Hacking The Industrial Network

By Frank Dickman, Industrial Infrastructure Consultant

Is Your Production Line or Process Management System at Risk?

The Problem
Malicious code, a Trojan program deliberately inserted into SCADA system software, manipulated valve positions and compressor outputs to cause a massive natural gas explosion along the Trans-Siberian pipeline, according to 2005 testimony before a U.S. House of Representatives subcommittee by a Director from Sandia National Laboratories.1 According to the Washington Post, the resulting fireball yielded “the most monumental non-nuclear explosion and fire ever seen from space.”2 The explosion was subsequently estimated at the equivalent of 3 kilotons.3 (In comparison, the 9/11 explosions at the World Trade Center were roughly 0.1 kiloton.)

According to Internet blogs and reports, hackers have begun to discover that SCADA (Supervisory Control and Data Acquisition) and DCS (Distributed Control Systems) are “cool” to hack.4 The interest of hackers has increased since reports of successful attacks began to emerge after 2001. A security consultant interviewed by the in-depth news program, PBS Frontline, told them “Penetrating a SCADA system that is running a Microsoft operating system takes less than two minutes.”5 DCS, SCADA, PLCs (Programmable Logic Controllers) and other legacy control systems have been used for decades in power plants and grids, oil and gas refineries, air traffic and railroad management, pipeline pumping stations, pharmaceutical plants, chemical plants, automated food and beverage lines, industrial processes, automotive assembly lines, and water treatment plants.

Sandia National Laboratories has been chartered over the last 15 years with testing and improving the security of U.S. infrastructure control systems. When interviewed by Frontline, they confirm that their Red Team has never failed to penetrate a U.S. system using publicly available methods. When they refer to the term SCADA, they include all real-time digital control systems, process control systems and other related technologies.

The History
Introduced in the late 1960s, PLCs were designed to eliminate the higher cost of complicated, relay-based control systems. By the 1980s, Distributed Control Systems achieved popularity within increasingly automated plant environments, with keyboards and workstations replacing large, individual control cabinets. Entire production lines and processes could be linked over industrial cable/bus networks (Modbus, Profibus, Fieldbus and others) to provide monitoring and control to a

foreman's desk. Dials, gauges and idiot lights were replaced by a pictorial representation of the process with fields displaying real-time information. The available systems were "proprietary," capturing market share by staying incompatible with competitive systems. By 1998, however, customers were beginning to demand open systems, common protocols and vendor interoperability. This closely mirrors the way that computer network standardization developed, but industrial networks have been far more resistant to open system competition. They remained largely incompatible.

It is also true that any given facility, be it a public utility, process, or production line, will contain a mix of old and new technologies. There will be rudimentary systems that remain in place because they still work, and new high speed processes that reflect the latest developments in efficiency and reduced cost. The oldest systems may have been designed or installed by long-departed engineers, and the documentation on these systems may be sketchy, as will be the documentation of modifications made over time.

Ethernet

It was obvious from the beginning of the new millennium that the next logical step would be the requirement of Ethernet connectivity between the front office and the plant or processes. Ethernet triumphed as the de facto network choice for corporate administration more than a decade ago. It was only a matter of time before it migrated to the management of the factory floor.

Ethernet offers instant access to shared data for multiple departments – inventory, shipping and receiving, purchasing, accounting, production, sales, CAD/CAM engineering and process control. Standardization, real-time access and better communication across the entire enterprise are some of the driving forces. Other drivers are that Ethernet network equipment and applications are readily available, less expensive, easier to install, maintain and administrate.6

A new industrial revolution is taking place on the factory floor as corporations discover the economic benefits of integrating their Information Technology (IT) networks with legacy process control and production systems.

Moore's Law effectively predicted that processor speeds will double every 18 months. This means that new gadgets and smaller, better, faster computers have been developed with revolutionary speed. But while the IT and computer-based markets evolve rapidly, the industrial side of the end-user market is fairly slow to adapt. It is sometimes considered too expensive to do so, or too disruptive to the process or production. NASA's Space Shuttle control systems and the FAA Air Traffic Control systems are antiquated by decades because it is too expensive and disruptive to update them.

Capital equipment is intended for long-term use, and is likely to remain in use for 10–20 years, until the capital expenditure has been amortized. As a result, it is not uncommon to find that the processors used in the equipment controls may be older versions, such as Intel 486, 386, or even 286 chips, as well as older versions of operating systems. These obsolete, reduced performance processors have long

been grandfathered, and there is a lack of support for upgrades or software-based security solutions for obsolete technology. Even more critical are the security risks for older Windows operating systems such as Windows 98, because Microsoft no longer supports these versions with security updates.

It should be noted that mainstream support for Windows 2000 has expired and extended support will be dropped by July 2010. Security issues with Windows Vista are currently being reported with considerable frequency.

Similar problems exist for PCs running on the operating systems from other manufacturers. Often, older versions are no longer supported and security holes can no longer be closed through software patches. And some processes or production lines cannot easily be interrupted to install frequent patches or software upgrades. An upgrade must be tested and proven “to do no harm” before incorporated into a production line.

There are a wide range of security technologies that can be used to protect the corporate network, but these are less successful within a production network. Traditional hardware-based systems (routers, bridges) used in the corporate network have the drawback that they can always be identified based on their Internet Protocol (IP) address – and are therefore highly susceptible to attack. This is particularly due to the fact that in many systems, specific numbered ports are left open in order to ensure unproblematic data transfer via the Internet connection.7

Unfortunately, software-based solutions (personal firewalls, anti-virus software) have other limitations: namely, they cannot run on some proprietary operating systems, due to lack of compatibility. Moreover, they often can’t be integrated into systems which use older processor technology – because these lack the necessary performance.

Blocking a virus attack would demand so much of the processor’s abilities that the whole system would be paralyzed. It should be mentioned that vulnerable software constantly requires updates – otherwise viruses can easily attack the operating system time and again through newly detected security holes. Yet such updates are complex, requiring extensive resources in manpower and capital.

Figure 1 illustrates a brief chronological history of publicly reported hacking incidents that provide a chilling insight into the problems and their potential for disruption and disaster. Some of these damaging exploits were kept secret for years. Many more incidents go unreported for reasons of national security or corporate embarrassment.

Even more go undetected. Properly executed, successful hacks are undetectable and untraceable. Professional hackers, criminal organizations, terrorists and nation states can conceal their attacks by using fast-flux to bounce their actions through thousands of botnet zombie computers located in other nations. Critical industrial design information can be stolen, stored on remotely enslaved computers, and resold or ransomed back to the owner.8

	A Short Chronological List of Widely Reported Incidents of Hacking and Disruption
A	**February 2009** - The highly evasive Conficker/Downadup worm infects 12-15 million computers, creating botnets and stealing information. - BBC
B	**June 2008** - "SCADA buffer overflow flaw revealed" - "Security Hole Exposes Utilities to Internet Attack" - Associated Press
C	**May 2008** - "SCADA vulnerability discovered...control software package used by as many as one-third of the world's industrial plants." - SC Magazine
D	**March 2008** - The Hatch nuclear plant in Georgia is forced into an emergency shutdown for 2 days as a result of a software update on a single business computer.
E	**February 2008** - Retailed Chinese digital picture frames contain a virus that: blocks security, replicates, steals passwords and financial information. - SF Chronicle
F	**January 2008** - "Hackers literally turn out the lights in multiple cities after breaking into electrical utilities and demanding extortion payments." - Associated Press
G	**September 2007** - Homeland Security reveals the DOE Idaho National Engineering Lab video showing a remote destruction of a large SCADA controlled generator.
H	**September 2007** - Hackers compromised dozens of Department of Homeland Security computers, moving sensitive information to Chinese websites. - CNN
I	**July 2007** - 3Com's security division, Tipping Point, demonstrates how a SCADA system flaw can be exploited to cause a system crash.
J	**November 2007** - "Insider Charged with Hacking California Canal System" - ComputerWorld
K	**November 2007** - "Solar Sunrise" - Three teenagers penetrate US Air Force logistic systems at various Middle East support bases.
L	**August 2007** - "Hackers Take Down the Most Wired Country in Europe" for a period of two weeks. - Wired Magazine
M	**June 2006** - LiveData flaw - "Information on these (SCADA) systems can be found by a determined attacker." - US-CERT (Computer Emergency Readiness Team)
N	**January 2006** - "A panel of public utility executives speaking at the Homeland Security for Networked Industries Conference agreed that remote monitoring and control systems, particularly SCADA systems, are vulnerable to intrusion attacks and should be protected more vigilantly." - UrgentComm
O	**January 2006** - "SCADA Security & Terrorism: We're Not Crying Wolf" presentation to the Black Hat Federal 2006 Conference by Xforce Internet Security Systems.
P	**August 2005** - 175 companies including Caterpillar, General Electric, UPS attacked by Zotob worm. DaimlerChrysler idles 50,000 workers at 13 US assembly plants.
Q	**2003-2005** - "Titan Rain" - US Department of Defense, Department of Energy and corporate networks are penetrated by Chinese People's Liberation Army, downloading 10-20 terabytes of data from the Pentagon's network. The hacking went undetected for two years.
R	**August 2003** - CSX Railroad loses signaling, dispatch and other control systems throughout their 23 state rail network due to a worm virus. - InformationWeek
S	**2003** - "Cyber War" - PBS Frontline interview at Sandia National Labs reports their Red Team never fails to penetrate US utilities using common public methods.
T	**January 2003** - Ohio Davis-Besse nuclear plant safety monitoring system knocked offline for 5-hours due to the Slammer worm.
U	**January 2003** "Slammer" worm infects 300,000 computers in the first 15 minutes, interrupting 911, ATM machines and airline reservation systems. Frontline
V	**September 2001** - "Nimda" worm infects millions of computers causing billions of dollars in damage. The originator of the worm is still unknown. - Frontline
W	**July 2001** - "Code Red" worm infects 300,000 computers in a month and then launches a simultaneous botnet attack on a White House web server. - Frontline
X	**April 2000** - The Russian government announces that hackers succeeded in gaining control of the world's largest natural gas pipeline network (GAZPROM).
Y	**April 2000** - Capture of hacker who used an Australian SCADA system to dump millions of gallons of sewage into hotel grounds for 3 months beginning in January.
Z	**1998-2000** - "Moonlight Maze" - For two years, hackers had penetrated the Pentagon, NASA, the Energy Department, private universities and research labs.
AA	**1998** - A 12-year-old hacked into Arizona's Roosevelt Dam. Federal authorities said he had complete SCADA system control of the dam's massive floodgates.
BB	**1997** - "Eligible Receiver" - An exercise uses publicly available hack methods to break into the Defense Department & Joint Chief Command system in 48 hours.
CC	**1997** - A teenager hacks into NYNEX and cuts off air and ground communication to Worchester Airport (Massachusetts) for 6 hours.
	Many more incidents go unreported for reasons of national security or corporate embarrassment. Even more go undetected. Properly executed, successful hacks are undetectable and untraceable.

Figure 1: A Short Chronological List of Widely Reported Incidents of Hacking and Disruption 9

The threat comes in many forms. It does not need to be an intelligently directed attack. The non-intelligent Slammer worm covered the globe in 30 minutes, infected business and Pentagon computers in the first eight minutes, and caused $3 billion worth of damage to Wall Street.10 Amateur soviet “kiddie-scripters” brought down “the most wired country in Europe” for two weeks through denial-of-service attacks by simply using botnets located in Egypt, Vietnam and Peru.11 Attacks on electrical and pipeline networks may seize the popular imagination, but the same industrial control networks are used in the production of everything from cars to candy bars. Worms and viruses can cause damage as easily as direct hacks.

Common Objections and Rationalizations

In the 1980s, when almost everything was analog, this was largely true. But since that time, plant operators and engineers have migrated to PC-based monitoring and controls, using graphical overlays to illustrate the facility processes in real time. Engineering and management PCs also have access to the larger corporate network, as well as the Internet and Intranet. In his book “The Art of Intrusion,” expert Kevin Mittnick clearly explains how a hacker, even a neophyte, can easily gain root (administrator) access to the entire network through the corporation’s public website, from anywhere in the world.12

It is common practice to include access to Web-based services on most programmable logic controllers. According to a major manufacturer of PLCs, the majority of their products are ordered with Web services enabled. Yet their own

study indicated that only 13% of customers actually configured and used the Web services. So 87% of users left the Web servers in the PLCs active with factory default passwords, like “1111.”13

This is nicknamed “security by obscurity” and has repeatedly been shown to be a false assumption. If the weaknesses in millions of lines of “indecipherable” computer operating system code can be hacked, the rudimentary logic instruction of a Digital Control System offers few obstacles. Engineered for safety, systems are designed to perform an emergency shutdown when any or all of a string of dangerous conditions are detected by instruments. These may include high/low limits of pressure, flow, temperature, liquid level, voltage, speed, explosivity or other parameters that could lead to a condition that damages equipment or threatens personnel safety. Recognizing and identifying such logic strings or icons on a ladder diagram is simplicity itself, even if the entire process is not completely understood.

There are only 5-6 leading DCS and SCADA systems used throughout the world, and there are millions of US and foreign engineers who have been trained in their use and implementation. Any suburban library will have on its shelves a dozen technical books on the precise methods of computer hacking. Cisco publishes a respected textbook titled “Penetration Testing and Network Defense,” which can be applied to penetrate corporate systems.14 And a new textbook titled “Hacking SCADA – Industrial Network Security from the Mind of the Attacker” is being offered on the Internet.15 Most of the SCADA manufacturers are foreign owned and most of US critical infrastructure technology products are now manufactured overseas.16

Individual personal computers are pinged and probed and tested every day while they are connected to the Internet. Regardless of the quality of antivirus software installed, malware (Trojans, viruses and worms) can be inadvertently downloaded from the Internet, and these can replicate themselves on portable memory devices of all types. In 2008, it was determined that digital picture frames, imported from China and sold by major big-box retailers (Best Buy, Sam’s Club, Target, Costco) were infected with a program that disabled antivirus software and then sent passwords and financial information to servers in China.17 And the software was analyzed as being far more capable and more sophisticated than required for these simple tasks.18 Two colonels of the Chinese People’s Liberation Army (PLA) had previously published “Unrestricted Warfare,” noting the use of computer network attacks, and the PLA has since coined the term “Integrated Network Electronic Warfare.”19

Following the successful “Eligible Receiver” attack on U.S. Department of Defense networks, new computer hardware and software was installed to see if anyone was getting in without permission. Within weeks of installation they showed that thousands of attempted illegal penetrations were going on daily. One general was incensed. “Before we had these IDS (Intrusion Detection Systems), we were never attacked. Now that we got them on the network, people are attacking our nets every day thousands of times trying to get in! And some of them are getting in!” 20

No one thought that commercial passenger jets would be hijacked and

simultaneously flown into skyscrapers either. Or that a mediocre storm, Hurricane Katrina, would largely destroy New Orleans for years. Or that a sudden financial crisis would bring worldwide production to a virtual standstill.

The expense of protection is a fraction of 1% of the IT budget. With the latest generation of equipment, a network of protection can be installed, plug and play, by a handful of technicians rather than IT managers. Production need not be interrupted. A security template, chosen by IT personnel from a CD loaded onto a server will automatically configure the parameters and level of protection for whole groups of thousands of devices. While Return on Investment (ROI) is in the range of several hundred percent a year, the simplest justification is “What will we suffer if a disaster shuts us down?”

Systems at Risk	
Aerospace Industry	Medical Centers
Automation	Oil & Gas Pipelines
ATM Kiosks	Packaging Equipment
Automotive Production	Petroleum Refining
Banking Services	Pharmaceutical
Bottling Plants	Point of Sale/Vending
Chemical Plants	Printing Equipment
Defense Plants	Remote Maintenance
Distributed Control Systems	Robotic Assembly
Engineering Design Groups	Satellite Communication
Government Offices	Security
Industrial Ethernet	Telecommunications
Lottery/Gambling Equipment	Utilities/Electric/Water/Etc.

Figure 2: Applications and Systems at Risk

Industry Recommendations
The consequences of production interruption in the industrial sector are much more serious than failures within the office network. If a production line fails for several hours, it can result in a much higher cost to the company than when a PC crashes in the office.

In 2005, the Zotob worm simultaneously attacked 175 major corporations including Caterpillar, General Electric, DaimlerChrysler and United Parcel Service.21 Thirteen U.S. DaimlerChrysler plants had to be shut down, idling their assembly lines and 50,000 workers.22 What do you think that cost per hour? The worm was later determined to have originated in Turkey, and linked with a credit card fraud ring.23

Corporate firewalls provide access security against Internet attacks from the outside world. Firewalls can protect corporate networks from most external intruders. But

the most harmful programs, capable of paralyzing automation systems, are often introduced internally. Surveys reveal that roughly 40% of security incidents involved insiders.24

External service technicians and contractors may need to be given network access, and employees and visiting consultants with laptops can inadvertently (or deliberately) introduce malicious software behind the external firewall. The so-called security cordon of firewalls at border crossings between departments often does not provide adequate protection. Effective decentralized approaches - referred to as “defense-in-depth” and “endpoint security” in the literature - are required, as are corresponding systems for the security of endpoint devices. In principle, architectures with small, distributed security systems are preferred.

The latest recommendation by the ARC Advisory Group (Automation Research Corporation) and the U.S. National Laboratories chartered to protect the economic technical infrastructure is to provide “defense-in-depth” by employing a distributed architecture with multiple firewalls and/or layers of firewalls.25 Just as mainframe computing evolved into PC networks, “defense-in-depth” security protection offers greater security, flexibility and lower cost.

How much money would be lost if production is interrupted for an hour, a day, or a month? It is a simple Return on Investment equation. But establishing production network security bears a close relationship to the logic of adhering to fire codes. If production capability is lost or irreversibly damaged, the total damage to the organization and its employees is multiplied, widespread and very expensive.

The Solution

A 2006 study by industrial network planners Röwaplan AG compared the total costs of distributed versus centralized security architectures.26 In a centralized approach, production system wiring leads to high first investment costs. The concentration of data terminals in the production area is usually low, so the utilization of switch and router modules for a centralized architecture is not high enough to provide a cost-effective solution. A distributed architecture is more economical.

The ideal solution would require several unique features. It should provide distributed “defense-in-depth” as a second or third layer of protection. It should be capable of providing various levels of security. It should be easy to implement, by technicians rather than network administrators, without modification to the network’s existing configuration.

Templates for devices should be configurable for single units or very large groups from a central location. It should be available in various appliance configurations, such as industrial mount, PCI card, patch cord dongle, and hotswap blades for a rack mounted backplane. It should be applicable in various network configurations. And it should provide hardware and software-based security concepts in a single component that can be seamlessly patched between the network and the segment to be protected. No drivers or additional software should be required.

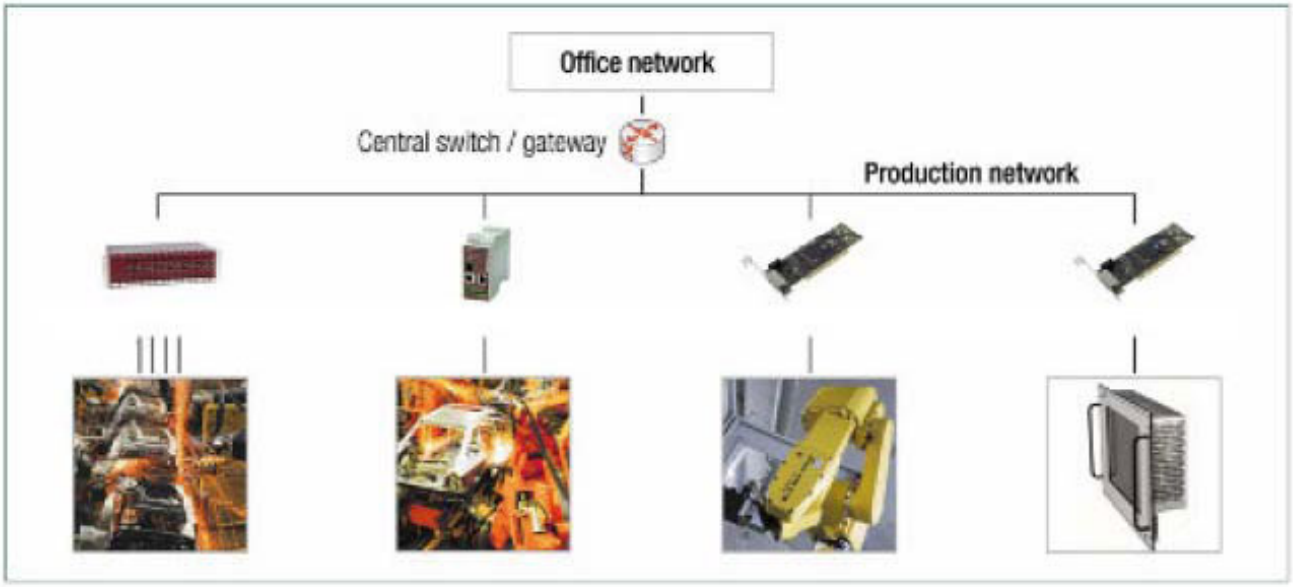

Figure 3: Various Applications and Formats Available: Rackmount, DIN mount and PCI cards

It should be capable of protecting network, broadband, ISDN or dial-up modem connections. It should provide a “Stateful Inspection Firewall” that monitors incoming and outgoing data packets based on pre defined rules offering secure and confidential communication via Virtual Private Network (VPN) tunnels. Ideally, the solution and firewall should be invisible to detection by intruders attempting to map the network. It is also much harder for worms and viruses to attack the system if they cannot see it. Network Address Translation (NAT) could be used to provideprotection by IP address masquerading.

Specific industrial solutions exist. They may be lesser known in the IT world because they exist in the industrial space, and they may be lesser known in the security world, where there is a tendency to concentrate on physical security and physical access. They are fairly known and marketed through industrial control suppliers, but there often exists a legacy misconception that the industrial network remains independent of the IT network, or that IT firewalls are sufficient. Having just one firewall as a gateway to the entire production network is insufficient protection.

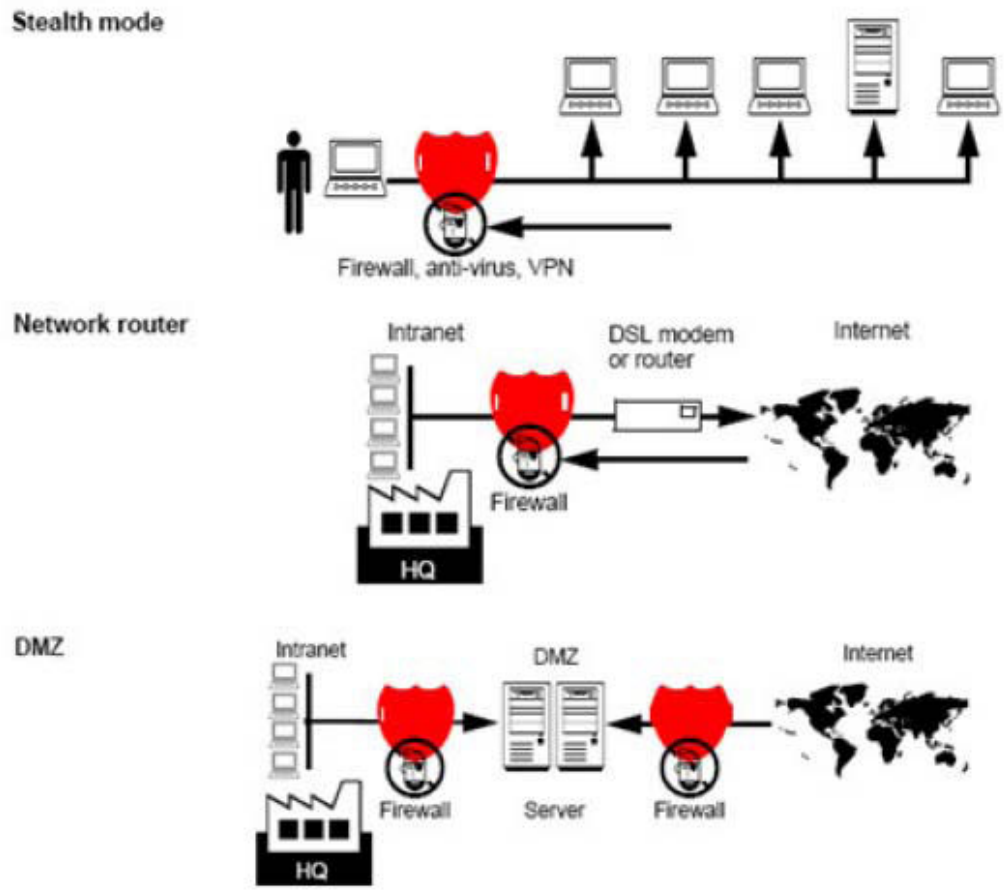

Figure 4: Various Network Configurations

Remote maintenance and diagnostics by vendor/supplier partners, for complex equipment provided by them, has become popular because it is far more economical than flying a technician halfway around the world to resolve a problem. Unfortunately, dedicated modems have previously been employed to provide access, and modems are notorious as unprotected backdoors into the network. The ideal solution would be one that denies access, even by the original manufacturer of the equipment, except when the equipment operations people request it, and when the connection is strictly authenticated, preferably via digital certificates of authority.

Some industrial-based solutions are already available. Products include Phoenix Contact FL mGuard™, Byers Tofino, Siemens Scalance, Weidmüller IE, Emerson Delta V firewall, Hirschmann Eagle mGuard™, and Innominate mGuard™. But it was only Innominate Security Technologies AG, the original developer of mGuard, that won the Frost & Sullivan “2008 Global Ethernet Security Product Value Leadership of the Year Award,” for their mGuard™ product family.27

Some of the products listed above are derived from the Innominate product set or licensed and rebranded OEM products based on earlier Innominate software releases.28 For the protection of individual production cells, the mGuard™ security devices are used in a decentralized, distributed architecture. These security appliances, a combination of hardware and software, have been designed specifically for use in industrial environments. They combine the characteristics of a

“Stateful Inspection Firewall” that offers options for encrypted, authenticated communication via VPN connections. An internationally patented “Stealth Mode” conceals the existence of the device, making it invisible to unauthorized detection via NAT IP masquerading. It offers high security for remote maintenance applications and an anti-virus engine with free updates. High availability is provided through built-in router redundancy. The excellent suitability for industrial applications lies in the fulfillment of relevant industrial standards and the ability to integrate with industrial controls, such as controllers, IPCs, Panel PCs, machinery and plant networks. It is IP 20 rated for harsh industrial environments.

Installed Innominate Security Technologies mGuard™ Systems	
Andritz	Pulp & Paper
Audi	Automotive Industry
BASF	Pharmaceutical Industry
BMW	Automotive Industry
Bosch	Packaging Technology
Daimler	Automotive Industry
Emhart Glass	Glass Forming and Inspection Machinery
Hirschmann	Automation and Control
Inmarsat	Satellite Communication
Kayser-Threde	Process Control Systems
KBA-Koenig & Bauer	Printing Machines
ND SatCom	Satellite Communication
Dr. Neuhaus Telekom	Telecommunications/Telemetry
Novartis	Pharmaceutical Industry
Phoenix Contact	Industrial Automation Technology
Scottish & Southern	Gas & Electric Transmission
Thales Raytheon Systems	Defense & Telecommunication Systems
Trumpf	Machine Tools/Laser Systems
Volkswagen	Automotive Industry

Figure 5: A remote services unit for DIN rail mounting with integrated analog modem or ISDN terminal adapter

Users are often concerned about the costs of design, configuration and maintenance of the network components. But the cost is not linear and decreases as the number of security devices rises, provided there is a central device management solution. Such a software-based Innominate Device Manager™ provides sophisticated templates, automated hierarchy, and an integrated Certificate Authority to produce VPN certificates with a high degree of automation in the configuration and updating of individual devices.

Thus, with a push-pull mechanism, a central management console supplies needed information to the decentralized components.

Figure 6 illustrates a variety of application points within the zones of a typical office/factory network. Physically different versions of the product are incorporated as required. In a telecommunications room, a backplane mounted in a 19” frame can effectively handle multiple paths from a single location. Multiple PCs, such as in an engineering group, can be protected with a slimline, rackmount unit. Individual

PCs can be protected with PCI cards. HMI (Human Machine Interface) stations on the factory floor can be protected by modules that can be DIN rail mounted into NEMA cabinets. And portable dongle-style patchcord units can be used by remote technicians, engineers and consultants whenever they access the Internet or the network.

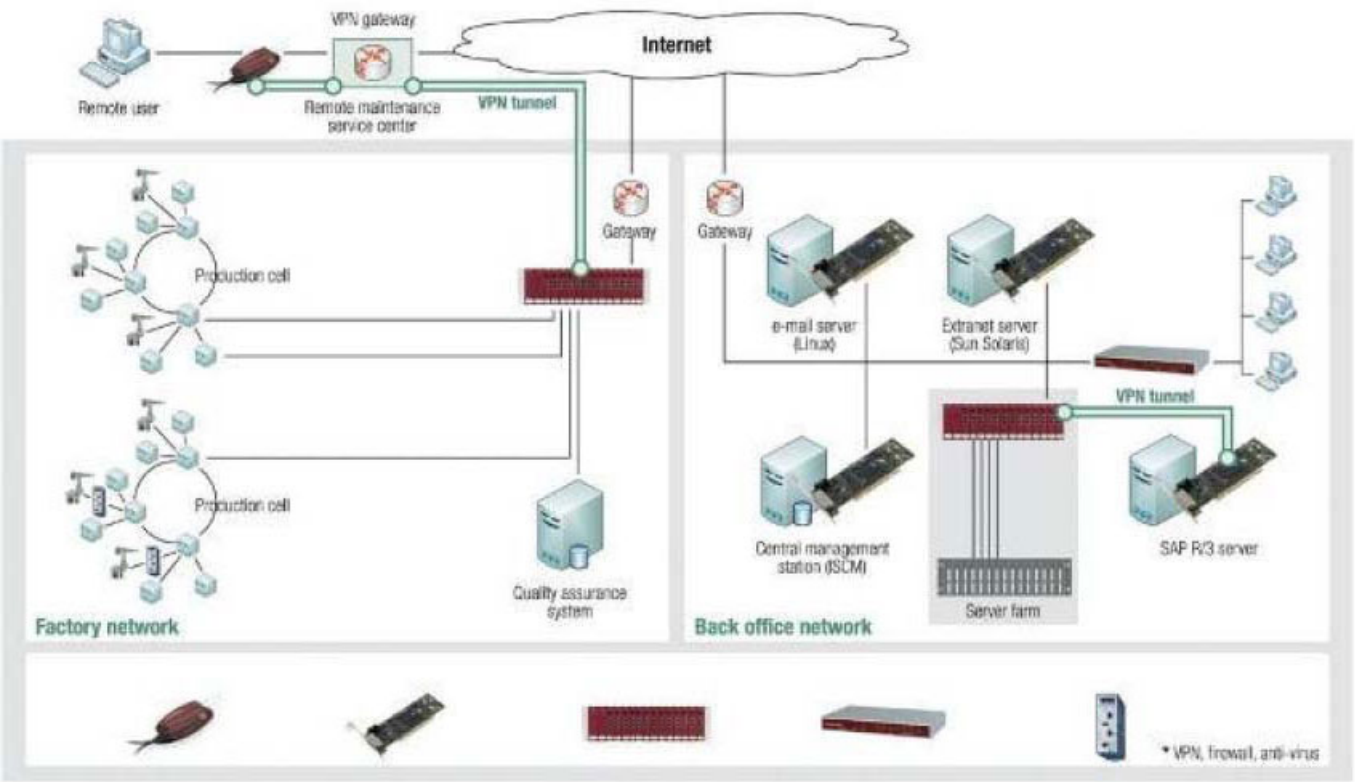

Figure 6: An Integrated Network Solution

Now that inexpensive solutions are available, the security of industrial networks can no longer be ignored. With threats to industrial networks increasing in complexity and scope, decision makers need to take action before it is too late.

Frank Dickman, BSMAE, RCDD, is a widely experienced engineering consultant and former delegate to NEMA, TIA/EIA, ISO, CENELEC and the BICSI Codes & Standards Committees. He is a technical consultant to a number of leading data communications firms and is a recognized expert on U.S. and International physical infrastructure network standards. Beyond telecommunications, his experience includes consulting engineering work for petroleum refineries, chemical plants, conventional and nuclear power plants, auto manufacturers and the aerospace industry. He can be reached at frankdickman@yahoo.com *[1].*

Endnotes and Sources

1. “SCADA Systems and the Terrorist Threat,” Joint Hearing, House of Representatives, One Hundred Ninth Congress, First Session, October 18, 2005, testimony of Dr. Samuel G. Varnado, Director, Sandia National Laboratories, pgs.18-23, available at www.fas.org/irp/congress/2005_hr/scada.pdf [2]

2. Hoffman, David E., “CIA Slipped Bugs to Soviets,” Washington Post, 2/26/2004, available at www.msnbc.msn.com/id/4394002 [3]
3. Larsen, Jason, “Breakage,” SCADA Security Presentation to the Black Hat 2008 Conference, Washington DC, available at www.blackhat.com/presentations/bh-dc-08/Larsen/Presentation/bh-dc-08-larsen.pdf [4]
4. Lewis, Dave, “SCADA Vulnerabilities,” hacking blog on SCADA Security, available at www.liquidmatrix.org/blog/2007/08/15/scada-vulnerabilites/ [5]
5. “Cyber War!,” PBS Frontline, WGBH Boston, available at www.pbs.org/wgbh/pages/frontline/shows/cyberwar [6]
6. Gould, Larry, “Industrial Ethernet: Wiring the Enterprise,” Automotive Design & Production, Gardner Publications, 2003, www.autofieldguide.com [7]
7. See Supplemental Footnotes and Sources for a list of commonly known ports likely to be left open by firewalls and exploited.
8. Knight, Gavin, “Cybercrime is in a State of Flux,” Guardian News, 3/29/2008, available at www.crimeresearch.org/articles/cybercrime0308/ [8]
9. See Supplemental Footnotes and Sources for line-by-line list of 29 footnotes.
10. “Cyber War!,” PBS Frontline, WGBH Boston, 2004, available at www.pbs.org/wgbh/pages/frontline/shows/cyberwar [6] and Clarke, Richard A., “Your Government Failed You,” HarperCollins, 2008, ISBN-978-0-06-147462-0.
11. Davis, Joshua, “Hackers Take Down the Most Wired Country in Europe,” Wired Magazine, 8/21/07, available at www.wired.com/print/politics/security/magazine/15-09/ff_estonia [9]
12. Mitnick, Kevin D. and Simon, William, “The Art of Intrusion,” Wiley Publishing, 2005, ISBN-0-7645 6959-7, particularly Chapters 8 & 9.
13. Turk, Robert J., “Cyber Incidents Involving Control Systems,” Idaho National Laboratory, October 2005, available at www.inl.gov/technicalpublications/Documents/3480144.pdf [10]
14. Whitaker, Andrew and Newman, Daniel, “Penetration Testing and Network Defense,” Cisco Press, 2005, ISBN-10: 1-58705-208-3.
15. Bodungen, Clint, Whitney, Jeff and Speake, Graham, “Hacking SCADA – Industrial Network Security from the Mind of the Attacker,” 2009, available at www.hackingscada.com [11]
16. “SCADA Systems and the Terrorist Threat,” Joint Hearing, House of Representatives, One Hundred Ninth Congress, First Session, October 18, 2005, testimony of Dr. Samuel G. Varnado, Director, Sandia National Laboratories, pgs.18-23, available at www.fas.org/irp/congress/2005_hr/scada.pdf [2]
17. Clarke, Richard A., “Your Government Failed You,” HarperCollins, 2008, ISBN-978-0-06-147462-0, pgs. 312, 315.
18. Gage, Deborah, “Virus from China: the Gift that Keeps on Giving,” San Francisco Chronicle, 2/15/2008, available at www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/02/15/BU47V0VOH.DTL [12]
19. Liang, Qiao and Xiangsui, Wang, “Unrestricted Warfare (Chaoxianzhan)” Pan American, 1999, ISBN-0971680728, available at www.terrorism.com/documents/TRC-Analysis/unrestricted.pdf [13]
20. Clarke, Richard A., “Your Government Failed You,” HarperCollins, 2008, ISBN-978-0-06-147462-0, pg. 292.

21. Keizer, Gregg, “Bots Break into 175 Companies in Year’s Biggest Attack,” Network Computing, 8/18/2005, available at www.networkcomputing.com/channels/networkinfrastructure/169300402 [14]
22. Ibid.
23. “Zotob Worm Linked to Credit Card Fraud Ring,” Michigan Technology News, 8/31/2005, available at www.mitechnews.com/articles.asp?Id=4454&sec=102 [15]
24. Richardson, Robert, “CSI Survey 2007: The 12th Annual Computer Crime and Security Survey,” Computer Security Institute, available at www.GoCSI.com [16] and “2005 FBI Computer Crime Survey,” Federal Bureau of Investigation, available at www.fbi.gov/publications/ccs2005.pdf [17]
25. Kuipers, David and Fabro, Mark, “Control Systems Cyber Security: Defense in Depth Strategies,” Idaho National Laboratory, May 2006, available at www.inl.gov/technicalpublications/Documents/3375141.pdf [18]
26. Röwaplan AG at http://www.roewaplan.com/ [19]
27. Frost & Sullivan “2008 Global Ethernet Security Product Value Leadership of the Year Award,” available at http://www.innominate.com/content/view/289/120/lang,en/ [20]
28. Bond, Andrew, “Vendors Seek Security Behind Berlin Firewall,” Industrial Automation Insider, Vol 11, No.8, August 2007, pgs. 3-4, available at www.controlglobal.com/articles/2007/270.html?page=2 [21]

Supplemental Footnotes and Sources

Footnote 7. Commonly known virtual ports that are likely left open by firewalls and exploited are: Port 21 (FTP), Port 23 (Telnet), Port 25 (SMTP), Port 53 (DNS), Port 80 (HTTP), Ports 139 and 445 (NetBIOS) and Port 1723 (Microsoft VPN), but even higher ports can be mapped by hackers using a standard Nmap program. (See www.wikipedia.com [22] for definitions of these protocols.)

Footnote 9. (See Figure 1: A Short Chronological List of Widely Reported Incidents of Hacking & Disruption)

A. Shiels, Maggie, “Microsoft Bounty for Worm Creator,” BBC News, 2/13/2009, available at http://news.bbc.co.uk/2/hi/technology/7887577.stm [23] and http://en.wikipedia.org/wiki/Conficker [24]

B. Kaplan, Dan, “ New SCADA Buffer Overflow Flaw Revealed,” SC Magazine, 6/11/2008, available at www.scmagazineus.com/New-SCADA-buffer-overflow-flaw-revealed/article/111... [25] and Robertson, Jordan, “Security Hole Exposes Utilities to Internet Attack,” Associated Press, 6/11/2008, available at http://apnews.myway.com/article/20080611/D917P7301.html [26]

C. Kaplan, Dan, “Rare SCADA Vulnerability Discovered,” SC Magazine, 5/8/2008, available at www.scmagazineus.com/Rare-SCADA-vulnerability-discovered/article/109956/ [27]

D. Krebs, Brian, “Cyber Incident Blamed for Nuclear Power Plant Shutdown,” Washington Post, 6/5/2008, available at www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958_pf.html [28]

E. Gage, Deborah, “Virus from China: the Gift that Keeps on Giving,” San Francisco Chronicle, 2/15/2008, available at www.sfgate.com/cgi-

bin/article.cgi?f=/c/a/2008/02/15/BU47V0VOH.DTL [12]
F. Bridis, Ted, “CIA: Hackers Demanding Cash Disrupted Power,” Associated Press, 1/18/2008, available at www.msnbc.msn.com/id/22734229/ [29]
G. “Sources: Staged Cyber Attack Reveals Vulnerability in Power Grids,” CNN, 9/26/2007, available at www.cnn.com/2007/US/09/26/power.at.risk/ [30] with video of the generator destruction at www.cnn.com/2007/US/09/26/power.at.risk/index.html#cnnSTCVideo [31]
H. “Investigators: Homeland Security Computers Hacked,” CNN, 9/24/07, available at www.cnn.com/2007/US/09/24/homelandsecurity.computers/index.html?eref=rss_topstories [32]
I. Lewis, Dave, “SCADA Vulnerabilities,” blog on SCADA Security, available at www.liquidmatrix.org/blog/2007/08/15/scada-vulnerabilites/ [5]
J. McMillan, Robert, “Insider Charged with Hacking California Canal System,” Computer World, 11/29/2007, available at www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9050098&source=NLTSEC&nlid=38 [33]
K. Clarke, Richard A., “Your Government Failed You,” HarperCollins, 2008, ISBN-978-0-06-147462-0, pg. 293.
L. Davis, Joshua, “Hackers Take Down the Most Wired Country in Europe,” Wired Magazine, 8/21/07, available at www.wired.com/print/politics/security/magazine/15-09/ff_estonia [9]
M. Lemos, Robert, “SCADA Industry Debates Plan Disclosure,” Security Focus, 6/16/2006, available at www.securityfocus.com/print/news/11396 [34]
N. Bischoff, Glenn, “Panel: SCADA Systems at Risk for Intrusion Attack,” UrgentComm, 1/11/2006, available at www.urgentcomm.com/news/scada_attack_hsni_011106/ [35]
O. Maynor, David and Graham, Robert, “SCADA Security and Terrorism: We’re not Crying Wolf,” Presentation to the Black at Federal 2006 Conference, Washington DC, 1/23-26/2006, available at www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf [36]
P. Keizer, Gregg, “Bots Break into 175 Companies in Year’s Biggest Attack,” Network Computing, 8/18/2005, available at www.networkcomputing.com/channels/networkinfrastructure/169300402 [14] and Roberts, Paul F.,“Zotob, PnP Worms Slam 13 Daimler Chrysler Plants,” eWeek, 8/18/2005, available at www.eweek.com/c/a/Security/Zotob-PnP-Worms-Slam-13-DaimlerChrysler-Plants/ [37]
Q. Thornburgh, Nathan, “Inside the Chinese Hack Attack,” Time Magazine, 8/25/2005, available at www.time.com/time/nation/article/0,8599,1098371,00.html [38] and Shannon, Elaine, “The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them),” Time Magazine, 8/29/2005, available at www.time.com/time/magazine/article/0,9171,1098961,00.html [39]
R. Niland, Marty, “Computer Virus Brings Down Train Signals,” Information Week, 8/20/03, available at www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=13100807 [40]
S. “Cyber War!,” PBS Frontline, WGBH Boston, 2004, available at www.pbs.org/wgbh/pages/frontline/shows/cyberwar [6]

T. Poulsen, Kevin, “Slammer Worm Crashed Ohio Nuke Plant Network,” Security Focus, 8/19/2003, available at www.securityfocus.com/news/6767 [41]
U. “Cyber War!,” PBS Frontline, WGBH Boston, 2004, available at www.pbs.org/wgbh/pages/frontline/shows/cyberwar [6]
V. Ibid.
W. Ibid.
X. “Hackers Hit Russia Gas Company,” Associated Press, 4/26/2000, available at www.asmconsortium.com/asm/asm_imps.nsf/932d013f4e59531707256b1f005fa9bb/07256aed005eb4ca862569820076733f!OpenDocument [42]
Y. Crawford, Michael, “Utility Hack Led to Security Overhaul,” Computer World Australia, 2/16/2006, available at www.computerworld.com/securitytopics/security/story/0,10801,108735,00.html [43]
Z. Clarke, Richard A., “Your Government Failed You,” HarperCollins, 2008, ISBN-978-0-06-147462-0, pg. 293.
AA. Gellman, Barton, “Cyber-Attacks by Al Qaeda Feared,” Washington Post, 6/22/2002, available at www.washingtonpost.com/wp-dyn/content/article/2006/06/12/AR2006061200711.html [44]
BB. Clarke, Richard A., “Your Government Failed You,” HarperCollins, 2008, ISBN-978-0-06-147462-0, pg. 292 and “Cyber War!,” PBS Frontline, WGBH Boston, 2004, available at www.pbs.org/wgbh/pages/frontline/shows/cyberwar [6]
CC. “Juvenile Computer Hacker Cuts Off FAA Tower at Regional Airport,” Press Release, US Department of Justice, 3/18/1998, available at www.usdoj.gov/criminal/cybercrime/juvenilepld.htm [45]

Other Sources

Harris, Shon et al, “Gray Hat Hacking – The Ethical Hacker’s Handbook,” 2nd Edition, McGraw Hill, 2008, ISBN-978-0-07-149568-4.
Nash, Troy, “Backdoors and Holes in Network Perimeters: A Case Study for Improving Your Control System Security,” US-CERT, Lawrence Livermore Labs, August 2005, available at www.USCERT.gov/control_systems/pdf/backdoor0503.pdf [46]
“2008 Information Security Breaches Survey,” BERR – Department for Business Enterprise and Regulatory Reform (UK), April 2008, available at www.berr.gov.uk/files/file45714.pdf [47]

Source URL (retrieved on *12/10/2013 - 1:08am*):
http://www.chem.info/news/2009/09/hacking-industrial-network

Links:
[1] mailto:frankdickman@yahoo.com
[2] http://www.fas.org/irp/congress/2005_hr/scada.pdf

[3] http://www.msnbc.msn.com/id/4394002
[4] http://www.blackhat.com/presentations/bh-dc-08/Larsen/Presentation/bh-dc-08-larsen.pdf
[5] http://www.liquidmatrix.org/blog/2007/08/15/scada-vulnerabilites/
[6] http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar
[7] http://www.autofieldguide.com/
[8] http://www.crimeresearch.org/articles/cybercrime0308/
[9] http://www.wired.com/print/politics/security/magazine/15-09/ff_estonia
[10] http://www.inl.gov/technicalpublications/Documents/3480144.pdf
[11] http://www.hackingscada.com
[12] http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/02/15/BU47V0VOH.DTL
[13] http://www.terrorism.com/documents/TRC-Analysis/unrestricted.pdf
[14] http://www.networkcomputing.com/channels/networkinfrastructure/169300402
[15] http://www.mitechnews.com/articles.asp?Id=4454&sec=102
[16] http://www.GoCSI.com
[17] http://www.fbi.gov/publications/ccs2005.pdf
[18] http://www.inl.gov/technicalpublications/Documents/3375141.pdf
[19] http://www.roewaplan.com/
[20] http://www.innominate.com/content/view/289/120/lang,en/
[21] http://www.controlglobal.com/articles/2007/270.html?page=2
[22] http://www.wikipedia.com/
[23] http://news.bbc.co.uk/2/hi/technology/7887577.stm
[24] http://en.wikipedia.org/wiki/Conficker
[25] http://www.scmagazineus.com/New-SCADA-buffer-overflow-flaw-revealed/article/111191/
[26] http://apnews.myway.com/article/20080611/D917P7301.html
[27] http://www.scmagazineus.com/Rare-SCADA-vulnerability-discovered/article/109956/
[28] http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958_pf.html
[29] http://www.msnbc.msn.com/id/22734229/
[30] http://www.cnn.com/2007/US/09/26/power.at.risk/
[31] http://www.cnn.com/2007/US/09/26/power.at.risk/index.html#cnnSTCVideo
[32] http://www.cnn.com/2007/US/09/24/homelandsecurity.computers/index.html?eref=rss_topstories
[33] http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9050098&source=NLTSEC&nlid=38
[34] http://www.securityfocus.com/print/news/11396
[35] http://www.urgentcomm.com/news/scada_attack_hsni_011106/
[36] http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf
[37] http://www.eweek.com/c/a/Security/Zotob-PnP-Worms-Slam-13-DaimlerChrysler-Plants/
[38] http://www.time.com/time/nation/article/0,8599,1098371,00.html
[39] http://www.time.com/time/magazine/article/0,9171,1098961,00.html
[40] http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=13100807
[41] http://www.securityfocus.com/news/6767
[42] http://www.asmconsortium.com/asm/asm_imps.nsf/932d013f4e59531707256b

1f005fa9bb/07256aed005eb4ca862569820076733f!OpenDocument
[43] http://www.computerworld.com/securitytopics/security/story/0,10801,108735,00.html
[44] http://www.washingtonpost.com/wp-dyn/content/article/2006/06/12/AR2006061200711.html
[45] http://www.usdoj.gov/criminal/cybercrime/juvenilepld.htm
[46] http://www.uscert.gov/control_systems/pdf/backdoor0503.pdf
[47] http://www.berr.gov.uk/files/file45714.pdf