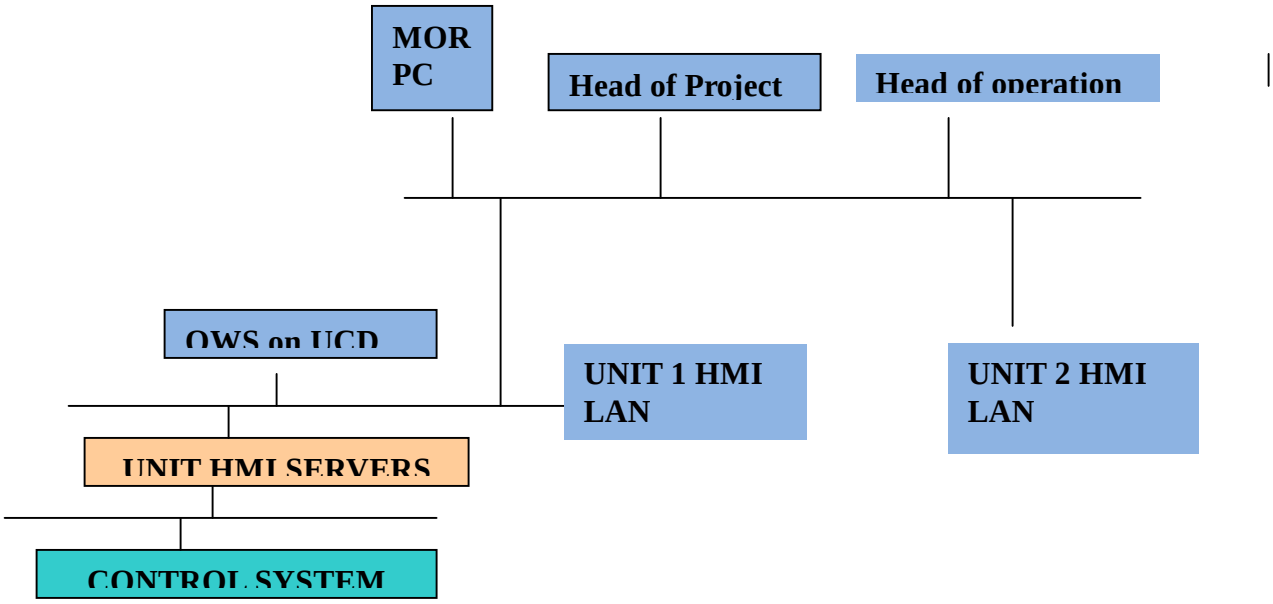


Figure 1: Typical DCS/PLC network in a power plant

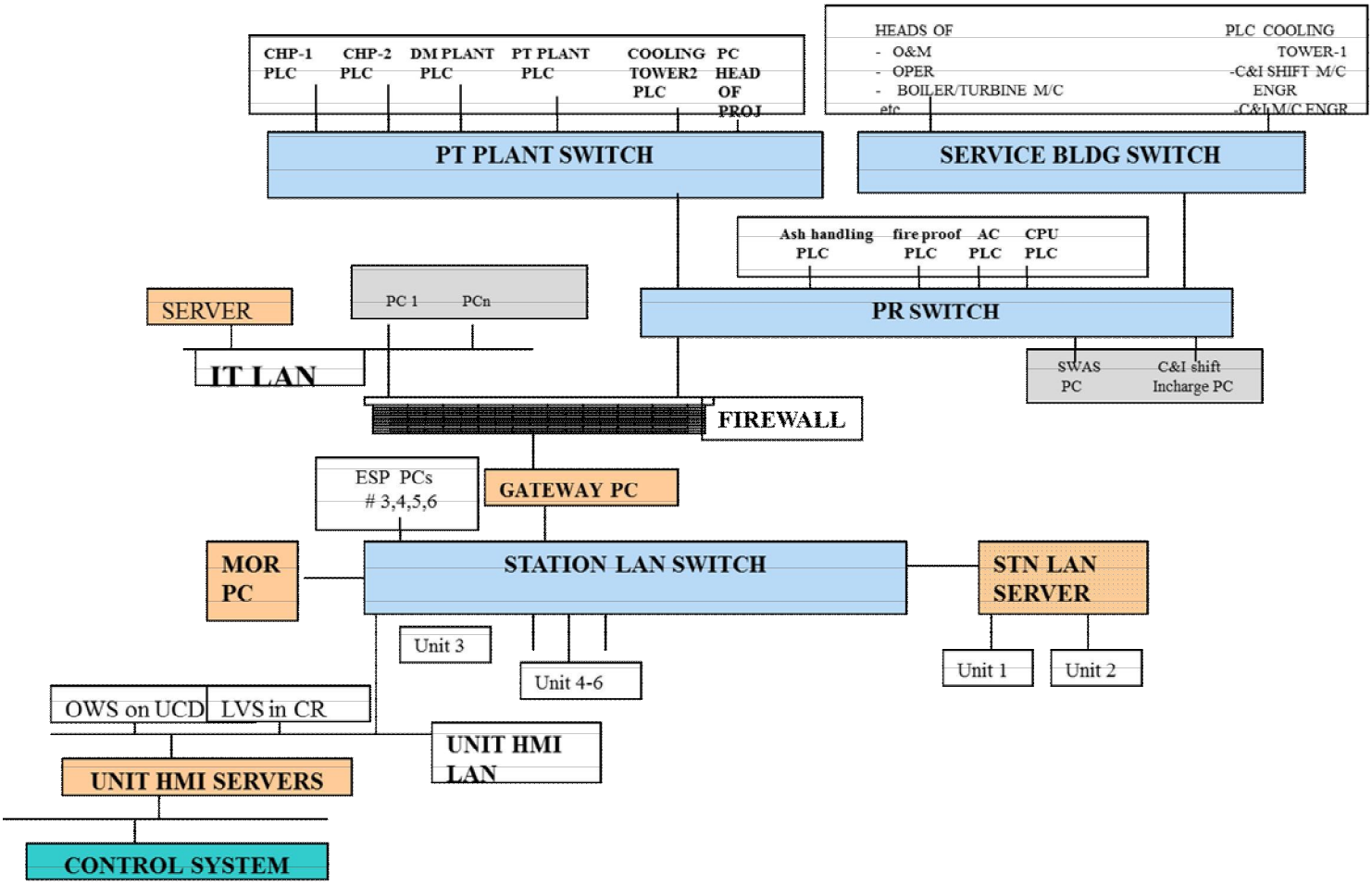


Figure 2: Typical DCS/PLC network in a power plant

3.0 CYBER THREATS LOOMING IN INDUSTRIAL CONTROL SYSTEMS:

With the interconnection of all the real time system of the plant, apart from data transfer, also the vulnerabilities of one system started getting transferred into the other systems. (Viruses, Worms, etc). Moreover, this provided a means of a malicious actor entering into the system through the network route.

Denial of Service attacks caused network clogging & hampering the normal functioning of the DCS.

Few of the targeted industrial cyber attacks related to the automation industry are listed below:

a) Sewage plant in Australia was hacked releasing millions of liters of sewage.
b) Browns Ferry nuclear plant was shutdown for two days because of excessive control bus network traffic.
c) Brazils' electrical grid attacked by Internet.

Probably, the most critical incident which shook the entire automation industry & changed the mindset of those who did not take cyber security in industrial automation systems seriously, was the Stuxnet worm. This stemed from the fact that heavy insider knowledge about the DCS was used to launch a directed sabotage, damaging targeted equipment. It involved modification of the plant logics, something unimaginable as it was always thought that cyber threats can only enter the HMI and disrupt the DCS working & not damage plant machinery by entering the control system.

More alarming is the fact is the trend is continuing. Duqu malware which is believed to be enhanced version of Stuxnet was also created around an year later & is believed to have attacked oil firms in Saudi Arabia.

All of these exploited a known vulnerability in the operating system either through internal means or external.

4.0 CYBER SECURITY PROGRAM:

The security counter measures in any installation are bundled as a cyber security program. This program rests on three pillars, PEOPLE, PROCESS & TECHNOLOGY. As with any system improvement

initiative, there is no substitute to awareness at the senior level of the plant & also the zeal of the people at the working level. Once this is ensured, there has to be clearly defined processes for all the actions expected of various personnel in the implementation & maintenance of a cyber security program. i.e. Security policies & procedures. Security policies are framed based on the risk analysis & business rationale & the security procedures translate these policies to clear steps delineating the process. Technology plays a very important role in the counter measures & here in particular in the context of cyber security, has to always keep pace with the latest developments & the latest security breaches. Technological aspects to be considered in a cyber security program consists of system architecture, hardware equipments & software to counter/isolate cyber vulnerabilities.

This is where the defense in depth approach comes into play; by employing multiple mechanisms, providing a sort of redundancy, the security improves many fold. The concept is similar to guarding a fort or castle.

5.0 THE ESSENTIAL COMPONENTS OF SECURITY PROGRAM :

A) **System architecture**:

A typical example of secured system architecture is presented in the figure below:

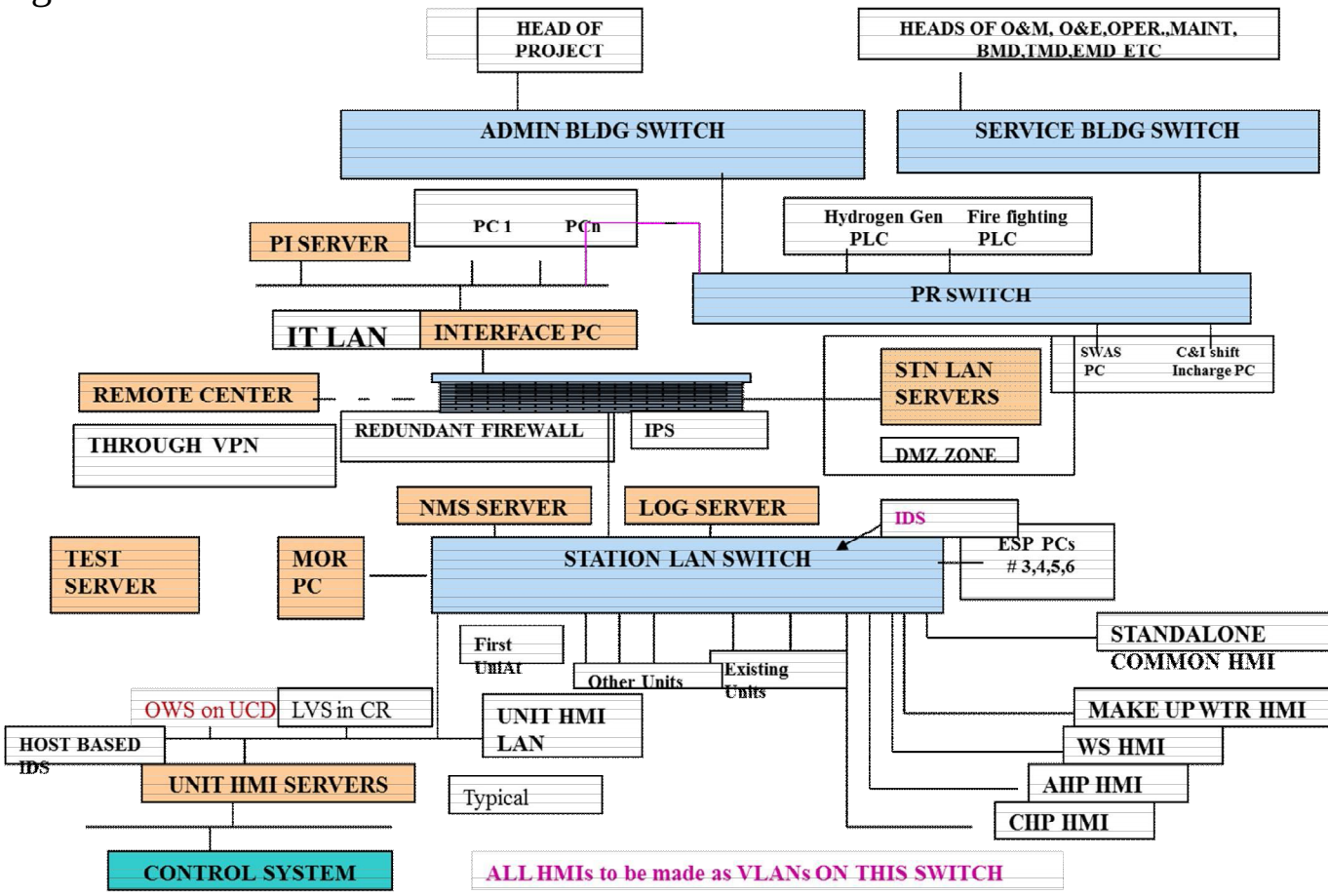


Figure 3 Secured System Architecture

Network segmentation is essential to a secured architecture & the different levels (as described in Table 1 below) have to be segregated.

Level	
0	Sensors & Actuators

1	Basic control
2	Operator Interface & Supervisory Control
3	Manufacturing Operations & Advanced Control
4	Business planning & Logistics

The different DCS are interconnected by a router switch & then a firewall with three zones is installed. The three zones are the inside zone which has the DCS, the outside zone which has all the third party systems (of Level 3 as well as the enterprise network of Level 4) and the demilitarized zone (DMZ) which has the Station LAN servers. The firewall ensures that no data is allowed directly from the outside zone to the inside zone. All data from outside is terminated at the DMZ. Eseentially, real time data to external world first travels from the DCS to the DMZ servers through the firewall & then from the DMZ to the external world again through the firewall. The same process is followed for data coming from external world as well. While implementing this, attempts are made to ensure different protocols for these data transfers i.e. one protocol for data transfer between outside zone & DMZ & another protocol for data transfer from inside zone to DMZ.

The firewall defines the basic process of DMZ through its port & IP filtering. Besides this, it is equipped with an Intrusion Protection system (IPS) which can be configured in two modes, i.e. Protection or Detection. The main difference between the two is whether the IPS is in line or offline. In protection or in-line mode, all the packets are examined for attack signatures & forwarded only when there are no attack signatures present. In detection or off line, the packets are examined for attack signatures in a node connected to the network & an alert is generated. As such, in detection mode, the network traffic flows uninterrupted. IPS configured in detection mode is also called IDS.

Since the firewall does not handle control traffic, and is placed at the perimeter of the DCS network, it is configured in IPS mode. An IDS is also placed in a node at the router (Later-3 switch) as here control traffic (traffic between DCS) is handled. Another method of enforcing defense in depth concept here is to ensure that the make of the IPS at the firewall & the router are different. Being different makes, there will be a variety in attack signatures & consequently more protection.

A dedicated port for remote connection for diagnostic support is provided at the firewall, suitable for VPN connection.

B) **Security Policies & Procedures**: Security policies & procedures provide a foundation of a security program & acts as a guide for managers, security team & users for their specific role within the security framework. It also articulates the management objectives while realizing a security program. Some of the security policies are firewall policy, third party access policy, media handling policy, change control policy, user access management policy, anti virus policy, information backup & restore policy, incident handling policy etc. All these policies include the business rationale behind the policy & the risk being addressed by it. These policies also define the constitution of the Information security team at the installation & the roles of its various members.

C) **Security Audits**: Security audit is a method of conformance to the various security policies & procedures & also intended to serve as a measure of how secure the system is. Typically, this is the last activity of a cyber security assessment program. However, this should be done periodically to ensure that the mitigation actions of previous audit is carried out & also to maintain the up-to date security readiness of the plant. Mainly, it has two constituents, vulnerability assessment using software tools which is conducted on each machine & penetration testing, which is a method of knowing

whether an ethical hacker is able to enter the system using an exploit. Many a time, identification of the vulnerability & its mitigation actions are considered sufficient in a security audit in a running plant, since use of the vulnerability or exploit is well known.

D) **Crisis management**: There should be well defined procedures for incident handling along with clear responsibilities of each member of the security team for recovery, analysis & reporting. Recovery depends to a large extent on the data back up & restoration procedures followed. Reporting mechanism to the higher management and also to the governing bodies is also very important as information transfer from unintended sources will lead to its own problems.

E) **Awareness, Knowledge & Skills**: Probably the most important aspect which triggers all other activities in a cyber security program is User Awareness. Knowing the security concerns being addressed by each activity along with its impact is key to success of the security program.

F) **Assistance Desk**: This is not mandatory for any cyber security program; but for a company with multiple installations, especially with multiple DCS, it is a good idea to have a centralized assistance desk. One of the main measure of security is the patch status of the installation. Patching being a continuous process can be closely monitored by the assistance desk, if connected remotely to the installation. Also, incident handling is largely facilitated through the assistance desk.

Patching the system. i.e. installing the OS patches, is by & large the most important requirement for keeping the system secure, especially when the system is connected through Internet for remote support or data analysis etc. Most of the cyber attacks had exploited a known vulnerability in the OS, for which a patch was announced

by the OS supplier, but was not installed in the system. Eg, the Stuxnet worm exploited many zero-day vulnerabilities in the OS. If the system was patched up to date, this sophisticated attack would not have materialized.

Having said this, these OS patches needs to be qualified by the DCS vendor before installing in the system. Many a time, the patch is re-distributed by the DCS vendor after qualification through various means.

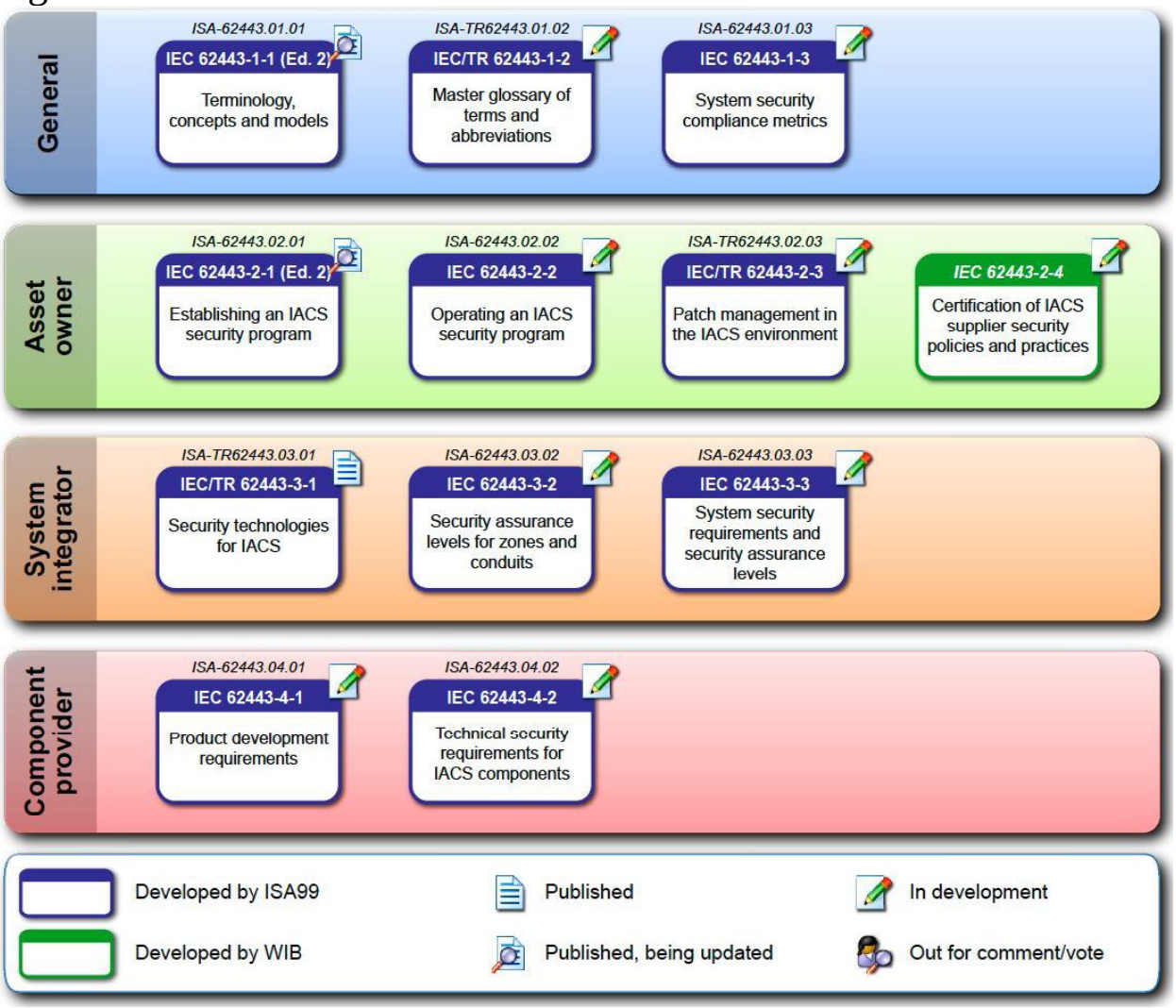
In order to instill more confidence in the maintenance personnel for patching the system, sometimes a test server/machine is also provided. This machine is of the same configuration as the target machine, but is offline. The patches are installed first here, & the machine is run to make sure there are no undesired behavior, before installing in the target machine.

6.0 IT SECURITY AND IACS SECURITY :

There are significant differences when we talk of security in a IACS environment as compared to an IT environment. Response in a IACS environment is critical; so when we implement software as security measures, its effect on the system response needs to be weighed. Equally important is the focus on availability in an IACS environment. Moreover, in the worst case, an industrial cyber attack like Stuxnet can not only disrupt the process, but also can damage plant equipment. Thus, in terms of impact, industrial cyber breaches can be very costly & more time consuming in terms of recovery.

7.0 SECURITY STANDARDS: Many different organizations like ISO, ISA , IEC, DIN have developed or in the process of developing cyber security standards. Standards help in benchmarking security practices followed & provide a common framework for all stakeholders to

interact & enforce a cyber security program. ISO/IEC 27000 family of standards caters to information security within corporate networks. Even though it is mainly intended for IT environment, many of its concepts like risk assessment, access control etc are applicable to industrial automation & control systems as well. The IEC 62443 standard is being developed specifically for the IACS environment & consists of various parts targeting different stake holders, i.e. asset owner, the system integrator, component providers or manufacturers. Different parts of the standard are in different stages of approval. Refer Figure



8.0 ISSUES OF CONCERN:

Generally, security audit is carried out by a third party auditor, i.e. an agency different from the system supplier or integrator. In India, we have CERT-IN empanelled auditors; but they are for IT security audit. As such, there is a need for security auditors, specialized or having experience in audit of process control domains. Independent bodies like ISA (Delhi section or Bangalore section) can take this initiative & train security auditors to take up jobs in the process control domain. Subsequently, these auditors can be empanelled by CERT-IN.

In such a scenario, the role of the DCS vendors in the security audits increases, especially since some of the mitigation actions like network segmentation or creating a DMZ can be best done by them, being OEMs. Even the end user are more comfortable with OEMs being involved in the cyber security program. By & large, the DCS vendors have responded very effectively to these challenges. In fact, some of these vendors are doing a cyber security assessment service by themselves to end customers. This is very much desirable, but the only challenge is getting a DCS system audited by a different DCS vendor.

Another important concern is the lack of an independent interface of process control or automation engineers with the regulatory bodies. Cyber security being essentially an IT area, the interface usually is handed by the IT department. As detailed in this paper, security in the IACS environment, is a separate niche area in itself. Hence, a need is felt to create an exclusive group in CERT-IN to address this type of security. This is even more important as critical infrastructure in India being always vulnerable, falls in this category.

9.0 CONCLUSION:

Cyber security in the IACS environment needs attention, given the impact it can cause. Defense in depth approach of having multiple

layers of security measures certainly helps particularly when the risk assessment reveals the benefits vis – a vis the investment made. Such an approach is highly recommended for the power industry being highly capital intensive & a critical infrastructure.

10.0 ACKNOWLEDGEMENTS:

The author is extremely grateful to Mrs. Arundhati Bhattacharya, GM(PE-C&I), NTPC for providing constant encouragement for study of this critical subject, realizing its importance in the context of the automation industry .Special thanks are also due to Mr. Chee Ban, cyber security expert from Honeywell, Malaysia for conducting an excellent workshop of cyber security, which reinforced many of the author's beliefs. The author also expresses his gratitude to ISA, Delhi section for providing an opportunity to express the aspects of a cyber security program from the end user perspective & to raise issues of concern to the automation community.

Cyber Security for Automation Systems in the Power Industry and Global Best Practices

Sarosh Muncherji, Sr. Security Consultant
Industrial IT Solutions, Honeywell Process Solutions

ABSTRACT

Process automation systems are increasingly based on open industry standards to facilitate interoperability and integration at lower costs. Increasing interconnection among control systems and exposure to the Internet increase the risk of cyber attacks and malware infections within critical control servers and workstations with potential widespread and disastrous consequences to the power grid, critical infrastructure and consumers. A robust cyber security program mitigates the risks by reducing exposure and deploying defense in depth cyber security controls.

KEYWORDS

Industrial Control System, Plant Control Network, cyber security, FERC, NERC CIP, compliance management, defense in depth.

INTRODUCTION

Automation systems in the power industry have evolved over decades from hard-wired relays to contemporary Industrial Control Systems (ICS) that can easily manage multiple geographically distant sites from a single control center that could be hundreds or thousands of kilometers away from the sites. Advances in several technologies have fueled the growth of automation. These include:

- Controllers have evolved from hardwired relays to versatile Programmable Logic Controllers (PLCs) that are networked using standard Ethernet and TCP/IP.
- Remote Terminal Units (RTUs) that are connected over Wide Area Networks (WANs) using standard communications protocols to facilitate remote monitoring and control.
- Input / Output (I/O) devices from being hardwired using proprietary protocols to devices that communicate wirelessly.
- Standard desktop and server computers that have flexible communications capabilities.
- Advances in software for process monitoring and control, data exchange and analysis and process optimization.
- Significant advances in electronic communications speeds and capabilities that promote interoperability and integration.

Presented at POWAT-2013, New Delhi, India; http://www.isa.org

GROWTH OF ICS

The late 1980s and early 1990s saw widespread deployment of TCP/IP worldwide for private and public networks. The mid 1990s saw explosive growth of the Internet. Corporations rapidly deployed the new network technologies to implement business applications such as World Wide Web publishing, email and Wide Area Networks to connect multiple remote sites with faster and more reliable communications links.

Inter-connections of Plant Control Networks (PCNs) were not limited to monitoring and control functions. Plant performance data that was generated by the ICS and associated systems was required by corporate functions in Operations, Engineering, IT and other departments. Thus PCNs were connected directly to the business networks to unlock the potential of this data. Operations managers could now view plant operations in real-time. Engineering had access to the plant performance data and devices to enable them to manage devices remotely. Gateways were opened up to the outside world for vendors of hardware, software and services to be able to easily connect to the PCN remotely to monitor and tune system performance, apply software updates and provide remote engineering services.

These achievements were accomplished without proper foresight of the potential security vulnerabilities that these inter-connections would expose the ICS to. Process control data and systems had traditionally operated on proprietary protocols and existed within isolated networks, hence there was very little, if any, thought given to the potential dangers these critical networks were now exposed to. Early generations of control systems and devices were not designed with high security. These low security features included:

- Well known default user names that could not be changed or were not changed. Inability to assign individual user names. Widespread use of shared user accounts.
- Default passwords that are never changed or are simple and well known to many persons. Passwords are often written down and kept in plain sight of the device.
- Unencrypted communications on the network.
- Large flat networks that allowed anyone on the network to access all devices.
- Visibility of sensitive control systems devices on the Internet.
- Absence of monitoring tools to log activities on devices and on the network.
- Software or firmware vulnerabilities that can be remotely exploited.
- Backdoors left by vendors for remote access.

EVOLUTION OF MALICIOUS SOFTWARE (MALWARE)

The growth of networks and the Internet corresponded with the emergence of malware. The late 1980s and early 1990s saw the emergence of the early PC viruses that were often mildly annoying and sometimes destructive, for example, overwriting the File Allocation Table or the boot sector of a hard drive. The period between 1999 and 2001 saw the evolution of viruses and worms that targeted Microsoft Windows and spread rapidly over the Internet and caused damage to millions of computers worldwide. The most famous of these were Melissa, LoveLetter, Code Red and Win32/Nimda. The cleanup costs are estimated to have been in the billions of dollars. [1]

These malware exploited the vulnerabilities that existed in popular software and made people conscious of the social impact of such attacks on their personal lives. Multiple attack vectors were

crafted to increase the rate of propagation of worms over networks. For example, The Win32/Nimda worm used five different infection vectors:

- Via email
- Via open network shares
- Via browsing of compromised web sites
- Exploitation of Microsoft IIS 4.0 / 5.0 vulnerabilities
- Via back doors left behind by the Code Red II worm

This early malware established that unprotected computers could be compromised in a number of ways that included social engineering. The intent of this generation of malware ranged from being mildly annoying to highly disruptive.

2004 saw malware that sought to make profits for its creators or for others by stealing information from affected users that could be sold, blackmailing users through "ransomware" or forcing pop-up ads. This era also saw the spread of botnets – networks of computers that have been infected and are under the secret control of attackers who issue commands to them to perform illegitimate activities without their owners' knowledge or consent. These include sending spam, stealing information, spreading malware and attacking other computers and networks through Denial of Service (DoS) attacks.

2010 saw the first of the most advanced malware developed to date that was created specifically for espionage and sabotage. These include Stuxnet, DuQu, Flame, Red October, Shamoon and others. Stuxnet demonstrated that control systems could be compromised to cause targeted sabotage of equipment. Flame is one of the most advanced espionage malware seen to date. It hijacked valid digital signatures and had the ability to record audio, screenshots, Skype conversations and keyboard and network activity. It could also turn an infected computer into a Bluetooth beacon that attempted to download contact information from nearby Bluetooth devices.

IMPACT OF LOSS OF POWER

Electrical power is the lifeblood of our public and private infrastructure and we take it for granted that it is always there. Consider the impact of the loss of power in the following selected areas:

- Home
    - Comfort: no heating, cooling or lighting
    - Kitchen: no oven, microwave or stove
    - Entertainment: no TV or radio
    - Communications: no cordless phones, no computer, no Internet
- Transportation
    - Chaos on streets because of inoperable traffic lights
    - Railways are crippled
    - Aircraft are grounded
- Economy
    - Shops and businesses close down
    - Short supply of food and other essentials
    - Loss of income

The largest blackouts in the past 60 years [2] have cumulatively affected over 1 billion people, with over half the number affected in a single incident in India in 2012.

Year / Location	People affected (m)	Location	Date
July 2012 India blackout	670	India	30–31 July 2012
2005 Java–Bali blackout	100	Indonesia	18 Aug 2005
1999 Southern Brazil blackout	97	Brazil	11 March 1999
2009 Brazil and Paraguay blackout	87	Brazil, Paraguay	10–11 Nov 2009
2003 Italy blackout	55	Italy, Switzerland, Austria, Slovenia, Croatia	28 Sep 2003
2003 US Northeast blackout	55	United States, Canada	14–15 Aug 2003
1965 US Northeast blackout	30	United States, Canada	9 Nov 1965

Thus we see the potential for significant disruption to large populations through the loss of this single critical infrastructure.

THREATS TO THE INDUSTRY

The energy industry worldwide is being warned of impending cyber threats. Recent headlines:

‘Cyber version of Pearl harbor’ looms over energy industry

Cyberattacks a global threat to energy industry

Cyber Threats to Energy Sector Happening at ‘Alarming Rate’

While these may sound overly melodramatic, similar to the media hype of Y2K just over a decade ago, there are significant vulnerabilities in the power infrastructure that are under real threats with potentially disastrous consequences.

Most power generation plants operating today have been installed in the second half of the last century. Recognition of cyber vulnerabilities and the need for protection of assets through cyber security is relatively recent, growing steadily through the 1990s. Given the long operational life of power infrastructure and significant capital expenses of upgrades, it is unsurprising that utilities are

reluctant to replace their control hardware and software systems unless required by business imperatives.

Some of the well-known vulnerabilities in control systems are:

USER ACCOUNTS

Older field devices and software were often shipped with default user accounts such as Administrator, Admin, Manager, Supervisor and Operator. These were usually hard coded into the firmware or application and could not be changed. It is relatively easy for an attacker to find the names of these accounts by doing a quick search on the Internet. Once the account name is known and remote access to the device is available, a brute force attack can be launched on the device to determine the password.

PASSWORDS

There are multiple issues associated with passwords.

- Many devices do not allow adequately long or complex passwords and often rely on simple 4 digit passwords that can be easily cracked.
- Default passwords are shipped with products and these passwords are not changed at all.
- Passwords are simple and obvious, such as ‘admin’.
- Passwords are written down and kept in plain view on monitors or in the same cabinet as the device.
- Passwords are not changed frequently, often because of the sheer logistics of changing the passwords on all devices over multiple distant sites.
- Passwords are transmitted from HMIs and Operator stations to devices over networks in plain text, with no encryption and are easily intercepted and discovered through simple network sniffing.

NETWORK DESIGN

Inter-networking multiple remote sites such as generation plants and substations provided significant benefits:

- Remote monitoring and control through Supervisory Control and Data Acquisition (SCADA) systems
- Reduced manpower or unmanned operations at remote sites
- Reduced travel time and costs through remote troubleshooting and engineering services

The early days of networking were focussed only on providing connectivity with little or no security concerns in the belief ‘security through obscurity’. After all, these were highly specialized devices and very few persons had the expertise to access and manage them. Besides, reliability of plant operations and management was a higher priority than security.

Thus the networks that provided all the above benefits also introduced new vulnerabilities if not securely designed, exposing potentially huge threat surfaces.

- Flat networks throughout the organization with a single addressing scheme for control system networks and corporate networks with little or no segregation of critical networks. This allowed anyone anywhere in the organization to access potentially unsecured devices.
- Exposure of control systems to the Internet through connectivity to the corporate network. A doctoral dissertation in 2011 by Eireann P. Leverett of the University of Cambridge describes the use of the SHODAN search engine to uncover industrial control systems connected to the Internet. He discovered over 10,000 connected devices. However, he did not investigate further to establish if any of these were related to critical infrastructure [3].
- Perimeter-only defense was believed to be adequate to keep attackers away. This ignored threat vectors posed by insiders and social engineering.

MONITORING

Continuous monitoring of all devices and systems is considered good practice for early detection of attacks. This is a well established standard for contemporary software and devices. Older devices lack the capability to monitor and log events such as unauthorized connection events and thus fall into a security blind spot.

VULNERABILITIES IN SOFTWARE AND PRACTICES

Software vulnerability is a weakness in the code or configuration of software that allows an attacker to compromise the software and possibly exploit it maliciously.

Several studies and tests have been conducted on industrial control systems to assess vulnerabilities in the software and in practices. A report in 2011 [4] by the United States Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) highlights specific vulnerabilities in ICS software code, configuration and networks.

Category	Common Vulnerability
Improper input validation	Buffer overflow Command injection Cross-site scripting Path traversal
Permissions, privileges and access controls	Improper access control (authorization) Incorrect default permissions
Improper authentication	Channel accessible by non-endpoint (man in the middle)
Insufficient verification of data authenticity	Cross-site request forgery Missing support for integrity check Download of code without integrity check
Indicator of poor code quality	NULL pointer reference
ICS software security configuration and maintenance	Poor patch management Improper security configuration
Credentials management	Insufficiently protected credentials Use of hard-coded credentials Weak password policies

Table 1: Summary of common ICS software security weaknesses

Category	Common Vulnerability
Permissions, privileges and access controls	Poor system access controls Open network shares on ICS hosts Improper security configuration
Improper authentication	Poor system identification / authentication controls
Credentials management	Weak password policies Insufficiently protected credentials
ICS software security configuration and maintenance	Weak testing environments Poor patch management Weak backup and restore abilities
Planning / policy / procedures	Insufficient security documentation Poor security documentation maintenance
Audit and accountability (event monitoring)	Lack of security audits / assessments Lack of logging or poor logging practices

Table 2: Summary of common ICS configuration weaknesses

Category	**Common Vulnerability**
Network design	No security perimeter defined Lack of network segmentation Lack of functional demilitarized zones (DMZs) Firewall bypassed
Weak firewall rules	Access to specific ports on host not restricted to required IP addresses Firewall rules are not tailored to ICS traffic
Network component configuration	Network devices not properly configured Port security not implemented on network equipment
Audit and accountability	Network architecture not well understood Weak enforcement of remote login policies Weak control of incoming and outgoing media Insufficient methods for monitoring control network events

Table 3: Summary of common ICS network weaknesses

Software vulnerabilities are published in the Common Vulnerabilities and Exposures (CVE) database and alerts are issued by US-CERT.

DEFENCE STRATEGIES

The threat landscape has grown considerably over the past two decades. Interconnections of ICS with business systems, stagnant technology, lack of understanding of security controls, absence of

security policies and reluctance to update systems, all contribute to the ever expanding threat surface and increasing cyber attacks on the energy sector.

A defense-in-depth strategy is recommended to combat this growing threat. This strategy is based on a holistic approach to understanding risk and creating specific defense mechanisms to strengthen the cyber security posture of an organization.

Figure 1shows an overview of an industrial control system with a defense-in-depth architecture [5].

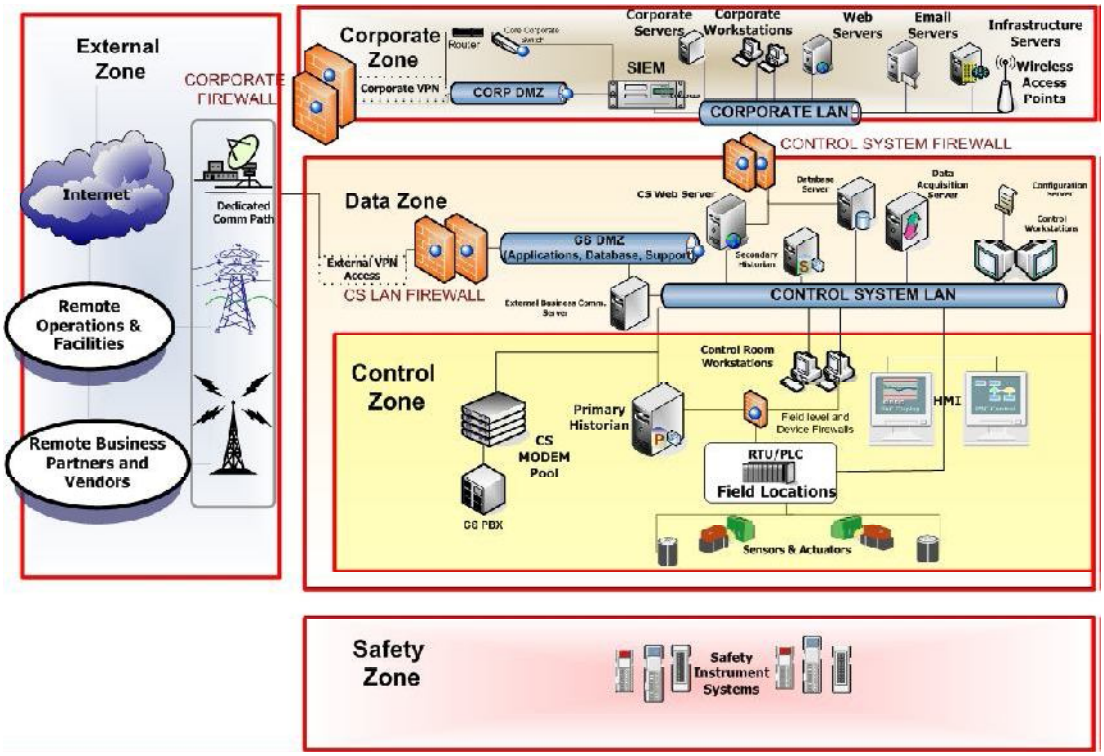


Figure 1: Defense-in-depth architecture

A defense-in-depth strategy encompasses management, operational and technical controls.

MANAGEMENT AND OPERATIONAL CONTROLS

- A clear cyber security policy that is communicated throughout the organization.
- Personnel risk assessment that includes background criminal checks.
- Cyber security awareness and training throughout the organization.
- Electronic and physical access procedures.
- Strict physical access controls to cyber assets with adequate monitoring and alarm facilities.
- A comprehensive configuration and change management program with separation of duties to ensure that all changes to cyber assets are authorized and are traceable.
- A security organization that has well established lines of communication within the business at all levels as required for protection of the cyber assets.
- A well-defined incident management plan that is exercised periodically.
- Supply chain management controls to ensure the integrity of software and devices before deployment in an operational environment.

- Periodic reviews of all management and technical controls to ensure compliance with the security policy.

TECHNICAL CONTROLS

- Identification of all affected cyber assets. This must include servers, workstations, portable computing devices, network equipment, modems, RTUs, PLCs, controllers, instruments and analyzers, etc.
- Perimeter defense at all network boundaries to monitor and control all inbound and outbound traffic and to allow only authorized connections required for operations.
- Network defense within all networks to monitor and analyze network traffic, detect unauthorized connections and disable unused ports.
- Strong identification and authentication controls for access to all devices where feasible.
- Strong access controls to ensure that access privileges to devices, programs and data are provided only as required for the business function. Access privilege levels to be commensurate with the business function.
- Each host and device to be hardened to remove or disable all unnecessary programs, services and communications capabilities.
- Strict controls on the use of portable media within sensitive networks.
- Host protection through intrusion detection, antivirus and whitelisting applications.
- Network intrusion detection and prevention systems to quickly detect and if possible, block attacks.
- All security related events such as logons, use of privileges and unauthorized and failed attempts at access to be logged to a central log server.
- Security Information and Event Management systems to manage event information and logs, analyze and correlate information from multiple sources and alert security personnel to anomalous behaviour.
- A robust patch management program to ensure that all hosts and devices are updated with security patches where feasible without adversely impacting operations.
- Comprehensive test procedures and a test environment that mirrors the operating environment for testing all patches and updates before rolling out to production.
- Backup and restore plans for all cyber assets. Plans to be exercised at least annually.

It may not be possible to deploy some of these technical controls as they may have an adverse impact on operations and may compromise safety. In such cases compensating controls may be deployed with a clear understanding of the associated risks.

CYBER SECURITY FRAMEWORKS

A comprehensive cyber security framework is one that adopts a defense-in-depth strategy to help assure security of cyber assets at all levels.

ISA/IEC-62443 (formerly ISA-99) is ongoing work to establish a set of standards, recommended practices, technical reports, and related information that will define procedures for implementing electronically secure manufacturing and control systems and security practices and assessing electronic security performance. Guidance is directed towards those responsible for designing,

implementing, or managing manufacturing and control systems and shall also apply to users, system integrators, security practitioners, and control systems manufacturers and vendors. [6]

ISO/IEC 27002:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 27002:2005 contains best practices of control objectives and controls in multiple areas of information security management. [7]

NERC CIP-002-3 – CIP-009-3 [8] standards for critical infrastructure protection are a mandatory regulatory requirement for electric utilities in the United States and Canada that meet the eligibility criteria.

NIST Special Publication 800-53 rev3, "Guide for Assessing the Security Controls in Federal Information Systems" [9], is a comprehensive framework of management and technical controls recommended by the National Institute of Standards and Technology for federal information systems in the US. Standards are grouped in the following families and classified as Technical, Operational or Management controls:

- AC - Access Control (Technical)
- AT – Awareness and Training (Operational)
- AU – Audit and Accountability (Technical)
- CA – Security Assessment and Authorization (Management)
- CM – Configuration Management (Operational)
- CP – Contingency Planning (Operational)
- IA – Identification and Authentication
- IR – Incident Response (Operational)
- MA – Maintenance (Operational)
- MP – Media Protection
- PE – Physical and Environmental Protection (Operational)
- PL – Planning (Management)
- PS – Personnel Security (Operational)
- RA – Risk Assessment (Management)
- SA – Systems and Services Acquisition (Management)
- SC – System and Communications Protection (Technical)
- SI – System and Information Integrity (Operational)

THE NORTH AMERICAN MODEL

The 2003 Northeast blackout in the United States and Canada led to the Federal Energy Regulatory Commission (FERC) being authorized to regulate the electric utility industry. The North American Electric Reliability Corporation (NERC) was mandated by FERC to be the Electric Reliability Organization (ERO) to develop standards and audit compliance under the regulation. The NERC Critical Infrastructure Protection (CIP) family of cyber security standards was approved as Version 1 in 2008 and is currently in Version 3. These standards are applicable to generation and transmission entities that meet the qualifying criteria.

The standards specify a wide range of policy, procedure, management and technical topics that need to be addressed by the utilities. These include:

- CIP-002-3: Critical Cyber Asset Identification
- CIP-003-3: Security Management Controls
- CIP-004-3: Personnel and Training
- CIP-005-3: Electronic Security Perimeter
- CIP-006-3: Physical Security of Critical Cyber Assets
- CIP-007-3: Systems Security Management
- CIP-008-3: Incident Reporting and Response Planning
- CIP-009-3: Recovery Plans for Critical Cyber Assets

The United States and Canada are divided into 9 regions that each has a Regional Entity that is responsible for compliance enforcement of the standards. Utilities are audited periodically by their Regional Entity for compliance to the standards.

ROADMAP TO A CYBER SECURITY PROGRAM

Implementation of an effective cyber security program requires rigorous methodology and execution. The methodology outlined below has been used effectively at several utilities.

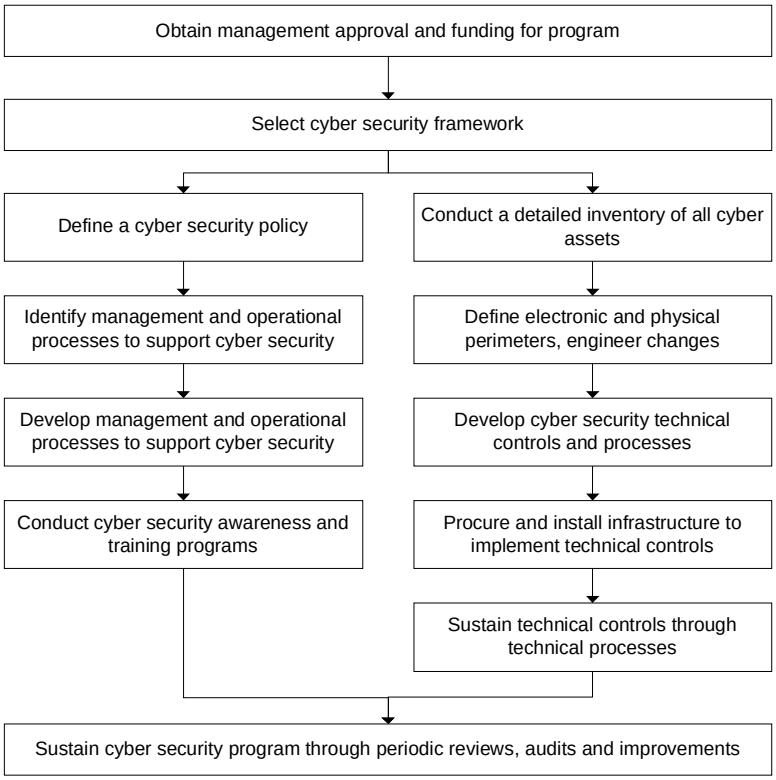


Figure 2: Overview of methodology to implement a cyber security program

CONCLUSION

This paper outlines the modernization of industrial control systems and the parallel evolution of malware and cyber attacks on the energy sector. A defense-in-depth strategy is recommended to strengthen the security posture of the utility. A methodology is outlined to facilitate planning and implementation of an effective cyber security program.

REFERENCES

1. Microsoft Security Intelligence Report: The evolution of malware and the threat landscape – a 10-year review, Microsoft, Feb 2012.
2. http://en.wikipedia.org/wiki/List_of_power_outages.
3. Quantitatively Assessing and Visualising Industrial System Attack Surfaces, Eireann P. Leverett, June 2011.
4. Common Cybersecurity Vulnerabilities in Industrial Control Systems, United States Department of Homeland Security, May 2011.
5. Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies, US Department of Homeland Security, Oct 2009.
6. http://www.isa.org
7. http://www.iso.org
8. http://www.nerc.com
9. http://csrc.nist.gov/publications/PubsSPs.html

Sarosh Muncherji was born in Jamshedpur, India. He graduated in Mechanical engineering from the National Institute of Technology, Rourkela. He joined the Information Technology Services of Tata Steel in Jamshedpur in 1983 and worked there for 21 years. He moved to Vancouver in Canada in 2005where he now lives and works as a security consultant with Honeywell Process Solutions, actively involved with the cyber security programs of electric utilities in Canada and the United States.

Glimpses of POWAT – 2012,

Power Automation Technology Event, Conference and Exhibition held on 13th & 14th January'2012 in Hotel "The Grand", Vasant Kunj, Nelson Mandela Road, New Delhi

A mega Technical Conference and Exhibition, **POWAT – 2012,** Conference and Exhibition on Power Automation Technology Coal based Thermal Power Plant, Gas based GTG Power Plant, Nuclear Power Plant Industries Domain was organized by ISA-Delhi Section in Hotel "The Grand", Vasant Kunj, Nelson Mandela Road, New Delhi on 13th and 14th January'2012. The event was graced by Chief Patron and Guest of Honour **Shri D. K. Jain, Director Technical, National Thermal Power Corporation,** Guest of Honour **Dr. M Ravi Kanth – C&MD-Projects & Development India Ltd.,** Guest of Honour **Shri Y S Mayya – C&MD-ECIL, Shri Ravi Kapoor – Head EPC, Thermal, LANCO Infratech,** ISA members from various parts of India & globe and esteemed guests from various industries.

D. K. Jain, Director Technical, NTPC and Dr. M Ravi Kanth – C&MD-PDIL lighting the lamps during inaugural session

Shri Alok Shrivastava, ISA-D President and Shri Ravi Kapoor, Head EPC, LANCO Infratech during their welcome address and keynote speech.

Shri D.K. Jain, Chief Guest addressing audience and Dr. M. Ravi Kanth, Guest of Honour addressing our esteemed audience and veterans from Instrumentation and Control Industry.

Technical session started with invited papers in Session-1 (in Day-1) on **"Power Spectrum"** by eminent speakers from reputed power industries on topics with **Session Chair Shri Sharad Anand, ED Engineering, NTPC and Session Co-Chair Shri Ganpatiraman, ED-BHEL-EDN**

- I&C for Safety of Nuclear Power Plants, by Shri A. K. Chandra, ED (C&I, E, R&D-ES), NPCIL, Mumbai.
- Optimisation for thermal Power Plants, by Shri Sai Kumar, DGM-BHEL EDN-Bangalore.

Shri A.K. Chandra, ED (C&I), NPCIL **Shri Sai Kumar from BHEL-EDN**

Session-2 started on Subject **"Automation in Thermal Power Plants"** with Session Chair Shri Ajit Kumar – GM-Nuclear- NTPC, and Session Co-chair Shri K R Bhardwaj – AGM-HOD-C&I- PEM BHEL. Following were the most useful topics for power industry:

- Volume measurement using 3D Technology by Mr. Motti Holler – PM Automation Solutions Ltd., Tel-Aviv, Israel.
- Microwave Blade Tip Sensing – Capabilities for Turbine Operators by Mr. Scott Billington , Mr. Michael Hafner and Mr. Tom Holst from Megitt Sensing Systems,Switzerland.

- Hazardous Area Classification and Methods of preventing fire and explosion hazards in Gas and Coal based Thermal Power Plants by Shri Ashok Panda, Shri Nikhilesh Kumar and Soumya from LANCO Infratech Ltd.
- Particulate Emission Monitoring by using Triboelectric Technology by Mr. Karl EhrstrÖm, CEO-SINTROL Oy, Finland and Vikram Singh Area Sales Manager (India)

Mr. Motti Holler during his lecture

Shri Ashok Panda from LANCO

Mr. Karl EhrstrÖm, CEO-SINTROL Oy, Finland.

Mr. Ravi Malik, I&C lead "Origin Energy"

Session 3 started with the subject "Automation Solution in Combined Cycle Power Plants" and this session was chaired by Mrs. Arundhati Bhattacharya, GM PE-C&I, NTPC along with session co-chair Shri Siddharth Ghosal, Director GE Energy. Following were the topics in this session which enlightened our audiences with Automation Solutions in Power Plants:

- Remote Operations and Monitoring of Origin Power Station and Managing Security of Control Systems by Mr. Ravi Malik, I&C lead "Origin Energy" Australia.
- Output loss Analysis – A tool to monitor Real time performance losses of a CCGT power station by Mr. Diwakar Kaushik and Vinay Pratap Singh, NTPC ERP.
- Reducing uncertainty in Fuel gas Measurement by Mass Spectrometry by Mr. Peter J traynor and Dr. Robert G Wright from Thermofisher Scientific, Sugar Land Texas and from Thermofisher Scientific from Winsford, Cheshire, UK.
- Greenhouse Gas Emissions Reporting – Combined Cycle Power Plant by Shri VVV Prakash and Shri Kalluri Anjaneyulu from Bechtel India Pvt. Ltd.

Mr. Diwakar Kaushik during his lecture and receiving memento from Mrs. Arundhati Bhattacharya

Mr. Peter J Traynor

Shri VVV Prakash

Mr. Prasenjit Pal and Mr. P. Sengupta from NTPC conducting the Quiz Competition

"Automation in Nuclear Power Plants" was the 1st technical sessions of day-2 and the session was chaired by Shri R.C. Dhup – ED-NTPC, Mumbai with Session Co-Chair Shri V.P. Raman – Director, Mottmac, Mumbai. Following burning topics were discussed by various eminent technocrats from NPCIL:

- Radiation Monitoring System in Nuclear Power Plants, by Shri Vinayak B, Shri N P Panchal, Shri N S Kaintura

- Fuel handling Controls in Presurised Heavy Water Reactors by Shri Nitin Rimza, Shri S Bandopadhyay, Mr. Joe Peter K, Shri P Nagabhushana, Shri M Bharathkumar, Shri K Agiladaeswari
- Power Control Requirements, Instruments and Techniques for Indian PHWRs by Shri Thangapandi, Shri Sujit Chattopadhyaya, Shri R Balasubramanian
- Reactor Control and Protection Systems of VVER-1000 by Shri Kamlesh Nathani, Mrs Nabanita Pyne and Shri S K Sen

Shri N S Kaintura of NPCIL

Shri Nitin Rimza of NPCIL

Shri Sujit Chattopadhyay from NPCIL

Mrs. Nabanita Pyne from NPCIL

"Automation Advancement in Various Field including Transmission and Distribution" was the subject in Session-5 with Session Chair Shri Y K Sehgal, ED Power Grid Corporation and Session Co-Chair Shri Shirish Chandra, Yokogawa, India. Following eminent specialists shared their experiences on the various subjects:

- Edifying the Smart Future of Power Utilities by Analysing the Concept of Generation Side of Virtual Power by Mrs. Saroj Chelluri DGM (PE-Elect), Amit Kulshreshtha DGM(PE-Mech) and Prasenjit Pal DGM and STA to D(T), NTPC

- Application of Foundation Fieldbus and DART Technology in Power Plants by Shri Arasu Thanigai, Business Development Manager, P&F Singapore
- Power to Control the Process Control by Ms Anuja Thukral, Phoenix Contact (India)
- Implementation of BOP PLC Standardization and BOP Network at Rosa Power Plant by Viswanathan Kumar from Reliance Infrastructure Ltd., Noida (India)

Mrs. Saroj Chelluri from NTPC

Shri Arasu Thanigai from P&F

Ms Anuja Thukral from Phoenix

Shri Viswanathan Kumar from Reliance

Safe and efficient operation of a plant is the motive of an operator and Plant Assets are very important for any industry. Post Lunch Session of Day-2 with Session Chair Shri N K Shrivastava-GM R&M, and Session Co-Chair Shri Pankaj Bhartiya, GM Cen-PEEP, NTPC Ltd. started on subject "Plant Asset Management" Technical experts on the said subject appraised the audiences with their experience and knowledge.

- Fleet optimization through real time Enterprise Integration by Shri Shekhar Kamath from OSI Soft.
- Effective Planning of Resources and Monitoring Overhaul Preparedness through ERP, Shri Anand Prakash & Shri Vinay Pratap Singh from NTPC ERP.

- Development of Automation Mechanism for inspection of power plant components in critical areas by Kishore Aggarwal, Badri Vishal Gupta and Rakesh Kumar Chakraborty, NTPC NETRA
- Advance Vibration Analysis & Diagnosis System For Power Plant Rotary Machine – It saves Cost and Increase Up-Time, by Shri Mukesh Vyas – Div Head – India Forbes Marshall Pvt. Ltd. – Shinkawa VMS System
- Monitoring Plant Assets using optimum selection of Technology and Methodology by Pankaj Kumar Sharma, Sr. Service Manager, GE India Industrial Pvt. Ltd. (Div. Bently Nevada)

Plant Asset Management – Presentation Team

Shri Shekhar Kamath of OSI Soft

Shri Anand Prakash from NTPC

Shri Kishore Aggarwal from NTPC NETRA

Shri Mukesh Vyas of Forbes Marshall

Mr. Pankaj Kumar Sharma, GE India

The whole world is now looking for source of energy which causes less pollution and this reminds us of Hydro Power Plant and Solar Power Generation solution. Topic of Technical Session -7 was the most burning subject "Automation in Hydro Power and Renewable Power Solution". The Session Chair was Shri A.K. Gupta, GM (Business development) NTPC Ltd. and Session Co-Chair was Shri Ramani Iyer, Forbes Marshall Ltd. Following experts from Power Sector in this renewable energy field explained how technology development is increasing the efficiency and operation of hydro Power Plants and Solar Power Plants.

- Latest technologies of Field Instrumentation, Data Collection and Reporting for Dams and Related Structures, **by Shri V. K. Rastogi from Encardio-rite Electronics Pvt. Ltd., Lucknow, India.**

- Two Axis Solar Tracking System, by **Shri S.P.S. Pundir, Shri Rakesh Swami, Shri Vishal Singh from NTPC NETRA**

Solar Thermal Power Plants – An. Overview of Automation, by Shri Ramesh Kasinath, ABB India

Shri Vishal Singh

Shri Ramesh Kasinatha

The last Technical Session of this POWAT-2012 was **"Panel discussion on Challenges of Rapid Obsolescence in Automation System and Valedictory Session". The Session was chaired by Shri S. P. Singh, Director (HR)-NTPC,** eminent technocrats and experts from different sectors of industries Shri Vinod Sharma- CEO- Meja Urja Nigam Pvt. Ltd., Shri Pankaj Bhartiya, GM-NTPC, Shri Shirish Chandra – Yokogawa India Ltd., Shri Rajeev Sharma – Alstom

Power were part of this panel discussion along with Panel Secretary and Technical Coordinator POWAT-2012 Shri Soumitra Bhattacharya. This Panel discussion was subject of interests for all the participants and audiences. Panel members explained various queries and curiosity of participants.

Shri Soumitra Bhattacharya

Shri S. P. Singh, Director (HR)-NTPC

Shri Soumitra Bhattacharya, Technical Coordinator, POWAT-2012 invited the Chair-person Shri S. P. Singh, Director (HR)-NTPC and all the participants for the Panel Discussion on Challenges of Rapid Obsolescence in Automation System and Valedictory Session.

Shri Vinod Sharma during Panel Discussion

Shri Shirish Chandra during Panel Discussion

Shri Pankaj Bhartiya, during Panel Discussion

Shri Rajeev Sharma during Panel Discussion

Shri S P Singh presented token of appreciation for best paper presentation to Mr. Motti Holler from PM Automation Solutions Ltd., Tel Aviv, Israel and Mr. Nitin Rimza from NPCIL, Mumbai.• Latest technologies of Field Instrumentation, Data Collection and Reporting for Dams and Related Structures, **by Shri V. K. Rastogi from Encardio-rite Electronics Pvt. Ltd., Lucknow, India.**

- Two Axis Solar Tracking System, by **Shri S.P.S. Pundir, Shri Rakesh Swami, Shri Vishal Singh from NTPC NETRA**

Solar Thermal Power Plants – An. Overview of Automation, by Shri Ramesh Kasinath, ABB India

Shri S P Singh presenting Blackberry to Guests winning lucky Dip Draw and token of appreciation to young ISA-D Student member for their contribution to ISA-D POWAT-2012

This mega event concluded with gala networking dinner with all esteemed guests and members and heartfelt memorable moments.

Notes

Notes

ECIL

The only multi- technology company that provides

Total Systems Solutions

Serving the needs of verticals of National Importance like Atomic Energy, Defence, Aerospace, Instrumentation & Security and IT & e-Governance

Committed to Self-Reliance

Offers: Control & Automation Equipment, Computer based Systems, Communication Systems, Antenna Systems, Encryption and Networking Systems, Integrated Security Solutions, Electronic Energy Meters, Electronic Voting Machines, e-Governance Solutions and more.

Electronics Corporation of India Limited

A Government of India Enterprise

(Department of Atomic Energy)

Hyderabad - 500 062

web: www.ecil.co.in E-mail: cbdg@ecil.co.in

NOT ONLY DO WE GENERATE POWER, WE ALSO EMPOWER LIVES.

Socio-economic development of the project area is a key component of our CSR policy. We are engaged in improving and creating infrastructure like roads, drainage, public toilets, health services, schools, electrification along with skill upgradation of people in and around our projects.

We are committed to generating power in an environmentally sustainable and socially responsive manner. Environmental Impact Assessment is an essential part of the project planning. Based on the findings of the EIA study, suitable Environment Management Plans are prepared and implemented, to alleviate or nullify any negative impact on environment due to setting up of a new hydroelectric project in an area.

Resettlement & Rehabilitation | Infrastructure Developement | Drinking Water | Health Services | Electrification | Education | Skill Upgradation | ITI Courses | Afforestation | Ash Utilisation