

# INDUSTRIAL CYBERSECURITY FOR POWER SYSTEM AND SCADA NETWORKS

Copyright Material IEEE  
Paper No. PCIC-2005-DV45

A. Creery, P.Eng. P.E.  
Member IEEE  
Universal Dynamics Ltd.  
100-13700 International Place  
Richmond, BC V6V 2X8 Canada  
acreery@udl.com

E. J. Byres, P.Eng.  
Senior Member IEEE  
BC Institute of Technology (BCIT)  
3700 Willingdon Avenue  
Burnaby, BC V5G 3H2 Canada  
eric\_byres@bcit.ca

**Abstract** – Many automation and modernization programs are now employing intranet/internet technologies in industrial control strategies. The ensuing systems are a mixture of state-of-the-art and legacy installations and create challenges in the implementation and enforcement of security measures. Control system intrusions can cause environmental damage, safety risks, poor quality and lost production.

This paper presents methods to determine and reduce the vulnerability of networked control systems to unintended and malicious intrusions. The procedure for conducting a thorough assessment of the process control networks to evaluate these risks is presented. Security issues are identified, as are technical and procedural countermeasures to mitigate these risks. Examples are drawn from past assessments and incidents. Once complete, the assessment results allow the network designer to plan infrastructure expansion with confidence in the security and reliability of the network's operation.

*Index Terms* - industrial networked control systems, network security, Ethernet communications, vulnerability assessment, secure network architecture, remote access, control system security, cybersecurity.

## I. INTRODUCTION

The use of interconnected microprocessors in industrial systems has grown exponentially over the past decade. Deployed for process control in Programmable Logic Controllers (PLC) and Distributed Control Systems (DCS) for many years, they have now moved into Intelligent Electronic Devices (IED) in applications such as substations, Motor Control Centers (MCC), and heat trace systems. The concern is that their connecting networks have grown as well, usually without much attention to the security ramifications. Intrusions, intentional and unintentional, can cause safety, environmental, production and quality problems. This paper looks at the process of assessing the current security situation, dealing with existing problems and planning for future network growth.

This security problem has been present for many years, but only recently have organizations been raising the engineering communities' awareness of it. A few standards and recommended practices exist, such as American Petroleum Institute (API) Standard 1164 [1], but

most are either unheard of or routinely ignored. In order to come to grips with this dilemma, the plant engineers must first understand the basics of the problem and then, with the facts in hand, assess and harden their existing networks. As new equipment is deployed, the security criteria must be kept firmly in mind.

## II. HISTORY

The Information Technology (IT) world has been dealing with the security problem for approximately two decades. Many organizations have been involved with this issue, from the U.S. National Institute of Standards and Technology (NIST), who published "Introduction to Computer Security: The NIST Handbook" [2], over 10 years ago, to the Internet Engineering task Force (IETF) who has created documents such as "RCF 2196 - Site Security Handbook" [3].

"British Standard 7799" [4], first published in February 1995, is a code of practice for information security management and a specification for an Information Security Management System (ISMS). BSI 7799 has become ISO/IEC 17799 [5], a standard code of practice, and a comprehensive catalogue of security practices.

In the industrial sector, work on IEEE "Standard 1402-2000: IEEE Guide for Electric Power Substation Physical and Electronic Security" first began in 1996 and the standard was approved in January 2000. Various methods and techniques to mitigate human intrusions upon electric power supply substations are presented in this guide [6]. As noted earlier, in the oil and gas sector, the API published "Standard 1164" September 2004 to address pipeline security issues for "Supervisory Control and Data Acquisition" (SCADA) systems.

"ISA-TR99.00.01-2004, Security Technologies for Manufacturing and Control Systems" [7], provides an overview of the types of electronic security technologies currently available to the Manufacturing and Control Systems environment. Its companion "ISA-TR99.00.02, Integrating Electronic Security into the Manufacturing and Control Systems Environment" [8] provides a framework for developing an electronic security program and provides a recommended organization and structure for the security plan.

Despite the ongoing work by these organizations, hybrid networks continue to form in the industrialized world. An examination of technical papers describing distributed networks, remote monitoring, “smart” motor control centers, automation and integration of substations reveals little, if any, discussion of security as a design criterion.

### III. NETWORKING BASICS

Power engineers deal daily with PLCs, wireless LANs, IEDs, power meters, protection relays and digitally controlled MCCs. These devices rely on networks to convey information and exchange commands.

Networking these devices together was traditionally accomplished through proprietary technologies. This made it difficult to connect to the network and created a natural impediment to electronic intrusion. However, today the connection of devices using Ethernet technology is increasingly being adopted. Consequently, interfacing of industrial equipment is much easier, but there is now significantly less isolation and natural security protection.

In order to understand the threats inherent in networking these computer systems, an awareness of networking basics is required. Communications over Ethernet use TCP/IP to identify nodes and ports to identify processes running on these nodes. Company networks, or intranets, are strung together using hubs, switches and routers. An example of this is shown in Fig. 1. User rights on these networked devices are either defined at the local computer or established in the “Domain”. Furthermore, intranets can be expanded by connecting to other intranets over the Internet using Virtual Private Networks (VPN). In this way, the network grows.

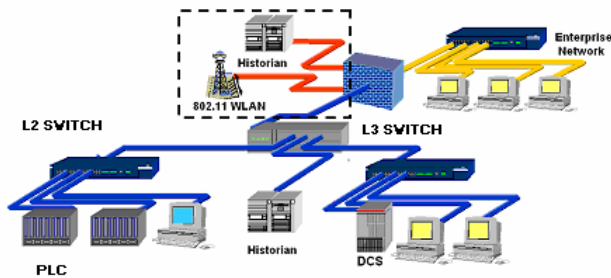


Fig. 1 Typical Hybrid Network

#### A. Networking Definitions

1) *TCP/IP*: Transmission Control Protocol/Internet Protocol is the basic communication language, or protocol, of the Internet. It is the set of rules that defines how computers route messages and exchange information. TCP/IP was originally designed for the UNIX operating system, but is now used in virtually every major computer operating system. *The main design goal of TCP/IP was to build an interconnection of networks, referred to as an internetwork, or internet, that provided universal communication services over heterogeneous physical networks* [9].

2) *Ports*: Applications running on computers will open connections to other computers using the concept of “ports”. The port number identifies a particular TCP/IP service to connect to. When a TCP/IP packet is received, the computer inspects the port number and uses this information to send the data to the correct application. The well-known ports range from 0 through 1023 and cover popular applications such as Hypertext Transfer Protocol (HTTP) on port 80. The registered ports are numbered from 1024 through 49151. The remaining ports, referred to as dynamic ports or private ports, are numbered from 49152 through 65535.

3) *Intranet*: An Intranet is an internet technology based computer network, closed to outsiders, that an organization uses for its own internal purposes.

4) *Hub*: A “Hub” is a multiport repeater used to connect multiple computers; signals received on any port are immediately retransmitted to all other ports of the hub.

5) *Switch*: A switch is a networking device that only transmits on the ports where the intended recipient of the data is located. By delivering messages only to the connected device that it was intended for (by keeping track of Media Access Control (MAC) addresses), network switches conserve network bandwidth and offer generally better performance and security than hubs.

6) *Router*: A router is a device that interconnects networks. It forwards or drops information based on the IP addressing present in the message.

7) *Firewall*: Firewalls are barriers between different networks and their associated devices that prevent unauthorized access to information resources.

8) *SNMP*: Simple Network Management Protocol is a standard that defines methods for remotely managing active network components such as switches and routers.

9) *VPN*: A “Virtual Private Network” (VPN) is a network where geographically removed networks are joined together via the Internet. Information sent across the Internet is encrypted. The resulting “virtual network” allows users to privately share information over the Internet. The use of these external resources makes the VPN an economical wide area networking option.

10) *Domain*: A domain looks after the assignment of user rights in distributed computing. Instead of maintaining separate copies of password and group files on each individual computer, the domain structure allows all domain members to “trust” the domain controller’s version of the password and group files.

Now armed with a rudimentary understanding of these networking basics, we will look at the industrial power and control systems and see how the issues surrounding this technology can place industrial control systems in jeopardy.

### IV. THE THREAT – ACTUAL INCIDENTS

The process equipment is controlled by devices such as PLCs, DCs and RTUs. These are typically monitored and controlled by Human Machine Interfaces (HMI). The majority of the HMI machines use common commercial operating systems. They are networked together to allow sharing of data. This data is gathered by maintenance and process groups and then transmitted to management

groups. The ability to do this has grown rapidly over the last few years. This has resulted in legacy network equipment being connected to state-of-the-art equipment, forming hybrid networks.

Most Personal computers (PC) can be “hacked” into using readily available tools that identify vulnerable programs running on the target PC. An open port is one that has a listening application running on the machine. An example of this is a service called “NetBIOS”, or Network Basic Input Output System. It is an Application Programming Interface (API) that allows client software access to LAN resources. NetBIOS can be used to either tie up (Denial of Service or DoS) or access a computer’s resources.

The British Columbia Institute of Technology (BCIT) is one of a few groups to track industrial cybersecurity incidents. The BCIT Industrial security Incident Database (ISID) contains information regarding security related attacks on process control and industrial networked systems. The information stored; nature of attack, technology employed and equipment used, can help companies set up protection for their networks. A typical data entry screen is shown in Fig. 2.

Fig. 2 Typical ISID Security Incident Entry Screen

The majority of industrial incidents prior to 2001 came from internal attacks, while after 2001 outside sources have become the most common attack vector. This swing has been attributed to increased use of common operating systems and applications, larger connected networks and automated “worm” attacks. Of those incidents where a financial impact was estimated, over half of them (7 in total) were greater than \$1M [10].

A common experience on the plant floor occurs when a “virus” or “worm” spreads between the networked control computers, reducing communications to a point where the operators no longer have control over the running equipment. For example, the North American Electric Reliability Council (NERC) has a report that shows the Slammer worm had a significant impact on some utilities. For example, “The worm migrated through a VPN connection to a company’s corporate network until it finally reached the critical supervisory control and data acquisition (SCADA) network. It infected a server on the control-center LAN that was running MS-SQL. The worm traffic blocked SCADA traffic.” [11]

According to an article in an industry magazine, publicly disclosed details of SCADA attacks in the chemical industry are scarce, but not unheard of. An intrusion into the SCADA systems of a global chemical company reportedly occurred where a “... disgruntled former employee was allegedly trying to disable the plant’s conveyor control, material storage, and chemical operating systems but was caught by a programmer happening to notice unusual activity.” [12]

At the ISA Expo in October 2004, attendees witnessed the compromising of a running PLC program. The PLC was set up to run a series of blinking lights. Using a network scanning tool downloaded from the internet, the speed and direction of the lights could be affected. As a final maneuver, the PLC was shut down altogether.

Control systems are typically vulnerable as installed. Unfortunately, it is usually only after an upset that steps are taken to secure these systems. This is regrettable as standards and guidelines are available to help stop the problems before they occur. Ultimately, security policies will be defined and understood and the network itself will receive the proper attention it deserves in the design phase. Until this time, and to deal with the many installed, vulnerable networked systems, a process of assessment and remediation must be followed.

## V. ASSESSMENT

While outside consultants with specialized knowledge of industrial networking equipment and control devices can be retained to perform the assessment, a certain measure of success can be achieved using internal resources. A good example of the effectiveness of self-assessments was demonstrated at a major oil company [13].

The IT staff created an in-depth quiz that allowed process engineers to assess the security of the control systems for which they were responsible. The assessment tool asked questions regarding the equipment deployed and its configuration. It then rated the security of the system in a number of areas, such as physical security, remote access management and password policy, and explained the reasons for the rating. Finally, it would make suggestions on how an individual might improve his score.

To reassure staff taking the test, the tests were carried out on the participants’ local computers and none of the assessment information was fed back to the IT department. However, the IT department subsequently received numerous requests for assistance in improving security from the control engineers, something that had rarely occurred in the past.

Whether performed by internal or external forces, an assessment will be more complete if founded on a strong, established methodology. An example is the one presented in the ISA’s “Technical Report ISA-TR99.00.02-2004: Integrating Electronic Security into the Manufacturing and Control Systems Environment”. This report outlines a multi-step approach to developing a cybersecurity program in industrial settings. The ISA Security Life Cycle Model is a fifteen-step process that covers all areas of security management from initial goal setting to post deployment re-evaluation of security counter measures. The entire model is shown in Fig. 3.

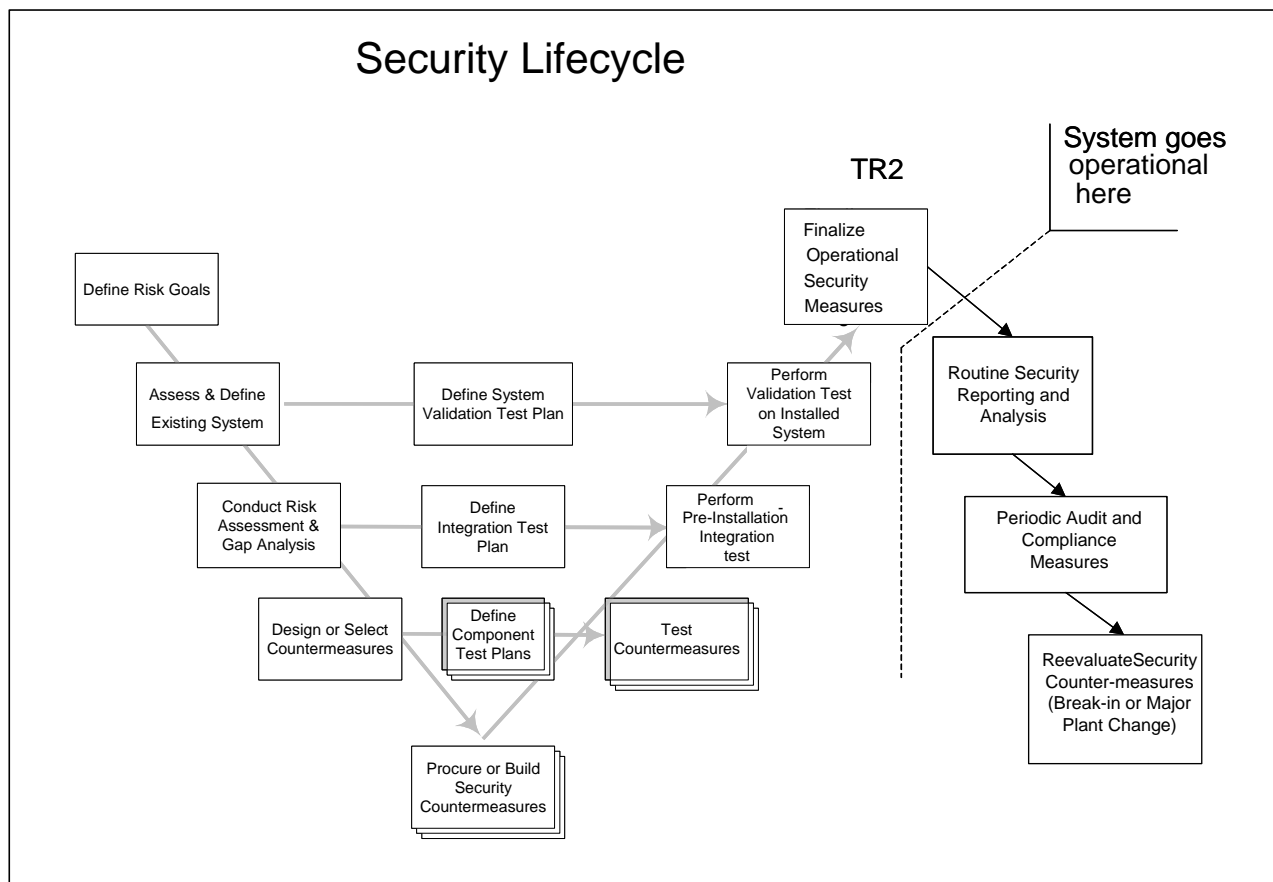


Fig. 3 ISA-TR99.00.02-2004 Security Life Cycle Model

### A. Assessment Procedure

The focus of an assessment can be found in steps two and three of the model, namely to “Assess and Define Existing System” and “Conduct Risk Assessment and Gap Analysis”.

### B. Human Element

Assessing the current cybersecurity situation at a particular site involves surveying key employees involved in the operations and security of the control networks and equipment at the plant site. A series of structured interviews regarding the cybersecurity of the networked systems is held. These interviews provide the basis for the technical analysis of the networked systems in terms of security. They are focused on determining:

- 1) General understanding, compliance and agreement to security policies used to protect network systems from cyber attack;
- 2) Current process system network architectures with respect to cybersecurity;
- 3) Remote connections to control systems devices on the site;
- 4) Any control system security concerns that are not currently addressed by the existing policies.

The focus is on both systems and devices and includes all aspects of control technology. This information

is initially recorded on standard interview sheets and then transferred to the project database. After the completion of each interview, the interviewer performs a preliminary assessment and assigns a risk level to each question. The interview sheets are then entered into the database and the Risk Level adjusted to improve the consistency of the individual assessors over the small sample of interviewees.

### C. Device Inventory

An inventory of networked control devices must be developed. A comprehensive list of devices is assembled and collated into the project database. This database will be expanded into a more complete asset database as the assessment is completed.

### D. Network Architecture

In this exercise, the network connectivity and configuration data of networked control devices is collected. Network diagrams of the control network system must be created that outline the key devices on the network. These network diagrams are graphical representations of the devices identified in the database. The diagram captures the basic logical network architecture, such as connectivity, combined with some of the physical network architecture like location of devices.

### E. Assessment Tool Development

From an initial review of the network architecture, security assessment instruments and procedures are selected. The intent is to use procedures and software tools that have a low probability of causing disruption to process operations.

Vulnerability Assessment (VA) scanning tools, widely used by IT administrators, determine if devices attached to the network are correctly configured and patched. Unfortunately, these supposed “Non-intrusive” tools can cause control devices to fail, making their use unacceptable in critical plant floor environments.

To address this concern, a set of non-intrusive security assessment instruments and procedures tailored to the specific control facilities at site must be developed. These must then be tested on similar, non-production control systems to ensure that they do not adversely impact the production systems.

### F. Device Assessment

The next task is to conduct a device assessment, investigating the networked devices in the process areas, including:

- Servers
- Human Machine Interfaces (HMI)
- Modems
- Routers/Switches
- Firewalls
- Programmable Logic Controllers (PLC)
- Distributed Control Systems (DCS)
- DCS and PLC Gateways
- Intelligent Electronic Devices (IED)

The information collected (as applicable) includes:

- Operating System Version/Patches/Service Pack
- Operating Processes and Services
- Applications (Approved and Non-Approved)
- Protection Software (Antivirus, Firewall)
- Connectivity Hardware (e.g., Ethernet, Serial, WLAN, Fieldbus, etc.)
- Connectivity Software (e.g., Remote Control, Web Access, Email, FTP, etc.)
- NetBIOS and NFS Shares
- Open IP Ports
- User and Password Security Policy
- User Lists
- Other Configuration
- Physical Security

The device assessment is carried out by physically visiting each device and applying the appropriate tool and assessment sheet. The assessment sheets identify basic device information such as the time of assessment, assessor, plant area, location, function, application, custodian, manufacturer, model, operating system and IP address. The device is then assessed for security risk in five areas (Physical Access, Software Access, External Connectivity, Device Specific Issues, and Comments and Observations).

### G. Collate Results and Analysis

Once the field assessment is complete, the assessment team commences the reduction and analysis of the collected device and interview data. The collected data from the Assessment Sheets and software tools are entered into the project database to be analyzed. An assessment report is then created, outlining the areas of both compliance and concern. A gap analysis, or comparison, with current industry best practices is completed. Here, a sound working knowledge of the technology and standards is required.

### H. Recommendations

Out of the analysis come recommended solutions to bring security practices in line with current industry best practices. Once the gaps are identified, solutions are proposed. These include:

1. Policy Development
2. Architectural Review
3. Review of External Connections
4. System Vulnerabilities
5. Device Vulnerabilities
6. Segmentation of Systems
7. Physical Security

## VI. PROTECTIVE MEASURES

After the initial steps of policy development and improved awareness are completed, the following steps will improve plant floor security.

### A. Security Policies

Consistent security policy alignment throughout the plant is required. Control system operators and engineers are usually very interested and capable of doing a good job securing the control systems, but they often lack the direction from senior management. As a result, the quality of the security efforts (such as anti-virus management) can vary widely, putting even well-secured systems in jeopardy. Site-wide security policies for the process control areas must be developed.

There is also a need to improve the communication and execution of security solutions between the IT group and the control engineers in the process areas. This will ensure security implementations crossing IT/Process boundaries are followed through without discontinuity.

Once this control system security policy is defined, we recommend that company management build an awareness of security understanding on the site by educating the control system staff on a regular basis.

One area of particular importance and complexity can be the question of a reasonable policy for passwords in critical control systems. Password policies in a control environment typically need to address issues not present in the IT arena. For example, how can an 8-digit password policy be used on a RTU that only allows a 3-digit numerical password? Or, consider that using standard IT password lockout procedures may not be acceptable for most HMI stations - the default needs to be to let the

operator in, not lock him out, the opposite of the IT assumption. Imagine how popular the security manager would be if, during a process emergency the operator panics and misspells his password three times, causing the HMI to lock out all access for the next 10 minutes. While password lockout is considered good policy for protecting servers, it does not apply in the control room.

### B. Network Architecture

Next to consistent and well-followed security policy, the network architecture is probably the most important technical factor in determining if a process control facility can be effectively secured from cyber attack. A poorly designed architecture will compromise deployed security countermeasures, offering a false sense of security.

An example of this occurred in January 2003, when the Slammer worm penetrated a number of plant floor networks that staff had believed were secure. The networks had firewalls separating them from the corporate network and were believed secure. In most cases, the infections occurred because poor network design allowed alternate pathways around the firewall in the form of poorly configured VPN tunnels, servers with dual network interface cards and shared network infrastructures.

### C. System Hardening

Remove unnecessary services and applications from process control computers. This system hardening results in tighter system security by shutting down unnecessary open ports, services and software. It involves identifying the uses of a particular computer and then disabling (or in some cases removing) all components that are not required for execution of that business function. For example, control computers often are preloaded with office applications for word processing, email and multi-media viewing. These make the PCs and consequently the control system more vulnerable to attack. For example, Fig. 4 shows a typical listing of open TCP/IP ports on a HMI computer. Only a fraction of these was needed for the operation of the control system. The other ports simply increase the opportunities for a hacker or virus to exploit the system.

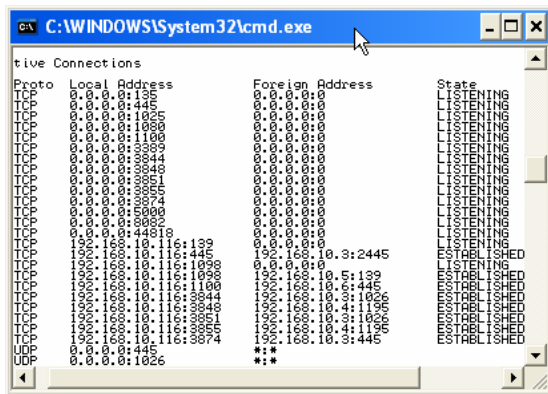


Fig. 4 Typical Open Ports on a Control System PCs

A file sharing policy for transfers across process firewalls and for inside the process control networks must also be established. This policy needs to be as secure as possible and eliminate the most common sharing errors that hackers exploit. Using file sharing software across firewalls should be strongly discouraged. The best practice of sharing files through a firewall does so through a relay server, typically by an encrypted file transfer protocol (FTP).

Past assessments have revealed that a majority of PCs on the control networks are open to one of the easiest and common attacks, namely taking over a shared "C\$" drive by brute force username and password guessing. Combine this with the use of simple passwords and easily guessed shared usernames, and a crack of the system is quick and easy.

### D. Remote Connections

The deployment of remote access software is a common practice in the industrial sector. Many users and equipment vendors use this type of software extensively to provide remote support of the process systems. It is often used for both LAN-based and external dial-up based access.

The plant should design and implement a standard policy to allow remote users to attach to process control machines. This process should include two-factor password and data encryption. Two-factor passwords are common these days and involve a key fob that displays a new 6-digit code that changes every sixty seconds. This code is combined with the password to authenticate the user to the system.

Furthermore, some form of central logging and administration of these connections should be implemented.

## VII. CONCLUSIONS

This paper has presented an overview of the security vulnerabilities of today's industrial control networks. These vulnerabilities exist despite abundant information, standards and recommended practices published by such organizations as the IEC, IEEE and ISA.

While a good understanding of the issues is required to appreciate the problem, the good news is that it does not take long for the plant engineering forces to get up to speed on the network issues surrounding cybersecurity. Unfortunately, the same can be said for the "hacker". Many incidents have occurred and even more are yet to come. Existing systems are vulnerable but can be secured. Given the resources available, future systems can be made secure from the start.

Assessing the existing network is straightforward. Producing a human assessment, device inventory and network diagram is the first step. Development of sensitive assessment tools that can gather the required information, but not affect the process computers is also required. All information is gathered, entered into a database, analyzed and then compared to Industry "Best Practices".

Recommendations likely to come out of an assessment are the development of a comprehensive

security policy, including a password policy, harden the existing embedded systems, secure and monitor remote connections. Above all implementation of security policies, education and alignment of IT and process control groups will go along way to securing existing networks and ensuring future ones are as safe as possible.

Whether internal or external forces assess the systems, the cybersecurity of the process control systems is only one critical piece of the overall corporate security goals and cannot be viewed in isolation. As a result, a cybersecurity assessment should be considered as an adjunct to the other corporate security efforts, rather than a standalone report.

Just as we put our substation equipment and control devices under lock and key, we need to secure the microprocessors and embedded systems that look after them. Creating a control system security structure that achieves industry best practices can be accomplished but will require effort as well as support and guidance from management to be realized.

### VIII. REFERENCES

- [1] *API Standard 1164 - SCADA Security*, American Petroleum Institute, September 2004.
- [2] *Introduction to Computer Security: The NIST Handbook*, National Institute of Standards and Technology, October 1995.
- [3] B. Fraser, "RCF 2196 - Site Security Handbook", *Internet Engineering Task Force*, September 1997, Pg. 21
- [4] *BSI 7799 Information Security*, British Standards Institute, 1995.
- [5] *ISO/IEC 17799, Code of Practice for Information Security Management*, International Organization for Standardization and the International Electrotechnical Commission, 2000.
- [6] IEEE Power Engineering Society, *IEEE Standard 1402-2000: IEEE Guide for Electric Power Substation Physical and Electronic Security*, IEEE, New York, NY, April 4, 2000.
- [7] *ISA-TR99.00.01-2004, Security Technologies for Manufacturing and Control Systems*, Instrumentation, Systems and Automation Society (ISA), 2004.
- [8] *ISA-TR99.00.02-2004, Integrating Electronic Security into the Manufacturing and Control Systems Environment*, Instrumentation, Systems and Automation Society (ISA), April 2004.
- [9] Adolfo Rodriguez, John Gatrell, John Karas and Roland Peschke, *TCP/IP Tutorial and Technical Overview*, IBM Corporation, International Technical Support Organization, Seventh Edition, August 2001.
- [10] Eric Byres and Justin Lowe, "The Myths and Facts behind Cyber Security Risks for Industrial Control Systems", VDE Congress 2004, Berlin.
- [11] "SQL Slammer Worm Lessons Learned For Consideration By The Electricity Sector", *North American Electric Reliability Council*, Princeton NJ, June 20, 2003
- [12] Esther D'Amico, Cybersecurity gains momentum, national groups introduce guidelines, *Chemical Week*, August 21, 2002, vol. 164, issue 33.

- [13] J. Lowe and B. Robertson, "Integrating Security in SCADA Solutions", *Electronic Security of SCADA, Control and Automation Systems Workshop*, National Infrastructure Security Coordination Centre (NISCC), London, UK, May 2003.

### IX. VITAE

**Adam Creery, P.Eng.** is the Manager of Electrical and Controls Engineering at Universal Dynamics. He has eighteen years of experience in the detailed design, design supervision, project management, construction supervision, and commissioning of power and control systems for industrial projects in a variety of industries, including power utilities, petrochemical, chemical, electrochemical, and pulp and paper. Mr. Creery's experience has covered a broad scope of electrical activities, from the design of high voltage installations to the design of networked process control systems.

**Eric J. Byres, P.Eng.** is the research leader at the Internet Engineering Lab at the British Columbia Institute of Technology, one of North America's leading research facilities in the field of industrial cybersecurity. For the past 15 years, he has specialized in data communications and controls systems in industrial environments, focusing on industrial Ethernet research and network security design. Mr. Byres provides consulting to G7 government security agencies, major oil companies and power utilities on cyber protection for critical infrastructures. Eric is also the chair of the ISA SP-99 Security Technologies Working Group, a standards effort focusing on the development of international framework for the protection of industrial facilities from cyber attack.

In 1999, Eric was the winner of the Best Paper Award at the Institute of Electrical and Electronic Engineers (IEEE) Pulp and Paper Industrial Applications Conference and in September 2000 he won the IEEE Outstanding Industry Applications Article award for his paper on network security. In May 2004 he was the recipient of the BCIT Applied Research Award for his contributions to in critical infrastructure security research. Most recently, he was honored with the Donald P. Eckman Education Award given by the Instrumentation, Systems, and Automation Society (ISA) for "outstanding educational and training contributions to the fields of industrial data communications, network security, and fieldbus technology".