

INDUSTRIAL NETWORK SECURITY FOR OIL
PIPELINE AUTOMATION AND CONTROL SYSTEM

(Conference ID: CFP/114/2017)

¹Eng. Lucky Mutambo P .Eng, ²Dr. Richard Silumbe

^{1,2}Information and Communications University, School of Engineering

SIN: 1206257440

Email: ¹mutambo.mwitwa@outlook.com, ²rsilumbe@zrdc.org

Abstract: *Many automation and modernization programs are now employing industrial internet of things technologies in industrial control systems. These ensuing systems are a mixture of state-of-the-art and legacy installations which create challenges in the implementation and enforcement of security measures. Control system intrusions can cause environmental damage, safety risks, poor quality and loss of 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 designers to plan infrastructure expansion with confidence in the security and reliability of the network's operation.*

Keywords: *Industrial networked control systems, Network security, Ethernet communications, Vulnerability assessment, secure network architecture, Remote access, Control system security, Cybersecurity.*

1. INTRODUCTION

1. Background

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 oil and gas pipelines, Motor Control Centers (MCC), and chemical process plants.

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 in the Crude Oil Pipeline Automation and Control Systems of Tanzania Zambia Mafuta Pipelines Limited [Tazama], a state company owned by two countries. The company was formed in 1968, it has seven [7] pump stations, one [1] main control center, and 1703 Kilometers in length.

In order to come to grips with this matter, 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.

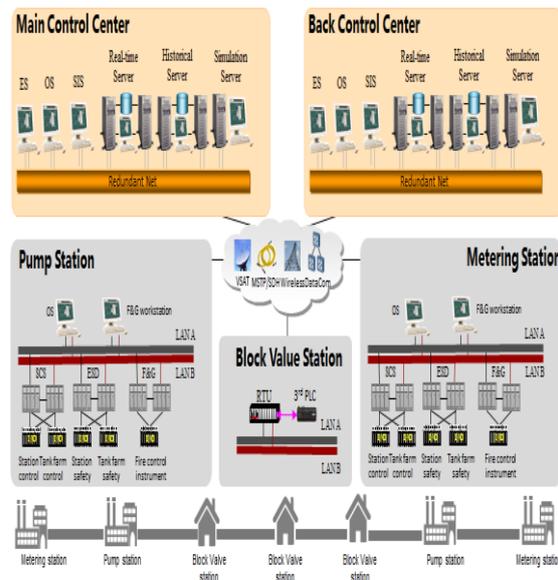


Fig. 1 Pipeline SCADA System

2. Statements of the problem

Automation and Control Systems have been at the core of critical infrastructures and industrial plants for many decades, and yet, there have been very few confirmed cases of cyberattacks.

Control systems, however, are more vulnerable now than before to computer vulnerabilities for many reasons:

Controllers are computers. Most of the original physical controls (traditionally conformed of a logic of electromechanical relays) have been replaced by microprocessors and embedded operating systems. These controllers may provide many functionalities, such as flexible configuration via a web server, and digital communication capabilities that allow remote access and control. The increased complexity of the software base may also increase implementation flaws (software bugs).

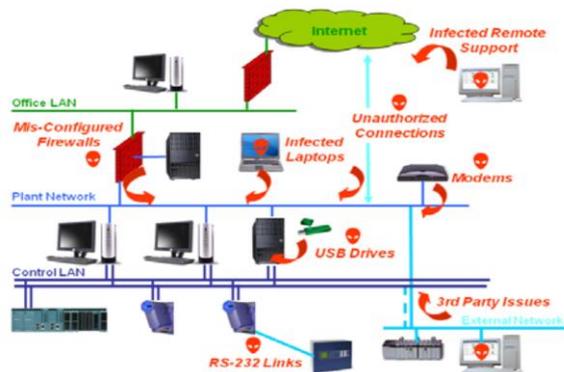
Networked. Control systems are not only remotely accessible, but increasingly for efficiency reasons they are being connected to corporate networks and the Internet. Even control systems designed to be closed may, in practice, not be perfectly isolated:

connectivity through uncontrolled connections can occur in many ways (e.g., via mobile devices).

Commodity IT solutions, although in the past control systems were generally made up of proprietary software and hardware components, today many control systems employ commodity IT systems; such as, off-the-shelf Windows computers, TCP/IP networking etc. Consequently, control systems inherit the vulnerabilities of these components.

Open design. Increasingly, even protocols that are unique to control systems are now more open and more accessible, therefore it is easier for an attacker to obtain the necessary knowledge to attack the system. This point is, however, controversial: security professionals generally argue that open design is preferable because they can find and fix bugs more easily. The debate between open design and closed design is an active one [1].

Increasing size and functionality, Wireless sensor networks and actuators are allowing industrial control systems to instrument and monitor larger number of events and operations. It is a standard security concern that new functionalities may give rise to new vulnerabilities.



Attack routes taken. In 75 incidents from 2002 to 2006, attackers and viruses infiltrated SCADA systems via secondary pathways nearly 50% of the time. (Source: *Industrial Security Incident Database, June 2006*)

3. Literature Review

In this paper I disclosed or summarized various articles or journals listed below, regarding the procedure for conducting a thorough assessment of the process control networks to evaluate the risks and come up with the technical and procedural countermeasures to mitigate these risks.

Once complete, as I mentioned earlier it allows the network designers to plan infrastructure expansion with confidence in the security and reliability of the network's operation.

HMI: Information from Answers.com

Last visited: February. 2017

<http://www.answers.com/topic/hmi>

CERT coordination center

Carnegie Mellon University's Software Engineering Institute, last visited: February. 2017

<http://www.cert.org>

CIA Triad, Wikipedia

Wikipedia, CIA Triad, last visited March 2017

http://en.wikipedia.org/wiki/CIA_triad#_Key_concepts

CS2SAT Control System Cyber Security Self-Assessment tool

U.S. Department of Homeland Security, last visited: February. 2017

http://www.uscert.gov/control_systems/pdf/CS2SAT.pdf

Gasoline Pipeline Rupture and Explosion at Whatcom Creek: A focus on response management. *Thor Cutler and Anthony Barber, U.S. Environmental Protection Agency, January 2001*

<http://www.iosc.org/papers/00888.pdf>

- Protecting Critical Infrastructure from Cyber Attacks
U.S. Department of Homeland Security, 2007
http://www.clcert.cl/seminario/US-CERT_Chile_2007-FINALv2.ppt
- Introduction to Control Systems, Security for IT Professionals
Department of Homeland Security (hard copy), September 2008
- 21 steps to improve cyber security of SCADA networks
Office of Energy Assurance U.S. Department of Energy, 2002
<http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf>
- Gazprom Fights 'Prejudice' Over South Stream Project
James Kanter, International Herald Tribune, April 2009
http://www.downstreamtoday.com/News/article.aspx?a_id=16139&AspxAutoDetectCookieSupport=1
- Penetration Testing of Industrial Control Systems
David P. Duggan, March 2005
http://www.sandia.gov/scada/documents/sand_2005_2846p.pdf
- Secure Networks for Process Control
Enterasys secure networks, February 2008
<http://www.enterasys.com/company/literature/sn-pc-wp.pdf>
- SCADA Networks
Martin and Bakhto, last visited: May 2009
<http://www.giac.org/resources/download.php?id=352&cat=7&c=ca895c6963263f1a47a0da5ccc789ded>
- Gas refineries at Defcon 1 as SCADA exploit goes wild, Dan Goodin, September 2008
http://www.theregister.co.uk/2008/09/08/scada_exploit_released/
- The Official ITIL Website
Last visit: June 2017
<http://www.itil-officialsite.com/home/home.asp>
- Mitigating the Top 10 Network Security Risks in SCADA and Process Control Systems
McAfee, April 2007
http://www.mcafee.com/us/local_content/white_papers/wp_cor_scada_001_0407.pdf
- The STRIDE threat model
Microsoft Corporation, last visited June 2017
<http://msdn.microsoft.com/en-us/library/ms954176.aspx>
- MultiSmart Pump Station Manager for Water and Wastewater Lift Stations
MultiTrode, last visited: June 2017
<http://www.multitrode.com/pump-station-manager>
- Guidance for Enforcement of CIP Standards
North American Electric Reliability Corporation, last visited: June 2017
http://www.nerc.com/files/Guidance_on_CIP_Standards.pdf
- NERC standard CIP-001-1 - Sabotage Reporting
North American Electric Reliability Corporation, November 2006
<http://www.nerc.com/files/CIP-001-1.pdf>
- NERC Standard CIP-002-1 – Critical Cyber Asset Identification
North American Electric Reliability Corporation, November 2006
<http://www.nerc.com/files/CIP-002-1.pdf>

NERC Standard CIP-003-1 – Security Management Controls
North American Electric Reliability Corporation, November 2006
<http://www.nerc.com/files/CIP-003-1.pdf>

NERC Standard CIP-004-1 - Personnel & Training
North American Electric Reliability Corporation, November 2006
<http://www.nerc.com/files/CIP-004-1.pdf>

NERC Standard CIP-005-1 - Electronic Security Perimeter(s)
North American Electric Reliability Corporation, November 2006
<http://www.nerc.com/files/CIP-005-1.pdf>

NERC Standard CIP-006-1 - Physical Security
North American Electric Reliability Corporation, November 2006
<http://www.nerc.com/files/CIP-006-1.pdf>
NERC Standard CIP-007-1 - Systems Security Management
North American Electric Reliability Corporation, November 2006
<http://www.nerc.com/files/CIP-007-1.pdf>

NERC Standard CIP-008-1 - Incident Reporting and Response Planning
North American Electric Reliability Corporation, November 2006
<http://www.nerc.com/files/CIP-008-1.pdf>

NERC Standard CIP-009-1 - Recovery Plans for Critical Cyber Assets
North American Electric Reliability Corporation, November 2006
<http://www.nerc.com/files/CIP-009-1.pdf>

Good Practice Guide Process Control and SCADA Security
National Infrastructure Security Co-ordination centre, November 2006

<http://www.cpni.gov.uk/Docs/re-20051025-00940.pdf>

Guide to Industrial Control Systems (ICS) Security, Special Publication 800-82
National Institute of Standards and Technology, September 2008
http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

Recommended Security Controls for Federal Information Systems and Organizations, Special Publication 800-53 Revision 3
National Institute of Standards and Technology, last visited: June 2017
<http://csrc.nist.gov/publications/drafts/800-53/800-53-rev3-FPDclean.Pdf>

New and original study on industrial cyber security reveals at least tenfold increase in number of successful attacks on process control and SCADA systems since 2000
PA Consulting Group, October 2004
http://www.paconsulting.com/news/press_release/2004/pr_myths_and_facts_behind_cyber_security_risks_for_industrial_control_systems.htm

Your Personal PLC Tutor Site - What is a PLC? *Last visited: June 2017*
<http://www.plcs.net/chapters/whatis1.htm>

Beating the hackers
Process Engineering, January 2007
<http://www.processengineering.co.uk/Articles/298007/Beating+the+hackers.htm>

Understanding SCADA System Security Vulnerabilities
Riptech, Inc., January 2001
<http://www.iwar.org.uk/cip/resources/utilities/SCADAWhitepaperfinal1.pdf>

The 2008 European Community SCADA and Process Control

Summit *SANS Institute, October 2008*

http://www.sans.org/euscada08_summit/

How the SEC Protects Investors, Maintains

Market Integrity *U.S. Securities and*

Exchange Commission, last visited: May

2009

<http://www.sec.gov/about/laws.shtml>

Slammer worm crashed Ohio nuke plant

network *Kevin Poulsen, Security Focus*

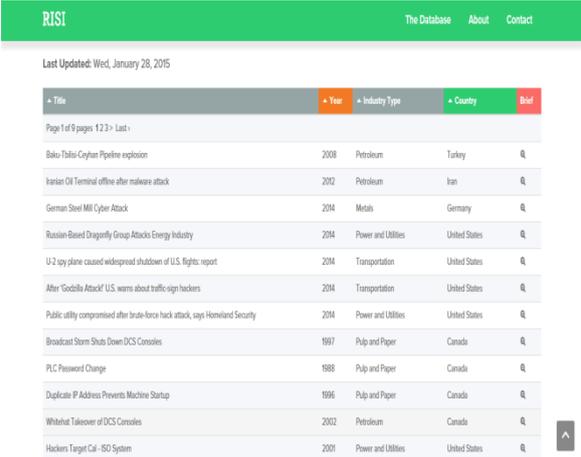
August 2003

<http://www.securityfocus.com/news/6767>

2. 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.

The Repository of Industrial Security Incidents is an online repository system that is used to track industrial cybersecurity incidents. The RISI Industrial Security Incident Online System 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 repository online system is shown in Fig. 2.



The screenshot shows the RISI website interface. At the top, there is a green header with the RISI logo and navigation links: 'The Database', 'About', and 'Contact'. Below the header, it says 'Last Updated: Wed, January 28, 2015'. The main content is a table with columns: 'Title', 'Year', 'Industry Type', 'Country', and 'Brief'. The table lists several incidents, including 'Baku Tatar Ceyhan Pipeline explosion' (2008, Petroleum, Turkey), 'Iranian Oil Terminal offline after malware attack' (2012, Petroleum, Iran), 'German Steel Mill Cyber Attack' (2014, Metals, Germany), 'Russian-Based Drifter Group Attacks Energy Industry' (2014, Power and Utilities, United States), 'U-2 spy plane caused widespread shutdown of U.S. flights: report' (2014, Transportation, United States), 'After "Godzilla Attack" U.S. warns about traffic sign hackers' (2014, Transportation, United States), 'Public utility compromised after brute-force hack attack, says Homeland Security' (2014, Power and Utilities, United States), 'Broadcast Storm Shuts Down DCS Consoles' (1997, Pulp and Paper, Canada), 'PLC Password Change' (1988, Pulp and Paper, Canada), 'Duplicate IP Address Prevents Machine Startup' (1996, Pulp and Paper, Canada), 'Whitehat Takeover of DCS Consoles' (2002, Petroleum, Canada), and 'Hackers Target Cal-ISO System' (2001, Power and Utilities, United States). Each row has a magnifying glass icon in the 'Brief' column.

| Title | Year | Industry Type | Country | Brief |
|--|------|---------------------|---------------|-------|
| Baku Tatar Ceyhan Pipeline explosion | 2008 | Petroleum | Turkey | 🔍 |
| Iranian Oil Terminal offline after malware attack | 2012 | Petroleum | Iran | 🔍 |
| German Steel Mill Cyber Attack | 2014 | Metals | Germany | 🔍 |
| Russian-Based Drifter Group Attacks Energy Industry | 2014 | Power and Utilities | United States | 🔍 |
| U-2 spy plane caused widespread shutdown of U.S. flights: report | 2014 | Transportation | United States | 🔍 |
| After "Godzilla Attack" U.S. warns about traffic sign hackers | 2014 | Transportation | United States | 🔍 |
| Public utility compromised after brute-force hack attack, says Homeland Security | 2014 | Power and Utilities | United States | 🔍 |
| Broadcast Storm Shuts Down DCS Consoles | 1997 | Pulp and Paper | Canada | 🔍 |
| PLC Password Change | 1988 | Pulp and Paper | Canada | 🔍 |
| Duplicate IP Address Prevents Machine Startup | 1996 | Pulp and Paper | Canada | 🔍 |
| Whitehat Takeover of DCS Consoles | 2002 | Petroleum | Canada | 🔍 |
| Hackers Target Cal-ISO System | 2001 | Power and Utilities | United States | 🔍 |

Fig. 2 Typical RISI Security Incident Online 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 [Eric Byres and Justin Lowe, 2004].

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, Repository of Industrial Security Incidents Online System has a report that shows that:

Iran has been forced to disconnect key oil facilities after suffering a malware attack. The computer virus is believed to have hit the internal computer systems at Iran’s oil ministry and its national oil company.

Equipment on the Kharg island and at other Iranian oil plants has been disconnected from the net as a precaution after suffering a malware attack.

Another report from North American Electric Reliability Council (NERC) 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".

Stuxnet the best-known attack at a SCADA system. The first versions were observed as early as in 2008 [N. Falliere, L. O. Murchu, and E. Chien, 2011]. It is suggested that the worm was developed by the US or Israel, and up to 60 percent of the infected computers were in Iran. Thus, computer security has also become an international relations issue [K. Hearn, P. A. Williams, and R. J. Mahncke, 2010]. Stuxnet is known for being the most advanced attack ever devised in cyberspace, and it is considered to be the first worm directed at ASC. Stuxnet leveraged several vulnerabilities and used advanced coding to infiltrate and cover its own tracks. Stuxnet is a worm which propagates through networks and installs itself on all Windows machines. Then it uses 0-days vulnerabilities to escalate privileges as to root-it the machine to create a persistence presence. Once it is installed, it looks for the WinCC and Step7 software, which are used to configure Siemens PLC S7 and S3 series. Stuxnet continues by infecting USB-keys so as to reach machines that are not connected to the network. It has two modes of attack; one for S3, looking for the specific PLC of type 6ES7-315-2, and one looking for a S7-413.

All in all, Stuxnet was the first to use four 0-day exploits, compromising two digital certificates and injecting malicious code into industrial controllers, and finally hiding it from the operator. Even after being analyzed it was feared that incorrect removal could cause damages. "Stuxnet could be used to cause a significant amount of damage if it

is not properly removed,"[R. McMillan, "Siemens"] this was later rebuffed as Siemens posted that customers had removed it without damages [Siemens, "Siemens recommendation]. The outcome of Stuxnet might have been as much as a thousand centrifuges damaged or destroyed in the Natanz Enrichment Plant [P. B. David Albright and C. Walrond, 2010].

Night Dragon; in February 2011 [White paper, McAfee, 2011], McAfee disclosed the discovery of a series of attacks against energy, petrochemical, and oil companies. The attacks were traced back to mainly Chinese addresses and are believed to have started in 2009. The attack was so well hidden that it was not exposed for two years. The attack was using SQL injection techniques for the servers exposed to the Internet. While basic in nature, SQL injections might result in gaining usernames and passwords for further penetrating the network. After the initial attack the attacker used the compromised servers to access the internal network and compromise more internal servers.

The paper outlines Night Dragon that had command and control servers and Remote Administration Toolkits (RATs). The attack might not have caused the physical damages that Stuxnet did, but it did manage to exfiltrate sensitive information such as financial documents regarding exploration sites and bid information.

The malware Zotob was first discovered in 2005 and was directed at a vulnerability in Microsoft Windows 2000 [P. Mangan, "W32.zotob. d." 2005]. Windows 2000 was, and still is, used as the underlying operating system in some control systems. The malware was developed by two men in their twenties, which caused the security community to reconsider how easy it was to develop malware. Zotob used vulnerability in the plug and play feature that made it possible

to access and control computers remotely. The malware was distributed over the Internet, and it spread fast. It also spread to control systems as some of them had Windows as the underlying operating system. Zotob was made with the guidance of the MS05-039 security advisory, which disclosed the vulnerability.

The attack caused damages even if a patch was available since most companies are slow to apply such patches. Zotob caused damages that on average cost 97000\$ to fix in addition to 80 hours of work to clean up for each site that was affected. [J. Stith, "Zotob damages hit \$97k, 2005].

Control systems are typically vulnerable as installed. Unfortunately, it is usually only after an upset that steps are taken to secure the 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.

3. 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 [J. Lowe and B. Robertson, 2003].

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 ANSI/ISA's "Part 1: Terminology, Concepts, and Models ANSI/ISA-99.00.01-2007 Security for Industrial Automation and Control Systems". This document outlines a multi-step approach to developing a cybersecurity program in industrial settings. The ISA Security Life Cycle is a process that covers all areas of security management from initial goal setting to post deployment re-evaluation of security counter measures. The following I present the steps of the security life cycle:

3.1 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".

3.2 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.

3.3 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.

3.4 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.

3.5 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.

3.6 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 and 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).

3.7 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.

3.8 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

4. PROTECTIVE MEASURES

After the initial steps of policy development and improved awareness are

completed, the following steps will improve plant floor security.

4.1 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, I 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 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 6-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.

4.2 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.

4.3 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.

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 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.

4.4 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 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.

5. CONCLUSIONS

Nowadays, isolated industrial control networks are converging on standard ICT-based systems bringing new security challenges and a large number of potential risks due to threats, vulnerabilities and failures. Some of these are associated to the TCP/IP standard, the use of open (hardware and software) components and wireless communication technologies.

In order to address some security issues, special attention should be paid to the network management. Critical control networks (SCADA systems) must supervise, through computational systems, the constant performance of other critical systems, whose services are essential for survivability, like for ex-ample electric energy. A failure or threat in the control of a critical system could mean the (total or partial) disruption of its services, and therefore massive chaos among interdependent infrastructures whose impact could be devastating for the well-being of our society and economy.

6. ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my regional management of Tazama Pipelines Limited, Eng. Jason Mwanza, Eng. George Chapu, and Eng. Collins Kalumba. Many thanks to Dr. Richard Silumbe, as my thesis advisor for your patience, support and guidance throughout this effort. Mr. Chanda Mataka, thank you for sharing your deep knowledge of critical infrastructure as well as your research expertise and patience. Without your assistance and the efforts of your personnel this thesis would not have been possible.

Lastly, thank you to my wife, daughter and two sons for your love and support. To my wife, thank you for your time and patience in supporting me throughout this effort. Also, thank you for your countless hours reviewing my writings and acting as a sounding board for my ideas. You and the kids are my continuing inspiration and motivation.

Eng. Lucky Mutambo, PEIZ

REFERENCES

- [1] Amin, S., Bayen, A., Ghaoui, L. E. and Sastry, S. S. [2007], Robust feasibility for control of water flow in a canal reservoir system, in 'Decision and Control, 2007 46th IEEE Conference on', pp. 1571–1577. Amin, S., Cárdenas, A. A. and Sastry, S. S. [2009 a].
- [2] A Safe and secure networked control systems under denial-of-service attacks, in R. Majumdar and P. Tabuada, eds, 'HSCC', Vol. 5469 of Lecture Notes in Computer Science, Springer, pp. 31–45.
- [3] Amin, S., Cárdenas, A. and Sastry, S. [2009 b], Safe and secure networked control systems under denial-of-service attacks. In R. Majumdar and P. Tabuada, eds, 'HSCC', Vol. 5469 of Lecture Notes in Computer Science, Springer, pp. 31–45. Amin, S., Litrico, X., Sastry, S. and Bayen, A. [2010],
- [4] Stealthy deception attacks on water SCADA systems, in 'Proc. 13th ACM International Conference on Hybrid Systems: Computation and Control (HSCC '10)', pp. 161–170. Anderson, R., Böhme, R., Clayton, R. and Moore, T. [2008],
- [5] Security economics and Euro-pean policy, in 'Proceedings of the Workshop on the Economics of Information Security WEIS', Hanover, NH, USA. Anderson, R. and Fuloria, S. [2009],
- [6] Security economics and critical national infrastructure in 'The Eighth Workshop on the Economics of Information Security'. Anderson, R. and Fuloria, S. [2010],
- [7] On the security economics of electricity metering, in 'The Ninth Workshop on the Economics of Information Security'. 174 Attorney, U. [2007],
- [8] 'Willows man arrested for hacking into Tehama Colusa Canal Authority computer system', http://www.usdoj.gov/usao/cae/press_releases/. Başar, T. and Olsder, G. [1999],
- [9] Dynamic Noncooperative Game Theory, second edition edn, SIAM Series in Classics in Applied Mathematics, Philadelphia, PA. Banda, M. K., Herty, M. and Klar, A. [2006],
- [10] 'Gas flow in pipeline networks', AIMS Journal on Networks and Heterogeneous Media (NHM) 1 (1), 41–56. Basseville, M. and Nikiforov, I. [1993],
- [11] Detection of abrupt changes: theory and application, Prentice-Hall, Inc., Upper Saddle River, NJ, USA. Bedjaoui, N., Weyer, E. and Bastin, G. [2009],
- [12] 'Methods for the localization of a leak in open water channels', Networks and Heterogeneous Media 4 (2)