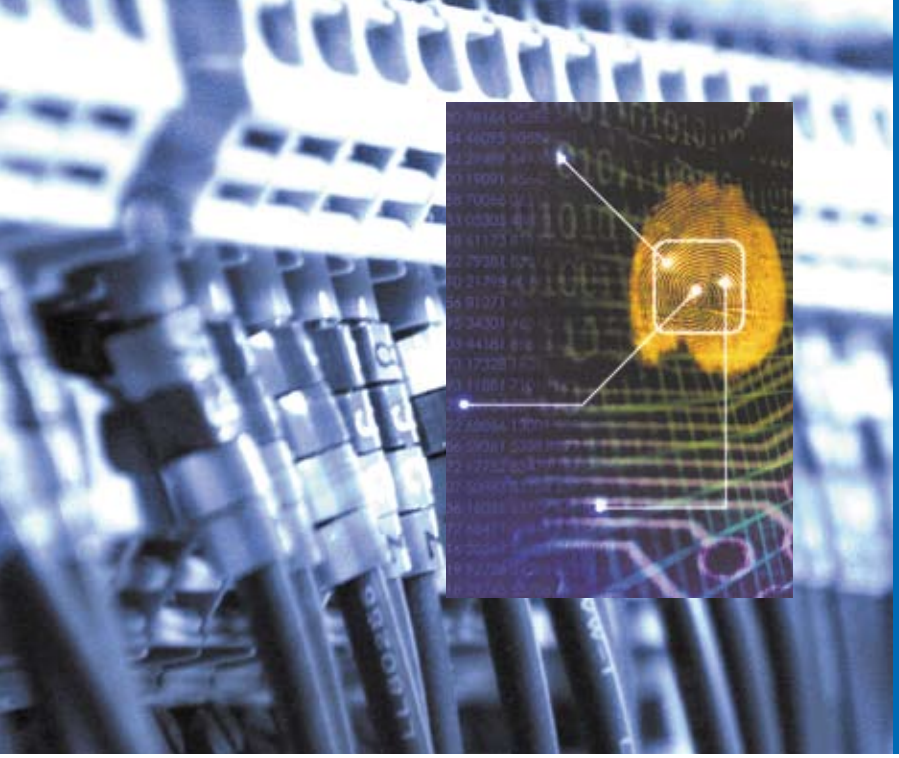


Technical Talk

By Mark Chisnall

Security checks for your manufacturing and control system

The machines we use in industry today are powerful and the integrated control systems that make them work are becoming extremely sophisticated. Controllers, drives and robots have thousands of lines of programmes and an equal amount of variables. Linked with IT systems controls can become vulnerable to security issues both internal and external, intentional and unintentional. The increasing need for information driven by ecommerce, supply chain management and internet connectivity puts further emphasis on the need for better security.

Companies also face more and more compliance requirements which often lead to alteration within the manufacturing process. It is therefore essential that information systems need to reflect these changes for accurate reporting and control within the plant facility. Unauthorised control program modification can result in reduced system reliability, unwanted production shutdown or wider implications with safety and quality.

Internally, even authorised staff may not have sufficient knowledge to modify control programmes which could effect the identification of security threats or even recognition that a problem was security related. Manufacturers must employ appropriate security techniques across maintenance and quality practises and in my opinion companies should seriously consider using an independent contractor with appropriate control system knowledge to oversee manufacturing change. As systems are becoming more sophisticated more companies are acknowledging their vulnerability and Suffolk Automation have seen a marked increase in support requests.

Protection in proportion

In general, you only need to protect things that have value to your business, and you should only apply protection in proportion to the value of the asset. This is an important concept, because investing in too much security creates an unnecessary expense and decreases accessibility to those who need access, which can hinder productivity. Evaluate and balance the level of exposure you are willing to risk against the importance of the assets being protected.

Manufacturing environmental changes regarding the complexity of the devices, networking, and regulations as well as pressure to perform financially, have contributed to the problems many companies are expressing.

It would be easy to keep things simple and not to use the more sophisticated devices, but that, for a progressive company involves going backwards. Engineers and maintenance personnel are not replacing controllers with the relay logic systems of yesterday. The use of sophisticated devices allows for much better coordinated control of all the variables associated with a manufacturing process, including tightly coordinated motion and information systems.

What does security mean?

Security can mean different things to different people. The best way to focus on this is to start by defining the terminology: Specifically, any loss of assets including product, plant, production, intellectual property, falls under the security umbrella. These losses can be extended to include physical damage to the environment and employees, and damage to the company reputation. In today's manufacturing environment integrated systems might include information about your customers, suppliers, order schedules, unit costs, recipes, procedures, quality benchmarks etc.

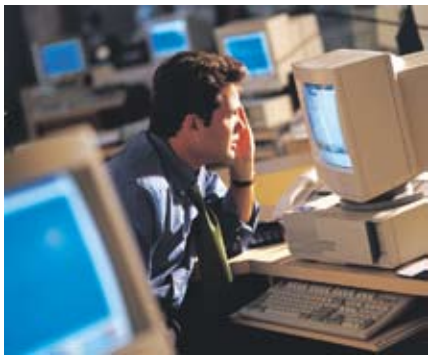
Business disruptions can come from many places, including both internal and external sources with the possibility of both malicious and accidental events. A recent study found that more than half of all security incidents were carried out by insiders. A similar study also found that half of these "insider" incidents were accidental.

Managing the risk

Start by evaluating and correctly prioritising the risks to your business processes and automation assets. It is critical to understand and evaluate the risks your business faces before taking remedial steps.

The next step is to develop a security program designed to reduce the identified risks to acceptable levels. Keep in mind that no security solution is

Technical Talk



perfect; your goal is to identify and manage the potential risks, and then reduce them to acceptable levels.

Every security programme should deliver a balanced approach to reducing risks, there are five major areas that should be covered;

a) prevention
b) detection
c) isolation
d) response
e) recovery

A security programme is only as good as its weakest link and a well balanced programme across all five areas will protect your business against unwanted and potentially damaging intrusions.

Layered Defence

Think of your first major defensive layer as a fortified wall protecting your company from the world at large. This protection would be in the form of a firewall, virus protection and other IT security tools.

The second layer of defence is an inner wall surrounding the plant and automation control. This layer isolates and protects the plant floor network from the rest of the company ensuring unwanted intrusion from unauthorised email, spam and denial of service attacks are blocked before causing potential harm to valuable manufacturing information and machinery.

Security through a double layered approach ensures you address not only network security but also data security, data integrity and network performance.

Other Considerations

Consider implementing security by installing a processor security lock. This feature can deny front port access to controllers from unauthorised personnel. You may even consider locking the cabinet doors and instituting a procedure for access.

Putting the key switch in "RUN" prevents remote programming by unauthorised visitors. One common problem in a connected controller environment is when employees are pressurised and rushed into configuring an incorrect device. If every device is in "RUN" except the one that you are altering, the odds of making a mistake are gone. Also, putting the controller in "RUN" requires a physical key change at the device to allow program configuration changes; therefore, even a visitor from outside could not alter the device until the key switch is changed from "RUN."

Consider implementing a centralised security administration system for configuration tools. This creates a much more secure environment, similar to moving from Windows for Workgroups (WFWG) to a domain-based system.

Today it is easy to spread a virus using a memory stick (the modern floppy disk). Work with IT to form a manufacturing, engineering, and IT group that understands manufacturing concerns and can work as a liaison with all of management, including operations, IT, and engineering, to better secure the automation systems. Within the group, consider some of the following:

Using antivirus, spyware, or malware tools; backup everything periodically; and create a realistic disaster recovery plan. Consider using root kit discovery tools. Be cautious here and consider testing all of this in a test lab prior to putting it into production.

Working with IT, analyse your system for security and sustainability – and install properly configured assets to support your disaster recovery plan. Outside companies such as Suffolk Automation will analyse your networks for current health and make recommendations. The net result of this type of analysis is that you will have an impartial baseline and know the exact status of each network in your automation environment.

They can also assess your automation systems security profile. This operation creates a baseline assessment for impartial strategic security planning.

Policy Enforcement

It is important to remember that policies are put in place to describe how employees and any authorised outsiders are expected to comply with processes and procedures. Policy enforcement means limiting access to your automation system to only those with a legitimate need. This is what security experts refer to as authentication and authorisation.

Conclusion

Information-Enabled Control Systems are critical to successful extraction of manufacturing data and turning it into business knowledge. Connecting these devices so that the data can be analysed and utilised in business and engineering decisions is not something to fear, but to be embraced with knowledge and awareness.

Mark Chisnall is Managing Director of Suffolk Automation, a company specialising in the design, development and installation of process control systems.

Please contact Mark if you have any questions on plant Automation or if you require a specific subject to be considered for future publication.

e: mark@suffolk-automation.co.uk
t: +44(0)1473 829188