Global Information Assurance Certification Paper

Ian Henderson
April 2nd 2004
GSEC Practical Assignment
Version 1.4b
Securing Process Control/ SCADA Systems

Abstract

This document describes a security remediation project which addressed how to secure a process control system. The system in question, like many others, had been designed to be stand alone but had over time become integrated with the site standard IT systems. The security remediation project attempted to secure the control system by extracting it from the standard IT systems while retaining the ability for IT users to access real time data. Lessons learnt during this project are equally applicable to a new build process control system. This project did not resolve all the security vulnerabilities common in process control system rather; it outlines the minimum a prudent operator would be expected to implement given the constraints presented in such a system.

Background

Process control or Supervisory Control and Data Acquisition (SCADA) systems are designed to provide real time control of industrial processes such as chemical plants, refining plants, pipelines, manufacturing plants, power generation plants, water distribution etc.

In the past, these systems were fully autonomous running bespoke operating systems on bespoke hardware using bespoke communications protocols. The massive increase in standard IT system deployments and the associated cost reductions generated significant pressure for control system vendors to adopt cheap of the shelf (COTS) technologies.

In the main, control system vendors ported their Human Machine Interfaces onto PC's running the Microsoft Windows operating system, this was quickly followed by optimisers, and historians. Although few final control devices use the Microsoft Windows operating system, almost all will now support TCP/IP connectivity.

The result is that control systems have transitioned from closed proprietary systems to open systems running standard operating systems that use standard communications protocols. This transition has allowed control engineers and developers to make advances both in the complexity of control schemes that can now be implemented and in the productivity of control engineers. In addition, connecting these systems to the corporate network has brought real time data to the business user allowing improved decision making to take place.

Unfortunately, the transition to standard IT equipment has not been accompanied by adoption of state of the art security policies, most control systems although connected to the corporate IT network are still treated as though they were proprietary closed system. This is a common problem across many industries and has been identified as a risk to the critical national infrastructure of many countries. Indeed there are several well documented

failures directly caused by beaches of the process control system security. Joe Weiss of Kema consulting comments that "Control system security breaches aren't just lurking in the shadows; they're real, in addition, they are happening globally."[1]

Existing System Security

The system addressed by the security remediation project, although designed to be stand alone, was integrated into the corporate IT infrastructure but did not conform to any of the corporate IT standards. There were many reasons for the integration, among these are:

- Process control support staff wanted to perform administrative functions from their corporate desktop.
- The business increasingly required real time data from the process control system to facilitate decision making.
- The process control network was installed before the corporate IT network "arrived".
- Cost savings were made by utilising "spare" corporate network infrastructure.

These requirements had been met by directly connecting the process control IP network to the corporate network. This was achieved via a switched network connection.

Although the process control servers and workstations are standard PC's, running standard Microsoft operating systems, the process control system vendor had not qualified any Anti Virus software to run on these machines. There was also no process to evaluate any hot fixes or security patches.

The process control system had been designed to meet a very exacting availability standard. The system was required to achieve an availability of greater than 99.999% (5 nines) or put another way, there should be no more than 5 minutes downtime per year!

To meet this requirement, the process control system was designed with a great deal of redundancy. Take the main process control application servers as an example. There are 2 servers each running a full version of the process control server application, At boot time, the process control server attempts to contact the primary process control server, if no primary server responds then the server considers itself to the primary server. Similarly, once both servers are running, the secondary server will periodically (every 5 seconds) poll the primary to check that it is alive, if it receives no response then it will assume the primary server role.

Each server is powered by redundant power supplies, the power itself is supplied by an Uninterruptible Power Supply (UPS) with 12 hours battery capacity and a standby diesel powered generator. The servers each include a RAID 5 array of hard disks.

Remote support of the system was provided by the vendor via dial up modems. The remote support facility was a contractual requirement

In summary then, the process control system had mainly been designed with resilience and safety in mind. However, the increased use of standard IT technologies had rendered this system susceptible to cyber attacks, thus

threatening their stability an d availability. Consequently, the safe and reliable operation of the plants under control was at risk. This project aimed to ensure the integrity and availability of control systems and its associated data .

Project Phase

As this type of project had no t been undertaken before a new approach was developed. The main steps are as follows:

1. Assemble a cross functional team with expertise from the worlds of control and IT, included in this team were the users of the system.
2. Identify the systems involved, bot h physically and logically, identify data flows and repositories. Identify who need ed data and where it was stored
3. Perform a risk assessment on the system.
4. From the risk assessment, develop a mitigation strategy, prioritise quick wins to encourage the pro ject team and the end users, don't try to solve all the problems in one go.
5. Monitor the success of the risk mitigation actions.
6. Repeat steps 2 throu gh 5 periodically to assure the security posture.

Although each of these steps is equally important, this document will deal mainly with step 5, the risk mitigation actions. Ot her steps are coved briefly for completeness.

Assemble Project Team

It was quickly reco gnised that the security problem could not be solved by one group alone. In general:

- Control Eng ineers understood the control system and the plant under control but did not understand the security flaws inherent in their Microsoft W indows based systems and TCP/IP networks.
- IT staff could bring a wealth of understanding on networking and IT secur ity but did not understand how "standard" IT solutions would affect the control system applications.
- The control system vendor understood in depth how their application worked but had no security experience.

An excellent example of this disjointed coverage was it was suggested that the security flaws in the control system could be revealed by running a simple NESSUS scan. The control engineers and the vendor's staff were reluctant to run the scan on a live system and so the scan was run on a hot spare/training system.
The outcome of the scan was to hard crash all the human machine interface machines (taking almost 2 hours to fully recover). If this had happened on the live system, the production plant would have almost certainly had to be shutdown for safety reasons.

The final project team consisted of staff from IT, Control, vendor and users. The users were not full time members of the team but were consulted on a regular basis to ensure that solutions developed by the team were workable in "real life".

System and User Identification

Once the team was assembled, the system identification phase began. The proved to be simpler than first expected, the control system was well documented and the data flows/users easy to find. The users fell into 3 categories outlined the table below

USER	LOCATION	Data Requirements
Control Room Operator / Team lead	Control System HMI	All data in real time (no more than 5 seconds old), alarming and trending of historical data
Control Engineer	Control System HMI or Corporate desktop	AS control room operator + administrative access to machine s
Planning/Mangers	Corporate desktop	Historical Data i.e. data that is greater than 1 minute old
Control System vendor staff and out of hours support staff	Vendor premises / remote sites	Administrative access to control system machines

Dealing with each of these groups in turn:
Control room operators required no corporate IT functionality from the control system, all corporate functionality (e-mail etc) was provided by a separate machine.
Control Engineers had a dedicated control system human machine interface but also required access to the control system from their corporate desktops. This was generally used for administrative functions.
Planning and site managers required "real time data"; they just didn't need it to be refreshed every 5 seconds. Their requirements were satisfied as long as the data was up to the minute.
Vendors and out of hours support staff (control engineers) require administrative access to machine from remote locations. This was achieved using a dial up modem.

Looking at these requirements, there are only 2 reasons for interconnectivity of the control system and the corporate IT system

1. Mangers and planning department require minute by minute historical data that is extracted from the control system historian using OPC protocol. OPC stands for OLE for Process Control and

is a widely used communications protocol used to share control system data, it is built on the Microsoft COM/DCOM model and regulated by the OPC foundation. "Based on fun damental standards and technology of the general computing market, the OPC Foundation adapts and creates specifications that fill industry - specific needs. OPC will continue to create new standards as needs arise and to adapt exist ing standards to utilize new technology. " [2]

2. Control Engineers require admin functionality from within the corporate network and out of hours require remote system access via a modem, this access point is shared with the control system vendor.

Risk assessment

4 main areas of risk were identified, each was ranked on the likelihood of damage or production impact occurring s a result of the risk area being compromised. These are, in order of perceived risk:

- Mode ms
- Network Connectivity
- Anti Virus
- Crisis response Planning

Modem connectivity was identified as a serious risk to the security of the system, the existing modem was not configured with any sec urity options. However remote connectivity was a "must have" for the control engineers and control sys tem vendors in order to provide out of hours support. Clearly another method of connectivity must be found.

Network segregation between the corporate network and the control system was identified as e ssential to reduce the risk to e ither network. Networ k segregation via a "full blown" internet facing style firewall was seen as being a sledge hammer to crack a nut and may not be financially viable.

Anti virus protection was missing entirely on the control system machines. The control system vendor did not accredit any AV vendor package and the system warranty explicitly prohibited installation of 3 rd party software onto the control system.

Crisis response plan for the control system concentrated on availability of spares and backups, no explicit plans w ere in place to deal with a virus outbreak or a hacking incident.

Risk Mitigation

The risk asses sment complete, the next step was to develop risk mitigation actions for each of the risks identified. The emphasis on quick wins to improve security was encou raged.

To make an immediate improvement in the security posture, the modem was physically disconnected, a quick review of the control system users and passwords revealed many unused accounts left over from system

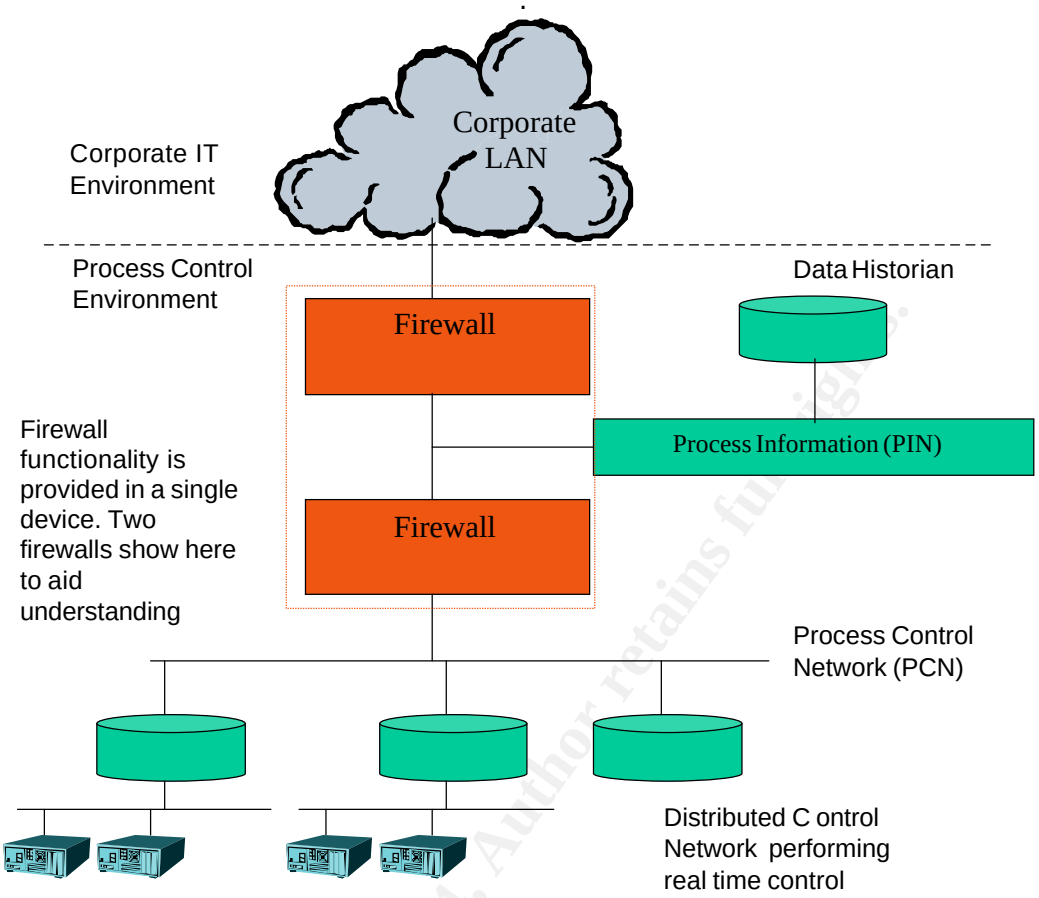
commissioning. These accounts were removed . Existing account passwords were tested for complexity by running the SAM file through a password cracking tool. Users with easily guessed passwords were requested to change to more complex passwords. Standard guidance on password complexity was readily available form the IT department.
The benefit in implementing these "quick wins" cannot be overstated, the team saw an immediate improvement in security, the users saw some tangible outcome from the team and both groups were encouraged to implement further improvements.

Modem and Network Connectivity

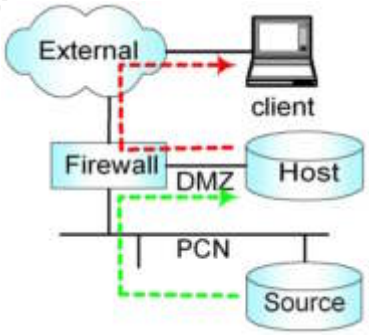
Risks 1 and 2, the modem and network connectivity were considered together as one could not be solved in isolation.

It was decided to re-design the control system network to remove the modem completely and to provide some level of network segregation from the corporate IT system.
The control system would be divided into private and semi public networks (when viewed from the corporate IT point of view). These networks would be known as the Process Control Network (PCN) and the Process Information Network (PIN) respectively. The Process Information Network acts as a DMZ between the control system and the corporate systems.
Options for network segregation identified were either, a router configured with Access Control Lists or a firewall.
Market research identified a suitable firewall, one which was designed to support a small office environment and was ideal to segregate the control system from the corporate IT network. The firewall included perimeter anti virus scanning on HTTP, FTP and SMTP and could act as a VPN end point.
The PIN, PCN and corporate IT networks would be inter-connected via this firewall. The data historian would move from the Process Control Network to Process Information Network. Users from the corporate IT network requiring access to the data historian would therefore not require access to the Process Control Network.

The resulting network design is shown below.



To provide a further layer of segregation , data would be pushed from the Process Control N etwork to the data historian on the PIN (DMZ). U sers would then pull data fro m the historian to applications on the cor porate network. This data flow is illustrated below.



An immediate consequence of i nterconnecting the process control environment to the corporate IT network in this way is to reduce the exposure to externally originated threats such as:

- Virus infections, worms and malicious Trojan -horse programs.
- Denial-of-service attacks from or via in terconnected environments.
- Unauthorised access and use from remote system.

- Subversion of process control systems by accidental or deliberate remote action.

Firewall rules were developed to facilitate data transfers described above. These rules ran into problems when trying to transfer data across the firewall using OPC. OPC is based on DCOM which uses a random port number each time a connection is made. This is obviously not firewall friendly as the firewall would have to opened up to include all "high ports" many of which are used for Trojan propagation. [3] Fortunately, this project was not the first to come across the problem. "There are several registry settings that control the DCOM port restriction functionality. All of the named values are located under the HKEY_LOCAL_MACHINE \Software\Microsoft\Rpc\Internet registry key." [4] Restricting the port range meant that sensible (tight) firewall rules could be implemented.

The next problem to be resolved was to provide administrative access to specific site staff and to vendor support staff i.e. replace the modem access. The outer network perimeter of the corporate IT network already had multiple defences against an Internet originated attack, including firewalls, intrusion detection systems and anti-virus scanning. Current dial-up connections bypassed all these protection mechanisms, as they are a direct interface into Process Control Network components from outside. Furthermore, as a dialup link can establish a direct path to a 3rd party network, the process control environment can be exposed to vulnerabilities present in such external networks. There are many automated tools, publicly available on the Internet, which can be used to find and attack poorly secured modems. A technique known as war dialling can be used to find such modems. "Today competitive market includes many freeware and commercial war dialling tools." [5]

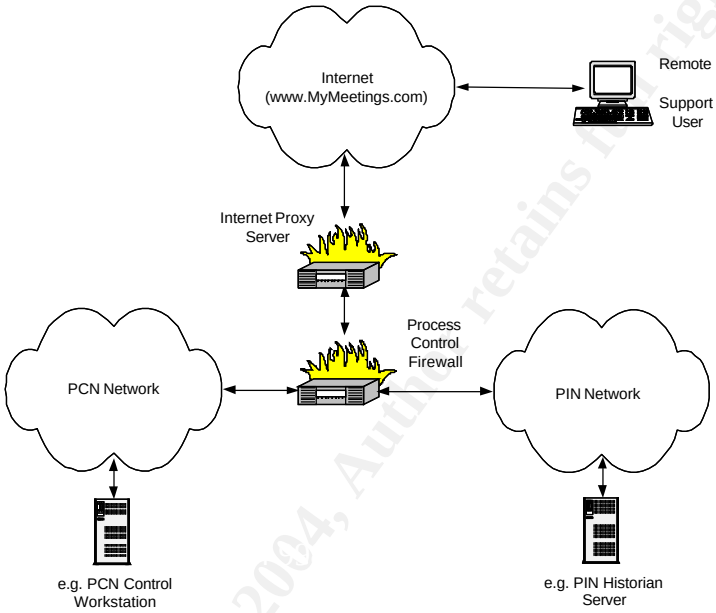
It was agreed that the control engineering staff could forego their administrative access to the Process Control Network from their corporate IT desktops. In the new security conscious paradigm, it was agreed that administrative functions were best performed local to the system where physical access and permit to work systems could be enforced. However, emergency out of hours support was still a requirement for the control team and for remote vendor support.

This remote connectivity was achieved by the installing of a Webex application in the Process Control environment. This would permit a reasonably secure remote access route to the applications and control environments that were accessed via dial-up remote access. This solution would also allow the vendors or third party support organisations a more secure method of access to the PCN environment via the internet, than was currently supported via remote dial-up access to PC-Anywhere or Carbon Copy type mechanisms.
Firewall configuration was required at the process control firewall and at the corporate network boundary firewall. The process control firewall had to be configured to allow the appropriate protocol (HTTP) to connect via the company internet proxy server to a specified internet Address (www.mymeetings.com). This connection was configured such that the

connection must be originated fr om within the PCN/PIN network by spe cific user action. This is the real beauty of this solution, no connection can be initiated from outside. When support is required, a n internal user has to initiate the connection and that same user can at any time terminate the connection. In addition, logging is enabled to provide an audit trail of all actions carried out by the remote user.

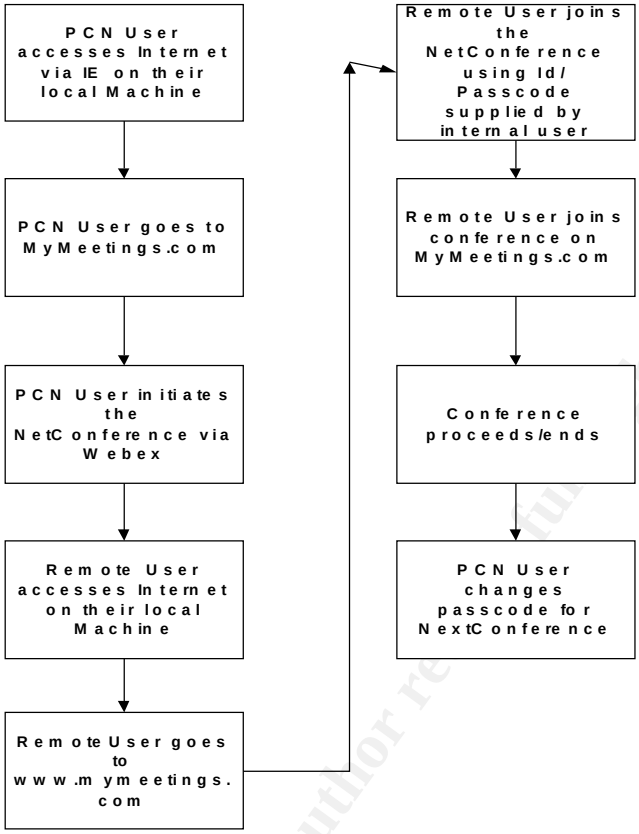
Architecture

Below is the architecture that was used to implement Webex within the process control environment.



Process Flowchart

Below is a sample flowchart of the process by which an external support organisation can securely access the PCN environment to conduct support activities.



Anti Virus Deployment

Although perimeter anti virus protection was provided by the firewall, applying the principle of defence in depth and recognising the risk of virus infection from removable media from within the process control system. It was agreed that anti virus protection was required within the control system itself.
The process control vendor was initially reluctant to accredit an anti virus product for use on their system, part of this reluctance was based on a fear that every client would ask them to accredit a different vendors product. This would be a significant overhead for the vendor. The project team asked the vendor to accredit one (any one) anti virus product for use on the control system. Installation of Anti Virus product on the control system required explicit agreement from the vendor as installation of 3rd party software was prohibited under the system warranty. Once the vendors internal accreditation process was complete, the issue of how and where to deploy AV on a control system was tackled. The following generic guidelines were drawn up:

- All process systems, especially those built on Microsoft Windows should be protected by an anti-virus product.

- Caution should be used when applying anti-virus software to process control systems. Anti-virus software should only be applied on process critical or safety critical systems where such software has been tested and accredited by the system vendors. Procedural/non-intrusive measures may be deployed when vendors guarantee would be voided by the installation of anti-virus measures or when vendors recommend against installing anti-virus measures on such systems.
- Where systems use platforms other than Microsoft Windows, the vendors should be consulted to determine if anti-virus measures are available. If available, it is recommended to install such protection.
- In the interest of avoiding update complexity, sites should strive to standardise on one anti-virus product where possible. It is recognised that the conflicting demand of vendors may not always make this achievable.
- Virus signature databases are expected to be refreshed daily, or earlier in case of an emergency update.
- Control system anti virus updates should be staged in the corporate IT environment. Process control systems should not connect to the internet to obtain updates.
- A staging server should be installed on the process information network. This server will provide a folder that can be shared out to the rest of the process control environment. This folder should have three sub folders for:
    1. The latest definitions from the corporate network (pending deployment testing)
    2. The current definitions that are used by the control nodes (i.e. deployment tested updates)
    3. The previous version of deployment tested definitions (to enable roll back to a previous version in the case of problems).

An FTP process was automated to download these updates on a regular basis (daily) to ensure that the latest updates are always available in the Process Control Network. An FTP process was preferred to copying from a network share in order to avoid having network shares enabled through the Process Control Network firewall and as previously stated the firewall provided anti virus scanning of FTP traffic.

Deployment test of signatures

To ensure the updated signatures have no detrimental effect on the operation of the system. The virus scan software on a single control node is triggered to update its signatures from the staging server. After fault free operation has been observed for an agreed period of time (3 hours) it is OK to assume that wider scale deployment of the signatures can take place.
Once this deployment test has been completed satisfactorily then the current definitions should be moved to the old definitions folder and the new definitions moved to the current definitions.
The final stage in the signature update process is to deploy the signature updates to the remaining process control nodes after deployment testing is complete. This is carried out by the auto update component of anti virus product. The process can be manually or automatically triggered. The

manual process will be required to update signatures in the event of an incident.
Care should be taken to ensure that only signature updates are automatically deployed as engine updates should be performed manually.

Crisis Response Planning

Despite implementing the other risk mitigation actions, it was recognised that there will always some susceptibility to future security vulnerabilities. These security vulnerabilities could arise from human error, procedures not being followed or technical vulnerabilities being identified in systems that are currently considered to be secure.
Consequently there is always the possibility of a cyber incident arising that could have a direct impact on process control environments. Therefore it is essential to implement a structured response process that will enable recovery from a cyber incident. This process should be documented in a site "Cyber Incident and Crisis Response Plan."

The objectives of an Incident and Crisis Response process are:

- To minimise the impact of a cyber attack on the process control environment.
- To ensure the safe operation of the production processes in the event of a cyber attack.
- To minimise the loss of production in the event of a cyber attack.
- To ensure full recovery of all normal Process Control Network facilities in an orderly manner

Definition of a Site Cyber Incident and Crisis Response Process

A high level Cyber Incident and Crisis Response process is outlined below. In developing this plan, the following areas were considered.

Notification and communication links

- Ensure regular and frequent security monitoring is in place and that unusual activity is reported to trigger the Cyber Incident and Crisis Response Process.
- Ensure links are in place between Process Control, IT and Security representatives as this is likely to be a key information route for the notification of virus alerts or new vulnerabilities.
- Ensure links are in place to the companies wider process control community. Warnings of problems might come from other sites within the companies process control community, alternatively other sites may benefit from notifications/experiences observed at this site.
- Ensure that the relationships between the Cyber Incident & Crisis Response Process and any other site-wide or specific Emergency Response Plans are fully understood.

Preparing for an incident

- Have a list of contacts who will be involved in the process available, including: site management, vendors, IT and process control staff.
- Have an up to date network diagram, list of assets and their configuration available.
- Ensure recent system backups are available. If backups are stored offsite, then consideration should be given as to whether the time to bring the backups back to site could be a constraint when responding to a given incident.

Who has the authority to act?

- Decide who has the authority to make decisions such as shutting down the Process Control Network or disconnecting from the Process Control Network from the corporate IT network
- Decide who has the authority to access systems to look for signs of intrusion and conduct further investigations.
- Decide who has the skill/expertise to act in each relevant area.
- Decide the procedure for reacting to an incident outside normal office hours.
- Decide the linkage between this plan and other existing site-wide or specific Emergency Response Procedures
- Decide the procedure for possible escalation of an incident

Priority of systems and dependencies

- Ensure that the control systems are prioritised so that in the event of an incident effort will be focussed on the key systems required for the safe operation of the site.
- Ensure that dependencies on other networks/systems are clearly understood. For example, one of the options available to a site when responding to a virus infection is to completely isolate the process control environment from all external networks.

User Training

- All staff, contractors and third parties who will be part of the Cyber Incident & Crisis Response process should be aware of their responsibilities and receive the required level of training.

Documentation

- Document all procedures, contacts, roles and responsibilities.
- In order to reflect new risks that may affect the Process Control Network, the Incident and Crisis Response Plan should be reviewed and updated on

a regular basis and after any security incidents.

Backup systems

Sites may already have backup or redundant systems in place for emergency use. These backup systems could range from a piece of redundant equipment to a fully redundant process control environment. However if these backup systems are based on the same technologies as the main systems they may be vulnerable to the same threats as the main systems. If they are permanently connected to the process control environment then it is likely that they will be equally affected by the same incident as the main systems. It may be possible to keep these backup systems powered off or isolated from the main systems in order to ensure they are not compromised when they are required.

If the site uses proprietary systems that are not running on common operating systems, such as Microsoft Windows, then the likelihood of known viruses affecting the system is much reduced. Thus, even in environments where common operating systems are used for primary control, older proprietary systems may provide a fallback option that retains basic control of the plant.

For installations where proprietary systems are not available and where no current backup systems exists, then it may be possible to construct some sort of redundant backup that will provide at least a minimal level of control in the event of a cyber incident.

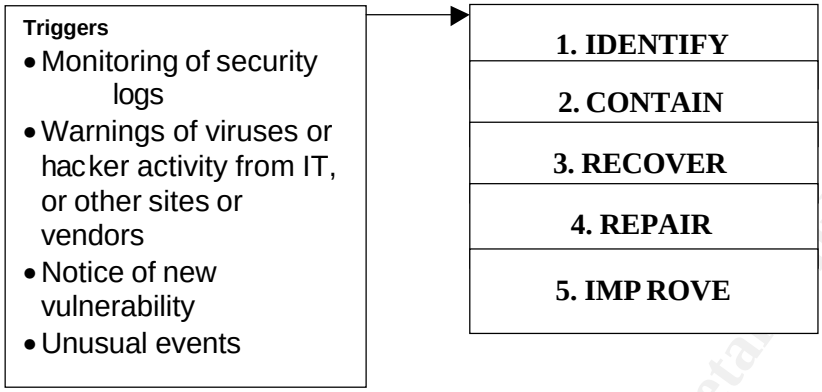
An example of such a backup system might consist of PCs/Servers (laptop or desktop) and simple networking equipment (hubs, cables etc.), together with control and configuration software (control application and programming software). The PC/Sever could be used to reconfigure the control environment and re-establish a certain level of control while the main environment is restored. However, this may not be possible or realistic in some situations where the control application relies on specific hardware or where the capital cost of a backup system is prohibitive.

In the event of loss of the Process Control Network due to virus attack, all IP-based systems that are normally operational should be considered infected and quarantined – this includes all network components (routers, switches and hubs). Consequently it is important that such systems are physically isolated from the Process Control Network or other networks until required for use in a crisis, as otherwise they might be infected in the same way as the main system and thus rendered useless. This can be done by ensuring the system is kept powered off and isolated from the Process Control Network until it is required for use in an incident. Similarly it is important to ensure that patch in procedures for the backup system ensure that no part of this 'clean' system is connected to any infected equipment as this would similarly render the backup system useless.

Cyber Incident & Crisis Response Process

High Level Process

A high level generic process was generated and is outlined below. This process may be customised by sites to form a site specific Cyber Incident & Crisis Response plan. This five -stage process is intended to highlight the key stages of the process and the differences from 'conventional' incident and crisis response planning procedures. It is likely that the detailed actions that a site performs in the event of an incident will be depen dant upon their specific circumstances and the technical design of their process control environment.



Process Stages Descriptions

IDENTIFY

Objective	**To identify the type of attack, risk to Process C ontrol Netw ork and actions required**
Actions	• Identify the type of incident (new vulnerability, virus, or hacker attack). • Identify the risk to which the P rocess Control Network is exposed • Identify possible impact of incident. • Identify next actions. The action might be to move to the next stage to contain an incident or to remain in a monitoring state until further developments occur.

CONTAIN

Objective	**To contain incident and preve nt further damage**
Actions	• Identify and implement actions to contain the situation and prevent further damage.

RECOVER

Objective	**To establish sufficient operations required to maintain safe production**
Actions	• Power up and patch in backup minimal equipment and systems to provide basic level of control • NB special care must be taken to ensure that the clean backu p

	control system is never connected to infected equipment as this might wipe out the backup systems as well.

REPAIR

Objective	**To restore normal systems operation in an orderly manner**
Actions	• Clean and restore systems to production in priority order. • NB special care must be taken to ensure clean restored systems are never connected to infected equipment in the restore process as they may become re -infected.

IMPROVE

Objective	**To identify causes of incident and identify improvements to prevent repetitio n**
Actions	• Carry out Post Incident Investigation and prepare incident report • Identify and implement security improvement actions

Process triggers

The above process only comes into effect when triggered by notification on an unusual event. This notificat ion might come from a variety of sources.

- Day to day security monitoring identifying unusual activity
- IT being notified of a new vir us
- Notification of a vulnerability from IT or Process control vendors
- Other sites experiencing problems with Process Control Network.

The effectiveness of the Incident and Crisis Response Process is dependent upon these information feeds. The latter three points are dependent upon good communication and notification links within the corporation and good relationships with prod uct vendors.

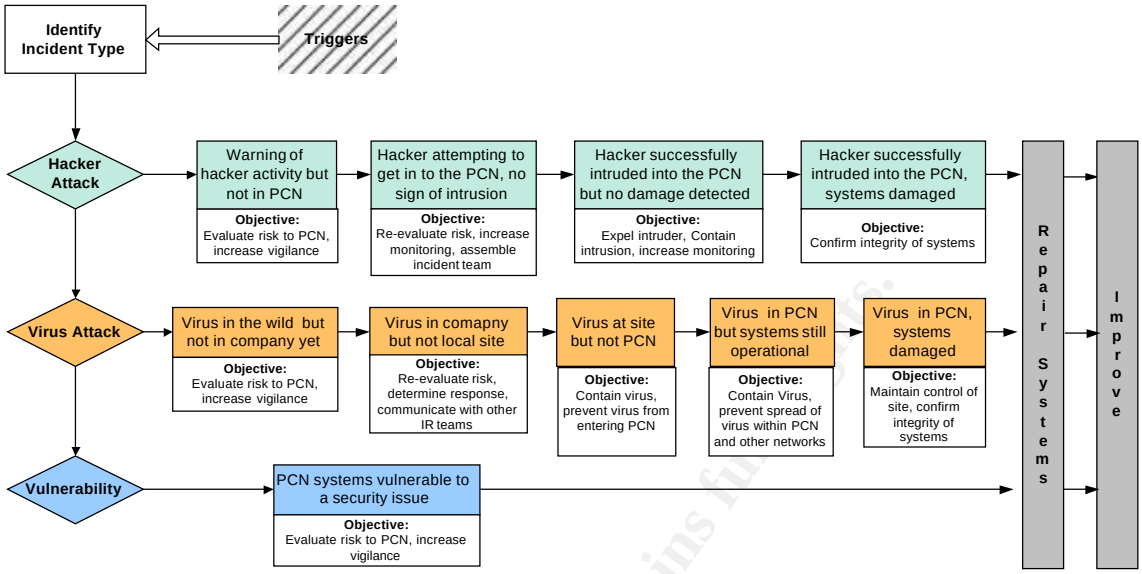
The first point highlights the importance of performing regular security monitoring of key systems on the process control environment. Examples of security monitoring activities are below .

- Monitor and inspect network device logs for unexpecte d behaviour
- Monitor and inspect system activities and logs for unexpected behaviour
- Inspect files and directories for unexpected changes
- Investigate unauthorised hardware attached to the Process Control Network
- Inspect physical resources for signs of unaut horized access
- Review reports by users and external contacts about suspicious and unexpected behaviour

Detailed Process Overview

The diagram below shows a more detailed view of the process and describes how the process may be applied to example cyber inci dent scenarios which are explored in more detail later, namely a hacker attack, a virus attack and a

new system security vulnerability.



Incident scenarios

Three scenarios were used to test the cyber incident response plan. Indicative actions are included at each stage to illustrate the sort of actions that might be considered in a real situation. Naturally these actions are specific and might not be appropriate for all sites. It should be noted that there are different courses of actions that might be followed for the different scenarios and how they develop in time.

Scenario 1 - Hacker Attack

1. Warning of hacker activity but not in Process Control Network
2. Hacker attempting to get in to the Process Control Network, no sign of intrusion
3. Hacker successfu lly in truded into the Process Con trol Network but no damage detected
4. Hacker successfully intruded into the Process Control Network, systems damaged
5. Repair systems
6. Improve secur ity

Scenario 2 - Virus Atta ck

1. Virus in the wild but n ot in company networks yet
2. Virus in company networks but not local site
3. Virus at site but not Process Control Network
4. Virus in Process Control Network but systems still operational
5. Virus in Process Control Network , systems damaged
6. Repair Systems
7. Improve se curity

Scenario 3 – A New Vulnerability Is Announced

1. Determine whether Process Control Network is affected by vulnerability
2. Repair System

Scenario 1 – Hacker Attack

1. Warning of hacker activity but not in Process Control Network	**IDENTIFY**
Objective: Ev aluate risk to Process Control Network , increase vigilance	
• Consider increasing level of security monitoring • Review security vulnerabilities of Process Control Network systems	

2. Hacker attempting to get into the Process Control Network, no sign of intr usion	**CONTAIN**
Objective: Assemble Incident Response team to determine threat level and response	
• Perform actions in step 1 AND • Assemble site cyber incident response team and brief on incident and intended actions. • Notify IT manager • Consider physically is olating the Process Control Network from all other networks at network boundaries until further information about the nature and impact of the incident beco mes available	

3. Intrusion detected but no damage evident	**CONTAIN**
Objective: Contain intrusion, increase monitoring	
• Perform actions in steps 1 & 2 AND • Physically isolate the Process Control Network from all other networks • Determine if any assets have been affected by the incident. Quarantine and label those assets that will be required for data f orensics or incident analysis purposes • Verify process control set-points are within operational norms • Change all passwords on Process Control Network user accounts	

4. Intrusion detected, damage of PROCESS CONTROL NETWORK evident	**RECOVER**
Objective: Expe l intruder, confirm integrity of systems	
The actions at this stage are highly site dependent however suggested actions are: If systems are still functioning: • Verify set points are within operational nor ms • Verify operation of safety systems • Deter mine whic h assets have been affected AND If systems are unavailable: • Perform actions in steps 1, 2 & 3 AND • Disconnect all systems from the Process Control Network	

- Patch in and power up redundant network equipment at critical connectivity points (e.g. a network hub or switch)
- Power up redundant control hardware (making sure there is no possibility of infection from infected machines) and establish control .
- Determine which assets have been affected by the in cident. Quarantine and label those assets that will be requi red for data forensics or incident analysis purposes.

5. Repair Systems	**REPAIR**

Objective: Secure and return systems to normal operation

- Liaise with Process Control System vendors.
- Consider bringing in specialist resources for performing data analysis and forensics
- Perform data analysis/forensics on quarantined machines to determine: how the incident arose, its likely impact and whether an audit trail is available which could assist in taking appropriate actions against the perpetrator or to assist law enforcement agencies with their investigations.
- Request that offsite backups are brought to site to assist in the system restoration exercises for compromised machines.
- Restore compromised equipment in business priority order from backups or by reinstalli ng. Input may be required from vendors.
- Patches and signature updates may be released by product vendors. Liaise with vendor prior to installing these patches on recovered or clean equipment.
- Restore network c onnectivity having considered effect on other connec ted parties and their state of readiness.

6. Report and Improve	**IMPROVE**

Objective: Identify causes and identify improvements

- Prepare a detailed incident report which should identify how the incident arose and why the Process Control Network wa s affected.
- Identify possible system security improvements to prevent reoccurrences

Scenario 2 – Virus Attack

1. Virus in the wild but not company yet	**IDENTIFY**

Objective: Evaluate risk to PROCESS CONTROL NETWORK , increase vigilance

- Conduct a Risk Asse ssment to determine probability and impact of the virus infection
- Consider increasing level of security monitoring
- Consider physically isolating the Process Control Network from all other networks until further information about the nature and impact of th e incident becomes availa ble
- Put the crisis management team on standby
- Monitor Anti-Virus websites for description of virus behaviours
- Back-up systems in case of attack, but do not overwrite old backups as these may be the only 'clean' source

2. Virus in company but not local site	**IDENTIFY**
Objective: Re-evaluate risk, determine response, communicate with other Incident Response teams	
• Perform actions in step 1 AND • Assemble a site cyber incident response team and brief on incident and intended actions • Brief operational staff on the situation • Ensure communications links with IT are operational • Strongly consider physically isolating the Process Control Network from all other networks. • Re-evaluate potential impact on Process Control Network. Review impacts as and when new information is available. • Assess safety of plant operation given latest info • Impose restrictions on importing data to the Process Control Network via removable media such as floppy disks.	

3. Virus at site but not Process Control Network	**CONTAIN**
Objective: Contain virus, prevent virus from entering PROCESS CONTROL NETWORK	
• Perform actions in 1 & 2 AND • Physically isolate the Process Control Network from all other networks.	

4. Virus in Process Control Network but systems still operational	**CONTAIN**
Objective: Contain Virus, prevent spread of virus within Process Control Network and other networks	
• Perform actions in steps 1, 2 & 3 AND • Determine if any assets have been affected by the virus • Disconnect and label all compromised workstations, terminals and servers from the Process Control Network. (NB powering machines down may cause damage to machines as some viruses run programs at start-up.) • Quarantine and label those assets that are infected to prevent accidental reconnection to the Process Control Network.	

5. Virus in Process Control Network – systems damaged	**RECOVER**
Objective: Maintain control of plant, confirm integrity of systems	
• Perform actions in steps 1, 2 & 3 AND • Disconnect all systems from the Process Control Network • Determine which assets have been affected by the incident. Quarantine and label those assets that will be required for data forensics or incident analysis purposes. • Patch in and power up redundant network equipment and at critical connectivity points (e.g. a network hub or switch) • Power up redundant control hardware (making sure there is no possibility of infection from infected machines) and establish control	

6. Repair / Patch	**REPAIR**
Objectives: Secure and return systems to normal operation	
• Request that off-site backups are brought to site to assist in the system restoration exercises for compromised machines.	

- Begin liasing with vendors.
- Consider bringing in specialist resources for performing data analysis and forensics
- Perform data analysis/forensics on qua rantined machines to determine: how the incident arose, its likely impact and whether an audit trail is available which could assist in taking appropriate actions against the perpetrator or to assist law enforcement agencies with their investigations.
- Patc hes and signature updates may be released by product vendors. Liaise with vendors before applying these updates
- Restore compromised equipment in business priority order from backups or by reinstalling. Input may be required fro m vendors
- Bring compromised machines online in accordance with vendor guidelines.
- Only reconnect machines to the Process Control Network if it has been determined that all the machines are defiantly free from the virus, if this is not done then it is highly likely that re -infection o f the Process Control Network will occur.
- Restore network c onnectivity having considered effect on other connected parties and their state of readiness.

7. Report and Improve	**IMPROVE**
Objective: Identify causes and identify improvements	

- Prepare a detai led incident report which should identify how the incident arose and why the Process Control Network was affected.
- Identify possible system security improvements to prevent reoccurrences

Scenario 3 – A new vulnerability is announced

1. A new vu lnerability is announced	**IDENTIFY**
Objectives: Assess risk of security issue	

- Determine whether Process Control Network is affected by vulnerability
- If Process Control Network may be affected assess risk. If risk is low consider monitoring situation until developme nts occur. If risk is high then consider implementing preventative measures (e.g. disconnection from IT networks)
- Update risk assessment as new information becomes available.

2. Repair / Patch	**REPAIR**
Objectives: Secure systems with new patches	

- If the risk of the security vulnerability being exploited is considered high then discuss the potential impact of applying patches to the Process Control Network system with the Process Control System vendor.
- Patches should be applied as part of a change control process which ensures proper testing before roll -out to live systems.

Ongoing Issues

As described above in the cyber incident response planning section, one can never remove all vulnerabilities , even a n air gapped system is susceptible to

malware via removable media. This is especially true in a process control system where the latest security patches may not be installable. Although this project has significantly increased the security of the control system, there are vulnerabilities that remain and will remain until the process control industry has caught up with the IT security sector. This project has also generated the impetus for a phase 2 security improvement programme, the most significant elements are outlined below.

Patch Management

The nature of the systems involved means that it is not practical to apply security patches in a timely manner. The control system vendor must first test and accredit such patches. This is a new requirement on the vendor and it will take time and effort before their internal processes are slick enough to accredit patches an acceptable time frame. Which of course raises the question as to what is an acceptable time frame? Given the seemingly endless reduction in the time between a vulnerability announcement and exploits being released, the vendors are targeting a turn around time of no greater than 10 days. This may not seem very ambitions but it represents a very significant step forward.

Vulnerability testing

As described above, standard vulnerability testing tools are wholly unsuitable for the process control environment where one device failure can be catastrophic.
Vulnerability testing/ evaluation tools will have to be developed specifically tailored for process control systems.

Operating system lock down

The complexities of the control system applications were such that the normal OS lock down processes were not applied for fear that these would impact the operability of the plant. Clearly this is an area where further study is required.

Intrusion Detection Systems

Traditional signature IDS's are not suitable for the process control environment as there are protocols running that are non-standard and therefore no signatures have been developed. Working with the control system vendor and a security specialist firm to develop control system specific IDS signatures is seen as a significant area of development which will provide yet another layer of protection for the control system.

Process Control Protocol Security

This project has deliberately avoided addressing security issues inherent in some of the intra process control communication protocols. Typically, these protocols have no security built in and are used on devices that are processor and or bandwidth constrained. These factors combined to make a security

retrofit impossible. The most that can be achieved is to wrap the entire system in a hard shell, or a series of hard shells. This was achieved by segregation of the control system from the internet, from the corporate network, from dial up access and by the application of host based anti virus products.

However, products are now being developed to provide protection for some common process control protocols. Most common among these is the MODBUS protocol.

"The protocol has no means of authenticating or authorizing the initiator of the request. Assuming the end-device is network accessible, malicious commands can be sent to it for a variety of objectives. To make matters worse, many of the end devices have no ability to perform packet filtering to even restrict which hosts may connect to the Modbus/TCP slave, let alone specific Modbus/TCP message types. Currently, the only reasonable solution is to filter via a firewall or router access control lists based on TCP port 502" [6]

Conclusion

This project has proven that process control systems security can be improved and that most (but not all) techniques from the standard IT world can be applied. A significant change in management of control system is called for and the effort required to implement this change should not be underestimated.

Despite the progress made, vulnerabilities remain, however, this project has shown that these can be protected by multiple defensive layers. It is recognised that this is only the beginning of an ongoing process that requires input from users, engineers and control system vendors.

References

[1] Joe Weiss, Kema Consulting Group "Kicking the control system bug, Preventing security breaches in plant control systems" ISA Intech (1 March 2004)
URL
http://www.isa.org/InTechTemplate.cfm?Section=InTech&template=/ContentManagement/ContentDisplay.cfm&ContentID=34074

[2] OPC Foundation, "What is OPC?"
URL http://www.opcfoundation.org/01_about/01_whatis.asp

[3] Joakim von Braun, von Braun Consultants and Simovits Consulting "Ports used by Trojans" (09-Dec-2002)
URL http://www.simovits.com/nyheter9902.html

[4] Michael Nelson. "Using Distributed Com with Firewalls" (19 March 1999)
URL http://www.microsoft.com/com/wpaper/dcomfw.asp

[5] Michael Gunn. "War Dialling" (5 October 2002)
URL http://www.sans.org/rr/papers/index.php?id=268

[6] OSDN Open Source Development Network," Transparent Modbus/TCP Filtering with Linux"
URL http://modbusfw.sourceforge.net/

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event