Security incidents and trends in SCADA and process industries

Supervisory Control and Data Acquisition and industrial control systems, with their traditional reliance on proprietary networks and hardware, have long been considered immune to the cyber attacks suffered by corporate information systems. Unfortunately, both academic research and in-the-field experience indicate misplaced confidence. The move to open standards such as Ethernet, TCP/IP, and web technologies allows hackers and virus writers to take advantage of the control industry's ignorance. The result is a growing number of unpublicised cyber-based security events that are affecting critical infrastructure and manufacturing industries. **Eric Byres, David Leversage and Nate Kube**

In making the case against complacency about control system security, this report summarises the incident information collected in the Industrial Security Incident Database (ISID). It describes a number of events that have directly affected process control systems indicating that the number of cyber incidents against SCADA and control systems worldwide has increased significantly since 2001. The majority of these incidents are coming from the Internet by way of opportunistic viruses, Trojan horses, and worms, but a surprisingly large number are directed acts of sabotage. In addition, the analysis indicates that many SCADA/process control networks (PCN) have poorly documented points of entry that provide secondary pathways into the system.

Historically, the industrial control and SCADA systems that are responsible for monitoring and controlling our critical infrastructures and manufacturing processes have operated in isolated environments. These control systems and devices communicated with each other almost exclusively, and rarely shared information with systems outside their environment.

As more components of control systems become interconnected with the outside world using IP-based standards, the probability and impact of a cyber attack will heighten. In fact, there is increasing concern among both government officials and control systems experts about potential cyber threats to the control systems that govern critical infrastructures. Even the flaws in SCADA specific technologies have become general knowledge – detailed presentations on how to exploit SCADA vulnerabilities have been given at black hat public gatherings[1]. What is lacking is good historical data to either back up or dismiss these concerns. Event data collected over the past five years by ISID could provide objective, relevant statistical data for security decisions.

The Industrial Security Incident Database

In early 2001 a security research team at the British Columbia Institute of Technology (BCIT) was asked by a major petroleum refining facility to investigate the possibility that their control systems could be impacted by cyber-related events such as hacking or viruses. In the course of this study it became apparent that accurate historical data on cyber impacts was badly lacking in the SCADA or process industries thus making accurate risk assessment extremely difficult.

To address this shortcoming, the authors founded ISID with assistance from Justin Lowe of PA Consulting. Modelled after similar safety-related databases in the process industries, ISID is intended to serve as an industry wide repository for collecting, analysing, and sharing high value information regarding cybersecurity incidents that directly affect SCADA, manufacturing, and process control systems. It provides an historical representation of industrial cybersecurity incidents from which industry can gain a realistic understanding of the risks associated with industrial cyber threats. It also gives its members reliable information support for adapting current security policies to reflect the changing dynamics of industrial cybersecurity.

ISID attempts to addresses questions such as:

- Which cybersecurity incidents are fact and which are urban myth?
- How urgent is the security risk to control systems?
- What security vulnerabilities are exploited?
- What are the threat sources?
- How serious are the consequences?

Incidents are obtained from either organisations voluntarily submitting a reporting form to ISID investigators, or from ISID staff harvesting reports from public sources such as the Internet, discussions at SCADA/industrial cybersecurity conferences, and relevant industrial publications. When an event is either submitted by an ISID member or noted in a public forum, it is reviewed and verified by the ISID researchers.

As of June 30, 2006, there are 116 incidents that have been investigated and logged in the ISID database, with 12 incidents pending investigation and entry. Of these 116 records in the database, nine with a reliability of Unknown or Unlikely and one with the reliability of Hoax/Urban Legend were excluded from analysis. An additional incident was also excluded because it had null data in the event date field and could not be used to obtain trend data. This left 105 records that were used for the analysis presented in the remainder of this report.

The changing landscape – a deceiving trend

The first question typically asked is whether or not the number of security incidents against SCADA and control systems is increasing or decreasing. To help answer this, **Fig. 1a** graphs the frequency distribution of incident event dates. There are 14 categories of years ranging from 1982, the earliest incident event date in the database, to June 2006.

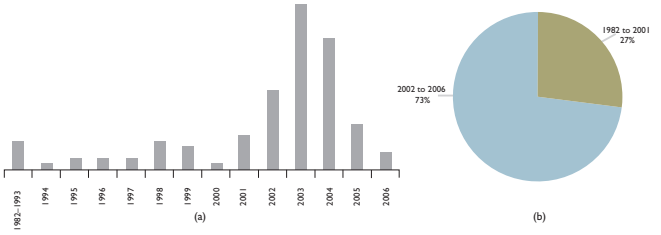

Fig. 1. Incident events by date from 1982 to June 1, 2006: (a) graphed as a frequency distribution; (b) charted as a percentage (105 records)

Clearly, cybersecurity incidents affecting control systems is not a new problem – as noted above, the earliest recorded incident occurred in 1982. However, these early incidents were sporadic, and the period of continuous annual incidents (i.e., where there is no year without a reported incident) didn't begin until 1994. The first year to see a significant increase in the frequency of cybersecurity incidents as compared ▶

to earlier years was 1998. Notice that there is a striking increase in the annual incident rate starting in late 2001. As **Fig. 1b** indicates, even though the period from 2002 to June 2006 represents less than 20% of the total time scale, it contains almost 75% of reported incidents.

While it is possible that some of this increase is due to the fact that the database was started in early 2001, we believe that the bulk of the increase is not. We have found that the event dates of incidents have a low correlation with the submission date, indicating that companies will report incidents long after they have actually occurred. Thus if more incidents had occurred prior to 2002, we would still expect to see a few of them being submitted as late as 2006. Since this is not happening, it appears that sometime between 2001 and 2002 there was a significant shift in incident occurrence rates. As we have noted in earlier papers on ISID, it appears that the time period between 2001 and 2002 marks a significant watershed for SCADA and controls security and is a natural partition for analysing trend data in more detail.

On first reading of the early indicators for 2006, it might suggest a marked decrease in the frequency of cyber attacks against the SCADA and Process Control industry as compared to the 2003/2004 period. However, based on our experience in previous years, this is unlikely to be the case: the time lag between the occurrence of an incident and when it is logged into the database (a mean delay of 13 months) is likely masking the true incident rates for 2005 and 2006. For example, at this point in 2005 only 10 incidents had been reported for 2004 and 15 for 2003; a year later that number had climbed to 23 and 29 respectively. Thus with eight incidents currently reported for 2005, we can assume that by 2007 the incident numbers for 2005 will be of the same magnitude as 2003 and 2004. **Figure 2** shows the predicted incident rates from 1994 to 2005 along with a moving average trend line.

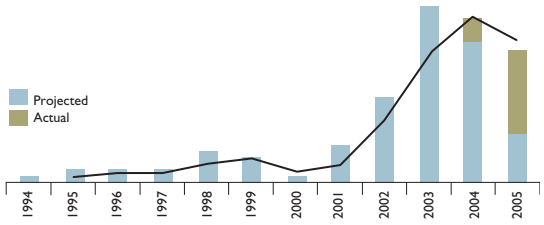

Fig. 2. Actual and predicted ISID incidents from 1994 to 2005

The good news is that while events have increased significantly since 2001, the rate appears to have levelled off in the past few years and may actually have decreased slightly in 2005/2006. It is likely that trends experienced in the critical infrastructure industries are following similar trends found in the overall IT world. According to a report written by IBM's Global Security Intelligence team, 'the global IT threat landscape is going through a fundamental shift, or evolution, in cyber crime from pervasive global outbreaks to smaller, stealthier attacks targeted at specific organisations'[2]. As IT networks are becoming increasingly more secure, it is anticipated that many of these attacks will target the most vulnerable access point within a company or organisation, which could easily be the SCADA or process control system.

Discussions with operators of traditional business crime reporting databases indicate that a typical incident database collects no better than one in ten of the actual events occurring. Twenty nine incidents were collected for 2003 and 23 for 2004, so it is likely that industry is experiencing at least 200 incidents per year at the present time. However, this number is probably several orders of magnitude low, due to the fact that of the 197 companies listed in the *Fortune 500* with significant manufacturing or critical infrastructure operations, only 14 currently report to ISID and several of these are rather sporadic in their reporting. Thus it is probable that 2000 to 3000 industrial cybersecurity incidents are occurring per year to Fortune 500 companies alone.

If this estimate is accurate, then it also indicates that even given the increasing acceptance of ISID, companies are still reluctant to provide information about security breaches. Intuitively one can expect that companies do not want disclosure of problems with their network. This is also consistent with research conducted by Katherine Campbell et al that found reports of security breaches can adversely affect a firm's stock price[3].

Finally, the companies that do report to ISID tend to be on the leading edge of industrial cybersecurity preparedness and thus are likely experiencing lower incident rates as compared to the other companies. If nothing else more quantative, these statistics indicate a continuing security incident problem, and it may be more widespread than most control systems professionals believe.

The changing threat

As we noted previously, the number of cyber incidents occurring against manufacturing systems took a significant jump in late 2001. This begs the question, 'Did the nature of these events change as well?'

To help answer this, the ISID data was analysed for incident type to get an idea of the threat sources. First, the period up to and including the year 2001 was investigated. **Figure 3a** shows the breakdown of 27 incidents between the years 1982 and 2001. Note that accidents, inappropriate employee activity, and disgruntled employees accounted for 74% of the problems, indicating that most of the threat, malicious or otherwise, was coming from within the company boundaries. These statistics correlate well with the numbers being expressed by security researchers in the IT world at the time. For example, 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.[4]

The ISID study team then produced the same graph for 78 incidents during the period 2002 to 2006, as shown in Fig. **3b**. In this time period externally generated incidents account for 60% of all events, indicating a surprising and significant change in threat source.

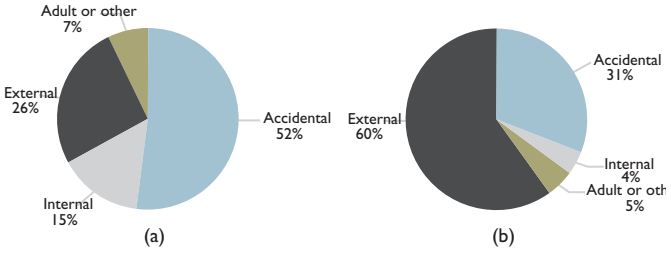

Fig. 3. (a) Incident types percentage charted as a from 1982 to 2001 (27 records); and (b) Incident types from 2002 to June 2006 (78 records)

Interestingly, the IT world appeared to experience the same shift. For example, Deloitte & Touche's 2003 *Global Security Survey*, examining 80 *Fortune 500* financial companies, found that 90% of security breaches originate from outside the company, rather than from rogue employees[5].

Although there is no definite answer as to why this dramatic change took place in late 2001, there are a few possible explanations. First, as noted earlier, control systems have historically operated in an isolated environment where control devices typically did not communicate with outside systems. The move to integrated business communications systems and the widespread use of commercial off-the-shelf (COTS) technologies like Ethernet and TCP/IP have meant this isolation has broken down, especially since 2000, when the Y2K crisis drove a massive upgrading of many systems.

The emergence of automated non-email worm attacks starting with *Code Red* on July 19, 2001, has meant that many of the intrusions have become nondirected and automated, and the control system may have become just a target of opportunity. Since control systems rarely use or allow SMTP traffic, earlier malware that used email as a vector were unlikely to penetrate the plant floor. On the other hand, protocols such as RPC and SQL are ubiquitous in control environments, allowing the worms using these vectors easy access. ▶

This second interpretation seems to be supported by a closer look at the external incidents between 2002 and 2006, of which 78% (**Fig. 4**) were the result of common viruses, Trojan horses, or worms. Particularly interesting is the fact that of these 36 malware attacks, only one (a *Sobig*-driven incident) used SMTP as its sole propagation technique. Three worms (*Slammer*, *Blaster*, and *Sasser*) accounted for over 50% of the incidents and these use the SQL Server Resolution Service (UDP Port 1443), the RPC Service (TCP Port 135) and the Microsoft-DS service (TCP port 445) respectively, to propagate to new victims.

One last item worth noting is that the majority of these worm events occurred months or years after the worm was widely known in the IT world and patches were available and proven for control systems. This indicates to us a lapse in security policy rather than technology, a point we will revisit later.

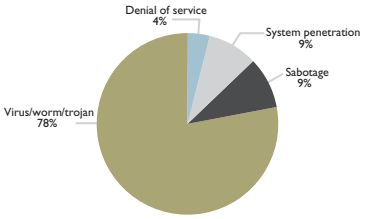

Fig. 4. The percentage total of each external incident type category, 2002 to 2006

The back door into the control system

One of the enduring beliefs held in the SCADA and control systems world is that control systems are secure because they are simply never connected to the Internet. But if this is the case, then how are all these viruses getting to the plant floor and infecting SCADA systems?

To answer this question, the study team looked more closely at the category of events reporting a remote point of entry. The data set was reduced to the 47 incidents that occurred between 2002 and 2006 and had 'Remote' in the point-of-entry field. **Figure 5** graphs the frequency distribution of each of the nine remote point-of-entry categories: Internet, corporate WAN, corporate business LAN, wireless system, trusted third party, VPN connection, public telecommunications network, and dial-up modem.

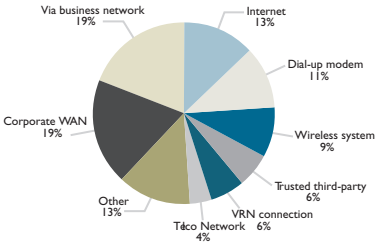

Fig. 5. Remote points of entry charted as a percentage from 2002 to 2006(47 records)

The results clearly show that while the business network (either LAN or WAN) was a major source, it was certainly not the only source. Secondary pathways such as dial-up connections, wireless systems, public telecommunications networks, VPNs, and third-party connections were all significant contributors.

While shocking to some, the large number of and variety of pathways common in automation systems is corroborated both by the keynote presentation at the 2006 Process Control Security Forum (PCSF) and a recent ARC Advisory Group survey[6]. The PCSF paper reported that at one representative large energy company, 80 to 90% of all control networks were shown to be connected to the enterprise network, which in turn, is interconnected to the Internet. In the case of the ARC survey, control engineers were asked about the types of connections that their automation networks had to the outside world. The summary results are shown to the left. Notice that the percentages in the ARC study do not add up to 100%, indicating that many automation networks had multiple connections. Both the research team's experience in conducting site security audits on control systems and the results in Fig. 6 indicate that most facilities have multiple pathways into their control system, not just one. For example, one survey in 2004 uncovered 17 different pathways, while site management believed there was only one control system to business network data historian link.

Company intranet	*47.5%*
Internet directly	*42.5%*
Direct dial-up	*35%*
wireless modems	*20%*
No connection	*17.5%*
Other connections	*8.0%*

The use of older technologies such as dial-up modems for remote support and the integration of new technologies such as VPN access, laptops, and IEEE 802.11 wireless present many pathways for attackers to gain access into the SCADA and process control networks. These include:

- Modems: Both leased-line and dial-up modems have been in use for decades to allow the remote support of control systems and are still widespread, especially on control devices that use serial communications or are located in remote locations. For example, the connection of maintenance modems to protection relays substations is a largely accepted practice throughout the North American power industry. Unfortunately, many of these modem/device pairs have been shown to have either no password or trivial passwords. Some are even so old as to not allow passwords at all.
- Wireless: There are many ways SCADA control systems companies use wireless technology. Traditionally, SCADA networks over large physical areas used licensed-band radio systems to allow remote nodes to communicate with a centralised management host. More recently, the large-scale use of 802.11 WLANs has created countless opportunities for intrusion and information theft.
- Third-party connections: Generally used for remote support by control systems vendors or product transfer by raw materials suppliers, these connections interconnect the control system to an outside network that may not follow the same security policies. Dial-up, long-haul serial, unencrypted wide area network, radio frequency, and VPN style connections are all used.
- VPNs: Often deployed as part of a third-party connection, these use encryption technologies such as SSL and IPsec to tunnel so-called secure communications across insecure networks (such as the Internet) and into the control network. Since the traffic is encrypted, it is commonly believed to be secure. VPNs do not protect the network and workstations against most data-driven attacks (i.e., viruses) when the end-nodes or networks are not also secured[7]. Additionally, such connections can often bypass firewall rules because data is received in an encrypted format and cannot be checked by the firewall.
- Mobile devices such as laptops, PDAs and Flash drives are often used in a variety of environments, each with different security policies and practices. This allows the spillover of security issues from one system to the other. For example, if laptops are used both in the plant environment and in a less secure home environment, malware obtained in one setting may be unwittingly transferred to the other.
- Internet: While commonly denied, both the ARC Study and a number of the incidents in the ISID show that control systems do get connected directly to the Internet. Reasons for this include a desire to download system patches or antivirus updates from vendor web sites, as well as a misguided desire to conduct typical office activities (such as email) from the plant floor.

Figure 6 (*over page*) illustrates a few of the locations of possible pathways into organisations that employ segregated process control/SCADA networks, and all of them have been points of entry for at least one ISID incident. For example, database records show that the *Slammer* worm had at least four different infiltration paths in the control systems it impacted:

1. The Davis-Besse nuclear power plant process computer and safety parameter display systems via a contractor's T1 line;
2. A power SCADA system via a VPN;
3. A petroleum control system via a laptop;
4. A paper machine HMI via a dial-up modem.

The bottom line is that security designs that assume all traffic into the control system will flow through a single choke point may be making a dangerous assumption. Focusing a single solution (such as the Internet firewall) on a single connection point is likely to miss many possible entry points into the control system and leave the system open to attack.

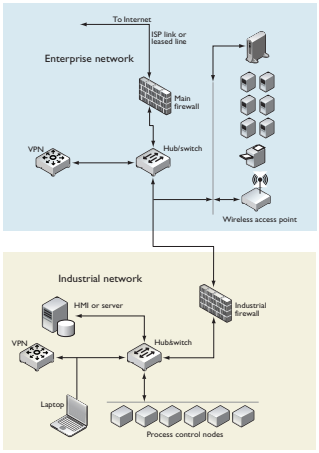

Fig. 6. Typical entry points in control network structure

Improving industrial control system security

This analysis of the ISID data indicates that organisations that operate SCADA and control systems have good reason to be concerned about cyber security. Not only have the number of incidents increased dramatically in the past five years, but the seriousness of these events appears to be increasing as well. Furthermore, the cost of each incident can be substantial. Even if there is no direct impact on production or revenue, there is cost associated with expenditure of employee time, the cost of upgrading/changing equipment, and the risk to corporate reputation.

Virus and worm-related incidents make up a significant proportion of the total number of incidents impacting control systems. They also account for a significant percentage of the overall costs incurred due to the high volume of such incidents. The high frequency of virus and worm incidents suggests that security methods that are in place in many control systems are insufficient. For example, a perimeter firewall protecting the business network offers little protection against internally released viruses from mobile laptops connected to the control network.

The analysis points to two areas where the security of the typical SCADA/PCN system could be improved significantly. First, the large number of incidents involving well known and easily addressed threat vectors indicate that many of the security issues need to be addressed through better policy, practices, and education programs rather than through pure technology based solutions. For example, incidents involving the *Slammer* worm continue to be submitted to the ISID, almost five years after the patch for this vulnerability was initially released. Flaws in security policy and employee/contractor awareness are the root cause in nearly all these cases, rather than a failure in technologies such as antivirus or firewall software.

Second, the existence of the numerous secondary pathways into the SCADA and control system point to the need for comprehensive, in-depth defence strategies. This includes better layering of firewall defences and the hardening of end-point devices through patch management, antivirus deployment, microfirewalls, and host firewalls within the SCADA/PCN proper. The remainder of this section describes both areas for improvement in more detail.

In any cyber security effort it is easy to get caught up in the razzle-dazzle of technological solutions and forget the soft aspects of security such as policy development, responsibilities, and staff training. Yet it is this human part of the equation that is critical to the success of any security program, not the technology.

Reviewing the incidents reported in the ISID, it becomes clear that the root cause of many of the events is a breakdown in these human factors rather than a true failure of technology. Thus it is critical that SCADA/control system owners and operators start by developing a comprehensive control system security management program that covers all aspects of industrial control system security, including cyber and physical security.

There are a number of excellent sources that provide guidance on how to create a control system security management system. The ISO/IEC 17799:2005 and ISO/IEC 27001:2005 standards specify a possible process from the IT perspective, while *ISA-99.00.02-Part 2: Establishing an Industrial Automation and Control System Security Program* defines the key requirements from a process control perspective. Industry-specific requirements for the electric power industry are defined in the North American Electrical Reliability Council (NERC) Standards CIP-002-1 through CIP-009-1.[8]

In addition to these formal standards are interpretive guides that help translate the language of standards into everyday terminology. A good example of this is the Symantec white paper, 'Effective Practices for Meeting NERC Critical Infrastructure Protection Requirements in the Electric Power Industry.' This paper summarises an effective security program into five key steps:

Step 1: Critical asset identification and risk assessment
Step 2: Security policy creation and update
Step 3: Disaster recovery planning
Step 4: Deployment of protective measures
Step 5: Security monitoring and management

Taking short cuts on any of these steps can be a recipe for disaster. For example, a number of incidents have occurred on sites where control system staff had moved well into Step 4 (deployment of protective measures) before completing the policy creation step. The result was that staff who did not understand the need for the security technologies on their site effectively nullified their security effectiveness by inappropriate actions. For example, during one particular site audit, network cables were discovered that circumvented the SCADA firewalls. The reason later given was that there was no risk analysis showing that the firewalls were important, nor was there a policy stating that bypassing them was unacceptable. Once again, this highlights the need for a control system security management system that is holistic and well designed, rather than a piecemeal approach to security.

The need for defence in depth

In many of our discussions with controls engineers, we hear the comment: 'We don't need to worry about securing our control system because the IT department has a firewall between the company and the Internet that will protect us.' Yet since nearly 40% of all reported incidents were transmitted from the business network to the control system, clearly this strategy isn't working.

Modern security practice mandates that effective security requires a defence in depth strategy where critical systems are protected by layers of security. Depending on a single corporate firewall for control system security violates that strategy by creating a single point of security failure. Once the attacker or worm has either broken through or circumvented the single firewall, the entire control system is left wide open to exploitation.

Furthermore, the security needs of the business network are not the same as the security needs of the control network. For example, the business firewall must typically allow users on the inside of the network to browse the Internet using HTTP, while the control system typically requires security policies that explicitly forbid this. Simply put, a single firewall cannot be all things to all departments. A good control system security strategy needs to offer layers of protection, starting with a dedicated control system firewall and progressing to specific protection for key devices and systems on the plant floor or SCADA system.

The primary control system firewall defines the security perimeter for the control system and acts as the choke point for all traffic between the outside world and the control system. Proper design and deployment of this firewall is critical: ideally, it should be deployed in the appropriate multilayer architecture described in the NISCC *Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks.* Often this is not the case; as Dorey noted in his PCSF keynote speech, comments like 'My networks aren't connected; my server uses a separate ▶

Quantifying the Cyber-Threat

The Cyber-Threat Impact Index (CTII) attempts to quantify the total impact of an incident by categorising it into one of three impact classes: low, moderate, and high. Instead of being wholly dependent on the direct financial impact, other factors such as loss of employee time, loss of hardware, environmental consequences, and health and safety issues are considered as well. Impact is then more accurately defined as the total transaction cost (or consequence) experienced by the organisation.

The table summarises the results of this categorising, and we can see that the majority of attacks can be classified as serious or moderate as defined by the CTII. The frequency of moderately severe incidents has increased steadily over the last few years. Given this, a future incident has about a 67% chance of being moderate or serious based on CTII categories averaged from 2001 to 2004.

	CTII			Percentage		
Year	Serious	Moderate	Low	Serious	Moderate	Low
2001	4	2	0	66.67%	33.33%	0.00%
2002	6	3	5	42.86%	21.43%	35.71%
2003	8	9	12	27.59%	31.03%	41.38%
2004	5	11	7	21.74%	47.83%	30.43%

network card to connect to the PCN and the corporate network' do not indicate a secure network design and are simply a great way to infect both networks. Similarly, using routers or switches with access control lists (ACL) is generally not acceptable. Detailed reasons for using proper firewalls and the basics of designing multilayer architectures are described in the NISCC Good Practice Guide.

Multifunction firewalls that combine firewall services, antivirus (A/V) services, VPN services, and intrusion detection services are also recommended. As noted previously, VPNs often bypass firewall rules because data is received in an encrypted format and cannot be validated by the firewall. Combining the firewall function and VPN function in one appliance addresses this issue because the firewall can be given the ability to decrypt (and if necessary re-encrypt) the VPN traffic.

Similarly, the challenges of deploying A/V in the control network can be partially addressed by multifunction firewalls. Systems that cannot use A/V software (such as PLCs) or systems where signature updating must be delayed can get some level of protection from a firewall that offers A/V services as well.

Once the electronic perimeter of the control system is secured, it is necessary to build the secondary layers of defence on the control system itself. This can be achieved using two primary techniques. For those control components (such as HMIs and data historians) that are based on traditional IT operating systems such as Windows and Linux, this can take advantage of the proven IT strategies of patch and antivirus management. For those devices like PLCs, RTUs, and DCS controllers, where patching or antivirus solutions are not readily available, the use of distributed security appliances is recommended. We will discuss both solutions in more detail below.

Patch and antivirus management

Hardening the control components that use common operating systems is a commonly suggested solution for improving system security. Yet with 78% of reported incidents in the last four years being malware-related, the deployment of A/V software and patch management in control systems obviously needs improvement.

The difficulty with both antivirus deployment and patch management in SCADA is that one cannot blindly deploy new A/V signatures or patches into the industrial control environment without risking disruption of operations. In fact, there have been at least two cases recorded in ISID where inappropriate deployment of A/V patches on the control system has caused loss of production.

This does not mean that the deployment of antivirus software or patches in control systems should be given up as impossible. A number of companies have demonstrated that careful A/V and patching policy and practice can be used in a balance of system reliability with the need for system security. For example, several major petroleum and chemical companies have publicly described how they successfully used antivirus technology and patch management on their control systems[10]. The Edison Electric Institute (EEI) has detailed recommendations on a tiered approach to patch management for control systems[11]. Finally, most of the major control equipment vendors now offer guidance on both patch management and A/V deployment for their control products. Thus there is little reason for SCADA system owners/operators not to have good patch and A/V programs in place today.

In many cases, the most critical devices in a control system are based on operating systems and architectures that do not allow the addition of security features such as A/V software or permit regular patching. Furthermore, the majority of control devices in use today offer no authentication, integrity, or confidentiality mechanisms, and can be completely controlled by any individual pinging the device. Thus the most critical devices on the plant floor are also the most vulnerable.

A rapidly evolving security solution is the use of low-cost security appliances deployed directly in front of each control device (or group of devices) that needs protection. These appliances provide protection directly at the critical edge device, similar to the way personal firewalls, antivirus software, or intrusion detection systems provide local protection for desktop computers and servers. The result is a true 'defence in depth' strategy, so that even if a hacker or virus manages to get through the main corporate firewall, they will still be faced with an army of SCADA-focused security devices that need to be breached before any damage can be done. Typically, each of these remote security appliances are centrally configured, monitored, and managed from a central management system. Because of their focus on protecting a small number of critical devices rather than a whole network, each appliance can be tuned to meet the security needs of the device it is protecting. ■

Abridged from the white paper *Security Incidents and Trends in the SCADA and Process Industries: A statistical review of the Industrial Security Incident Database* www.symantec.com

References

1. *We have your water supply, and printers*. Brumcon report, *The Register*, Oct 20, 2003 www.toorcon.org/2005/conference.html?id=16 www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf

2. Surge in criminal-driven cyber attacks anticipated in 2006, *IBM Global Business Security Index Report*, Dec 2005

3. Katherine Campbell, Lawrence A. Gordon, Martin P.Loeb and Lei Zhou; The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market, *Journal of Computer Security*, Vol. 11, No. 3, 2003, pp. 431-448

4. Tony Stephanou; Assessing and Exploiting the Internal Security of an Organization, *The SANS Institute*, Mar 13, 2001

5. Nash, Emma; H*ackers bigger threat than rogue staff*, VNU Publications, May 15, 2003, www.vnunet.com/News/1140907

6. Bob Mick; *Manufacturing Security Status & Strategies* ARC Advisory Group, Oct 2005

7. ISA-TR99.00.01-2004, Security Technologies for Manufacturing and Control Systems, Instrumentation, *Systems and Automation Society* (ISA), 2004

8. http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html *Effective Practices for Meeting NERC Critical Infrastructure Protection Requirements in the Electric Power Industry*," Symantec Corporation, 2006 http://www.symantec.com/enterprise/solutions/focus.jsp?solid=electric&solfid=nerc

9. Eric Byres, John Karsch, and Joel Carter, *NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks*, National Infrastructure Security Co-ordination Centre (NISCC), Jul 8, 2004.

10. Eric Cosman; Patch Management at Dow Chemical, *ARC Tenth Annual Forum on Manufacturing*, ARC Research, Feb 20-24, 2006

11. *Patch Management Strategies for the Electric Sector*, white paper, Edison Electric Institute—IT Security Working Group, March 2004