

• Network Spoofing and Denial of Service attacks: Process alarms are lost because the network is clogged with spurious requests. Beyond just performance degradation, these are serious safety issues.

• Eavesdropping and password cracking: confidentiality and safety issues.

• Tampering, impersonation, system modification: The system is open to malicious intent.

Secure architecture & location

in Cyber Automation, Security comes from proper design, operation and maintenance of security architectures and infrastructures which provide up to date protection. An acceptable network security environment includes built-in high security engineered into the architecture, at the same time allowing operators, supervisors and administrators the ability to interact with the system without constantly getting into arduous, tedious and prolonged procedures. If it's too difficult, knowledgeable people will quickly find a way around the system – the well-intentioned, honest but impatient insider.

Well thought out network security architectures provide the mechanisms necessary to prioritize and manage traffic, restrict outside traffic, and give preferential treatment to control traffic. Systems pertaining around Cyber Automation must have the ability to recognize broadcast attacks that can create denial of service conditions, to prevent problem situations before they occur. When anything happens outside the bounds established for the control network, it must be captured as an auditable event as part of the Autonomous Systems, the event logs must be reviewed regularly to determine if unauthorized changes are made.

Anti Virus software from companies like McAfee or Symantec could be part of a good security strategy, but this is not sufficient. Standard anti-virus and anti-spam packages were developed for typical PC users, not for sophisticated, real-time control systems. They need to be adapted specifically for use with automation control systems.

Good Autonomous Systems should provide preconfigured security settings for files, directories, and registry keys to protect against viruses, malicious users, and inadvertent actions. There should be preconfigured groups and group policies that define desktop and console behavior: Operators should be limited to say just auto start applications, supervisors could be very secure, engineers could be restricted to relevant engineering functions, and administrators could have unlimited access with secure settings. Clearly the administrative procedures (password protection, etc.) should be subject to maximum security procedures.

Management of the network is the key to security protection. As they say about Quality, business performance, and even about Life – Network Security is a journey, not a destination!