The Myths and Facts behind Cyber Security Risks for Industrial Control Systems

Eric Byres, P.E.
Research Manager
BCIT Internet Engineering Lab
Burnaby BC, V5G 3H2
ebyres@bcit.ca

Dr. Dan Hoffman
Associate Professor
University of Victoria, Dept. of Computer Science
Victoria, BC, V8W 3P6
dhoffman@csr.csc.uvic.ca

KEYWORDS

Security, Ethernet, TCP/IP, Network Intrusion, Hacking, Control Systems, PLC, DCS

ABSTRACT

Process control systems, with their reliance on proprietary networks and hardware, have long been considered immune to the network attacks that have wrecked so much havoc on corporate information systems. Unfortunately, new research indicates this complacency is misplaced – the move to open standards such as Ethernet, TCP/IP and web technologies has let hackers take advantage of the process industries ignorance. This talk describes five network-based incidents that directly impacted process control systems and the lessons that can be learned from these security events.

INTRODUCTION

Over the past ten years industrial control systems have seen a significant increase in the use of computer networks and related Internet technologies to transfer information from the plant floor to supervisory and business computer systems. For example, most industrial plants now use networked process historian servers to allow business users to access real-time data from the distributed control systems (DCS) and programmable logic controllers (PLC). There are also many other possible business/process interfaces, such as using remote Windows sessions to the DCS, or direct file transfer from PLCs to spreadsheets. Regardless of the method, each involves a network connection between the process and the business systems.

At the same time, there has been an explosion in the use of Ethernet and TCP/IP in industry for process control networks. For many years the control systems used proprietary industrial networks, such as Data Highway Plus or Genius I/O, giving them a considerable degree of protection from the outside world. Today many DCS and PLC systems use protocols like Ethernet, TCP/IP, and HTTP as a critical component of their architecture, resulting in easier interfacing at the cost of less isolation and security.

CONFLICTING CULTURES

While technologies such as Ethernet and TCP/IP allow for significant cost savings and improved interfacing for industry, it is important to understand that their origins are rooted in a culture very different from the factory floor. Even the neophyte Internet user can spot these differences in terms of reliability – occasional failures are common and tolerated on the Internet while most control systems are expected to operate for months, if not years, without interruption. Similarly, the tradition of beta testing many new Internet products in the field and recovering from problems by simply rebooting servers or switches contrasts sharply with standard plant floor practices. This is not surprising since the risk impact of outages on the Internet are typically loss of data, while outages in the process environment will certainly result in loss of production and may even cause loss of equipment or life.

Very simply, the Internet culture and the technologies that it has created are based on the idea that performance is paramount and outages, while undesirable, are acceptable. This is clearly not true for the industrial system.

Nowhere is this cultural difference more pronounced than in the area of cyber security. Considerable media and research attention has focused on the topics of Internet viruses and hacking, but the reality is that most Internet hosts are only lightly secured. For example, KC Claffy of the Cooperative Association for Internet Data Analysis (CAIDA) reports that plaintext passwords are still very common on the Internet, a clear violation of the most rudimentary security standards (1). Similarly, until recently most IP networks were openly connected to the outside world, while the factory engineer has always demanded that the control system networks be isolated from the rest of the company information systems. Even where security is well defined, the primary goal in the Internet is to protect the central server and not the edge client. In process control the edge device, such as the PLC or smart drive controller, is considered far more important than a central host such as a data historian server.

Looking at these differences in needs and cultures, which the authors have attempted to summarize in Table 1, it is clear that the industrial control world must not blindly accept the solutions of the Internet world. These technologies may be extremely useful but they require careful consideration before they are implemented on the plant floor.

To understand how the solutions need modification in terms of cyber security, this paper looks at a number of industrial cyber security case histories and the lessons these can teach us about the dangers of blind adoption of Internet security strategies on the plant floor. We then discuss series of recommendations for a sound plant floor approach to incorporating Internet Technology.

TABLE 1: COMPARISON OF INTERNET AND FACTORY FLOOR EXPECTATIONS AND PRACTICES

	Internet	Factory Floor
Reliability	Occasional failures tolerated Beta test in the field acceptable	Outages intolerable Thorough QA testing expected
Risk Impact	Loss of data	Loss of production, equipment, life
Performance	High throughput demanded High delay and jitter accepted	Modest throughput acceptable High delay a serious concern
Risk Management	Recover by reboot Safety is a non-issue	Fault tolerance essential Explicit hazard analysis expected
Security	Most sites insecure Little separation between intranets on same site Focus is central server security	Tight physical security Isolated MIS network from plant network Focus is edge control device stability

REPORTED INCIDENTS

The British Columbia Institute of Technology Internet Engineering Lab (BCIT/IEL) maintains an industrial cyber security incident database that tracks incidents involving process control systems in all sectors of manufacturing. While most companies are reluctant to report cyber attacks or even internal accidents, there are now enough events to allow some basic statistical analysis of the data.

Since the initiation of the tracking project, 22 incidents have been logged in the database. Interestingly some of these incidents occurred long before the Internet became a household word. For example, the first reported case of plant floor “hacking” occurred in 1988 on an Allen-Bradley DH+, which was used by an angry worker to modify a different department's PLC-5. He (or she) changed the password to something obscene, blocking all maintenance access to the system (it was believed that the culprit found the original password on a post-it note).

Incidents like the one noted above also highlight the fact that the standard IT firewall approach to security will not protect the plant floor since most incidents are occurring inside the firewall. Even when the attackers are on the outside, firewalls don’t always protect the factory floor. For example, in October 2001, an Australian man was sent to prison for two years after he was found guilty of hacking into a waste management system and causing millions of liters of raw sewage to spill out into local parks, rivers and the grounds of a Hyatt Regency hotel (2). He did it because the area’s Council rejected the job application he had made to work as a controls engineer at the plant. Court reports show that he attacked the control system not through the firewall, but through a wireless network used for SCADA control.

Often the incidents are not deliberately malicious but the results are devastating nonetheless. A good example of this type of problem occurred in a large East Coast paper mill in 1998 (3). The mill had just completed an upgrade of its paper machine, during which a number of engineers had been brought in from head office to assist with DCS commissioning. Everyone on the DCS commissioning team knew the passwords for the control system computers and when the project was completed, no one bothered to change them.

Trouble started about a month later when one of the head-office engineers decided he needed a good data source for an expert-systems experiment he was running. Using the company's wide area network (WAN), he was able to connect into the mill network from the corporate headquarters several hundred miles away. Once into the mill's business LAN, he was able to connect to the DCS through a link originally set-up to allow mill supervisors to view operators screens from their offices. He then loaded a small program onto one of the DCS graphics stations (a UNIX machine). This program asked all DCS devices to dump their data back to him once every five minutes.

All this would have worked fine, except that the engineer's new task would occasionally overload one of the DCS to PLC communications gateways, and it would stop reading the PLC data. This, of course, caused the machine operators great panic as they lost control of the motors controlled by the PLCs. Soon the electrical department was busy troubleshooting the PLCs. Meanwhile the head-office engineer had left the company to work for a competitor.

Eventually the problem was solved by an eagle-eyed mill engineer who noticed that the problems always occurred at intervals that were at multiple of five minutes. Suspecting that it might be software induced, he started to inspect all the tasks running on the DCS computers and found the offending task. Of course, by then the lost production in the mill had been substantial.

LESSONS LEARNED

These incidents and the others in the database can provide some important guidelines as to the causes of industrial cyber events. The first conclusion we can draw is that there is a problem and it may be more widespread than most process engineers believe. These incidents show four clear groupings that can be listed in approximate order of severity as:

- Audit
- Accidental
- Non-malicious intrusion
- Malicious intrusion

The second lesson is that of these incidents, employees caused over 50% of them. This correlates well with data from FBI studies on the sources of cyber attacks:

> *A study by the FBI and the Computer Security Institute on Cybercrime, released in 2000 found that 71% of security breaches were carried out by insiders. This is supported by the realization that persons with high technical skill and process knowledge pose the greatest threat to an organization.* (4)

In other words, most of the security risks to a control network may not be an Internet teenager on a joy ride, but rather, a disgruntled employee.

If attacks do occur from outside the plant floor, the infiltration rarely occurs directly from the Internet. Instead it typically is via backdoor connections such as:

- Desktop modems

- Wireless networks
- Laptop computers
- Trusted vendor connections

Another cause of security events is a blind dependence on the IT security department. Most IT departments' primary responsibility is to prevent external threats through firewall and account management. They are generally unfamiliar with process reliability issues, equipment or industrial protocols and thus must work with the plant floor engineers to create an effective solution. In many plants political infighting prevents this from happening.

Finally the vulnerability of PLC, DCS and SCADA Systems is poorly understood and usually underestimated. Most control systems, particularly the human machine interfaces (HMI) rely heavily on Microsoft Windows operating systems with vulnerabilities that are well understood by hackers. The controllers systems that are not Windows-based generally have poor security designs and weak protection. These systems have tended to hide behind "security through obscurity". It has become clear that hackers don't need to understand a system to wreck it.

RECOMMENDATIONS

These security incident database results show that hackers have both the means and the will to disrupt DCS and PLC operations. Ten years ago that might have been unlikely since process networks were proprietary systems that were isolated from most corporate systems. Today that has changed because we are building sensor-to-boardroom integrated systems that use open standards such as Ethernet, TCP/IP and web technologies.

Depending on the corporate firewall to protect the process isn't the answer because it ignores the fact that at least 50% of all corporate hacking is from inside the firewall. To make matters worst, there are a number reasons that standard IT security standards can't be directly applied to the plant floor. First the nature of process control systems, with their reliance on unusual operating systems and applications, means that many of the software-based security solutions will not run, or if they do run, they will interfere with the process systems. Secondly, traditional IT security techniques focus on threats from outside the organization. As we noted earlier, this is not the primary risk for process control security. So the process control world is faced with creating its own security standards.

Where do you start if you want to build a solid cyber defense for your control system? At the present time, there are few best-practices guides or standards to guide process engineers, so the challenge is considerable. However they are not insurmountable if an organized implementation strategy is followed.

The first step is to conduct a cyber-security audit of your control systems to understand exactly how secure your system is today and where its vulnerabilities might lie. These audits typically will have a slightly different focus from the usual IT security audit, due to the different systems and goals of the process environment. It is also critical that it be conducted by people familiar with both security and plant floor operations – in one documented incident an inappropriately used cyber scanning tool was responsible for accidentally shutting down all the operating PLC systems on the floor of a major food manufacturer.

The next stage is to develop a security policy for process control systems: a statement of the goals, responsibilities and accepted behaviors required to maintain a secure process environment. The policy gives broad guidance and demonstrates senior management support for security-related facilities and actions across the organization. A security policy should be technology and architecture independent and should omit the implementing procedures and processes. In other words, the security policy outlines what you want to achieve, not how to do it.

Once the security goals are defined, an overall network architecture can be developed. This usually involves creating a multi-level network with firewalls between the layers. For example, a simple architecture might divide the plant into two levels – a business network level and a process control network level. For firewalls there a number of options to choose from. The simplest and fastest is usually a packet inspection firewall that checks each network packet against a filter list to determine if the packet should be forwarded or not. These can often be implemented directly in an Ethernet switch. More complex firewalls include proxy firewalls and air-gap systems. Regardless of which style you select, it is usually best to make it a different brand than the one used for the corporate Internet firewall.

While the firewall is the lock on the door to the process network, it is not the burglar alarm. You need some method of monitoring traffic and identifying malicious activity on the network. The tool to achieve this is known as an intrusion detection system (IDS) and can range from a simple scan detector, to a heuristic engine that profiles user behavior, to a system that takes explicit action against the suspected intruder. In the process world, traffic patterns tend to be very consistent so even simple traffic matrices that show who is talking to who can be a big help. For example, if a PC in the accounting area suddenly starts chatting up a storm to a PLC, it might be time to take a closer look. An IDS can also help you configure your firewall filters by showing what traffic patterns are normal and what patterns need to be blocked.

The layered security model is very strong if it is implemented without exceptions. Unfortunately, we all know there will be exceptions. For example, a control vendor may need to connect to a PLC via a modem to offer technical support. As tempting as it might sound, banning non-standard connections outright is not usually feasible since the primary goal is ease of production, not ease of security. What is needed is a system which can ensure that exceptions are logged and handled by means other than the standard firewall access. For example a configuration policy and tracking system of all modem connections might be a first step. A more advanced solution might be to set up a secured remote access server attached to the firewall as a common dial-in point for all vendors.

The final stage of the security strategy is to develop an incident response plan. Many times we have worked with companies that know they are being hacked but don't know how to deal with it. Rather than waiting until they were in trouble, these firms should have established a Security Response Team and a process to deal with incidents in advance. The team would monitor events and be prepared to act quickly in the event of a serious incident.

CONCLUSIONS

Over the past ten years industrial control systems have seen a significant increase in the use of computer networks and related Internet technologies to transfer information from the plant floor to supervisory and business computer systems. At the same time, there has been an explosion in the use of Ethernet and TCP/IP in industry for process control networks. While technologies such as Ethernet and TCP/IP allow for significant cost savings and improved interfacing for industry, it is important to understand that their origins are rooted in a culture very different from the factory floor.

Both recent industrial experience and laboratory tests of Ethernet-based PLCs clearly show the risks of adopting Internet technology without careful attention to security. With proper planning, however, the risks can be mitigated. Most important are a security policy, careful design of the network architecture, exception tracking, and an incident response team.

Internet technology has much to offer on the plant floor. The trick is to adopt the technology but not the culture.

REFERENCES

(1) KC Claffey, "Internet measurement: myths about Internet data", http://www.caida.org/outreach/presentations/Myths2002, CAIDA, UCSD.

(2) http://www.theregister.co.uk/content/4/22579.html.

(3) E.J. Byres, "Network secures process control", InTech, Instrument Society of America, pp. 92-93, Oct. 1998.

(4) T. Stephanou, "Assessing and exploiting the internal security of an organization", SANS Institute, Mar. 2001.