ISA Delhi Section

एनटीपीसी NTPC
A Maharatna Company

"CYBER SECURITY"
(Defence in Depth Approach)

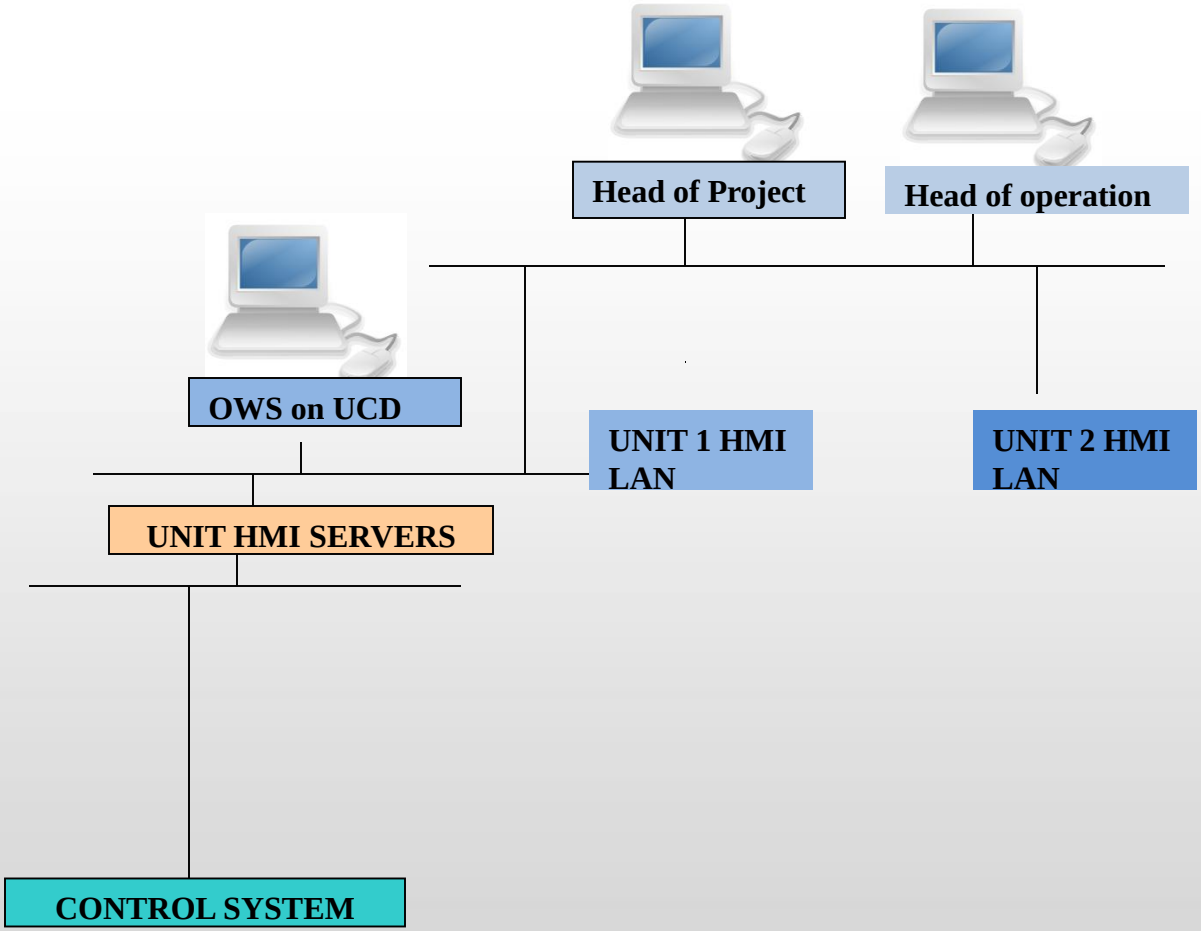
Technical Presentation
by

Mr. R. Sarangapani
&
Mr. Amit Kumar Singh
(NTPC-Ltd)

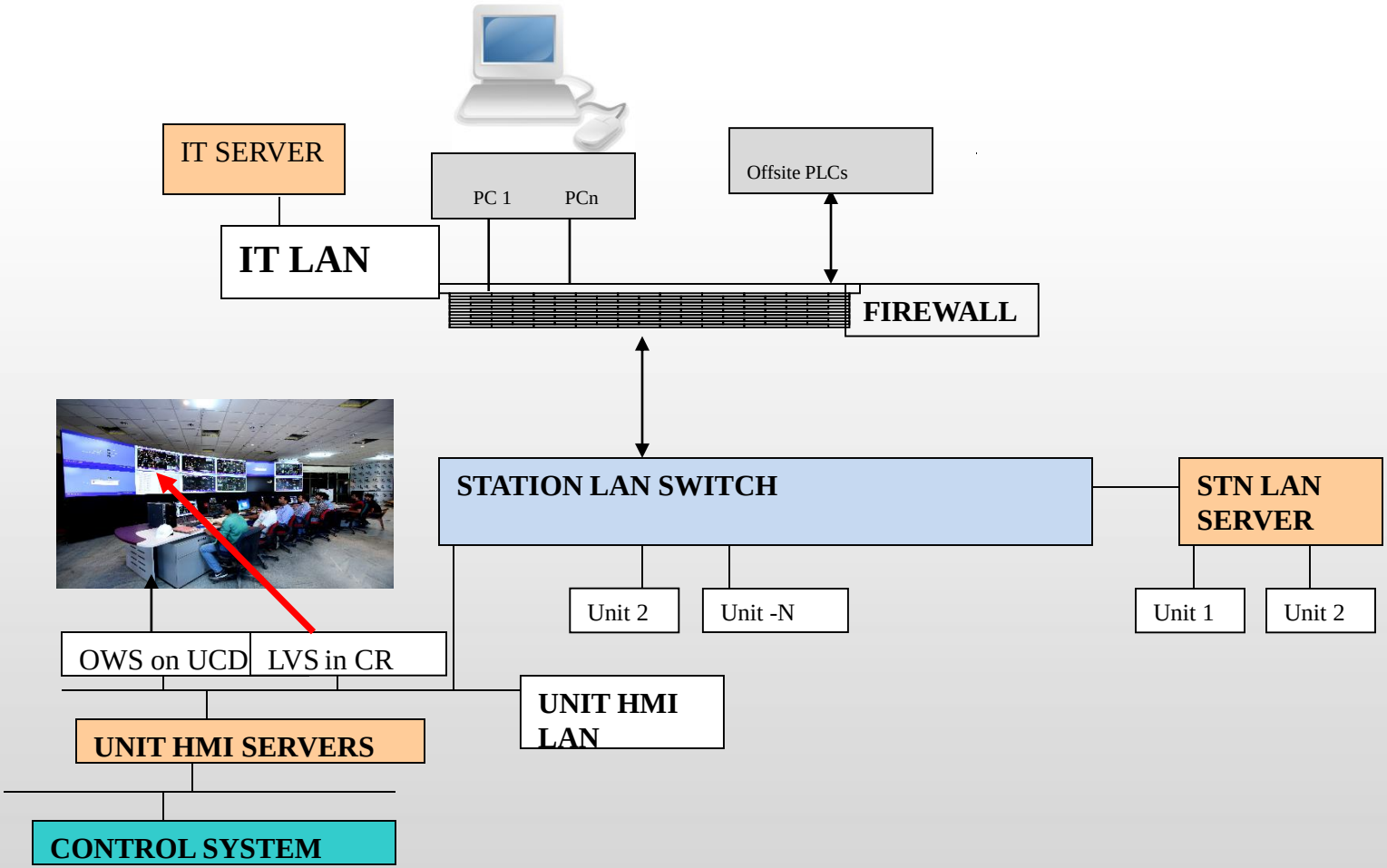
Presentation Agenda

- Networking in Distributed Control Systems & significant changes.
- Targeted attacks & Major Security threats
- Cyber Security of DCS in NTPC
- Security Policy & Procedures
- Security Audit
- Security Standards
- Areas addressed by standards
- Vendor Certification
- Best Practices
- Issues facing our industry
- End user concerns

Networking in DCS- The scenario before….



The scenario thereafter….



ISA Delhi Section

A Maharatna Company

Significant Changes

- Windows Operating system entered DCS
- Use of Commercial off the shelf (COTS) hardware/ software in DCS
- Open architecture (Use of commercial network protocols)
- Continuous connection with enterprise network for real time data of DCS
- Inclusion of Wireless network connectivity for distant offsite DCS connectivity

But these are some of the associated by-products..

- Virus
- Worms
- Trojan Horse
- Denial of Service (DOS) Attacks & DDOS(Distributed Denial of Services)
- Phishing & Spear phishing
- Pharming

Targeted Attacks & APT

- Targeted attacks are defined as the attacks which are destined to target a particular organization
- APT –Advanced –use of full spectrum of computer intrusion technologies and techniques. Combine multiple attack methodologies and tools in order to reach and compromise their target
- Persistent –priority to a specific task, rather than opportunistically seeking immediate financial gain
- Threat – means that there is a level of coordinated human involvement in the attack

Trend

- There is growing trend of compromise to DCS/SCADA systems, including Human Machine Interface (HMI), historians, and other connected devices.
- This trend has manifested itself in two major ways:

  i) Malware disguised as valid DCS/SCADA applications

  ii) Malware used to scan and identify specific DCS/SCADA port/services

Cyber attacks on Automation Systems do not just result in production downtimes but can compromise equipment & human safety

ISA Delhi Section

एनटीपीसी NTPC A Maharatna Company

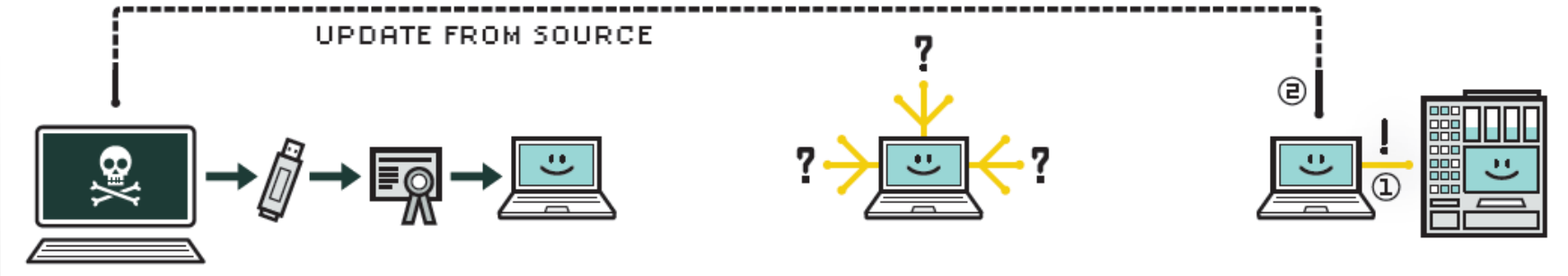
Some major security incidents in Process Control domain…

- Sewage plant in Australia hacked releasing millions of liters of sewage
- Davis-Besse nuclear power plant safety monitoring system disabled
- Browns Ferry nuclear plant shutdown for two days because of excessive control bus network traffic
- 13 US auto plants shut down by an Internet worm named Zotob
- Brazil's electrical grid attacked via the Internet
- Stuxnet hit Siemens control system in Iran Nuclear plant July 2010
- Crouching YETI
- Ukraine Power grid was shutdown due to Black energy Malware
- And many more….

Stuxnet

- Stuxnet targeted specific installations in Iran associated with Uranium enrichment facility.
- Only 10 initial targets
- Resulting in over 14k infections
- Malware Targeted for a **Specific type of PLC** having a **Specific Configuration**
- It installs malware into memory block DB890 of the PLC that monitors the Profibus messaging bus of the system.
- When certain criteria are met, it periodically modifies the frequency to 1410 Hz and then to 2 Hz and then to 1064 Hz, and thus affects the operation of the connected motors by changing their rotational speed.
- It also installs a rootkit that hides the malware on the system and masks the changes in rotational speed from monitoring systems.

Process Flow of Stuxnet attack



- **1. Infection**

Entered into a system

(Stuxnet via USB)

- **2. Search**

Check whether a given machine is part of the targeted industrial control system

- **3. Update**

If the system isn't a target then do nothing.

If its is, then attempt to access the internet and download a more recent version of itself (upgrade)

ISA Delhi Section

A Maharatna Company

Process Flow of Stuxnet attack: Contd.

- **4. Compromise**

Compromise the target system by exploiting vulnerabilities

(Stuxnet- Zero day vulnerabilities; software weakness that haven't been identified by security experts)

- **5. Control**

Take control of industrial control system

(Stuxnet- Centrifuges- making them spin themselves to failure)

- **6. Deceive & Destroy**

Provide false feedback to outside world

Destroy the intended target

Energetic Bear / Crouching Yeti

- It uses highly-effective and newly-formed malware known as “Havex” to break into the industrial control system (ICS)/SCADA systems of their targeted companies.

- The Havex malware infects a company’s ICS, it then relays sensitive company data and information back to the hackers through the command-and-control (C&C) servers.

- ICS-CERT testing has determined that the Havex payload has caused multiple common OPC platforms to intermittently crash i.e. Denial of service effect on applications reliant on OPC communications.

Energetic Bear / Crouching Yeti

- APT campaign since 2010, 2800+ victims world wide.
- Spreading via

  a)Emails with exploit

  b)Infected legitimate web sites (Watering hole)

  c)Infected (repacked) legitimate installation packages(hosted on vendor's website).
- Contains a number of different Trojans, backdoors and exploit packs
- It Compromised Legitimate web sites as Control centers

  Example:"eWon" –Belgium SCADA software ,"MB Connect LineGmbH" –PLC remote control software,"MESA Imaging AG"– super speed 3D cameras and sensors manufacturer (Switzerland)

  List of ports used by Havex in order to discover OPC:
  - 502- Modbus
  - 102 & 44818 PLC exploits

Black Energy(BE) Malware Ukraine Attack:A Short case study

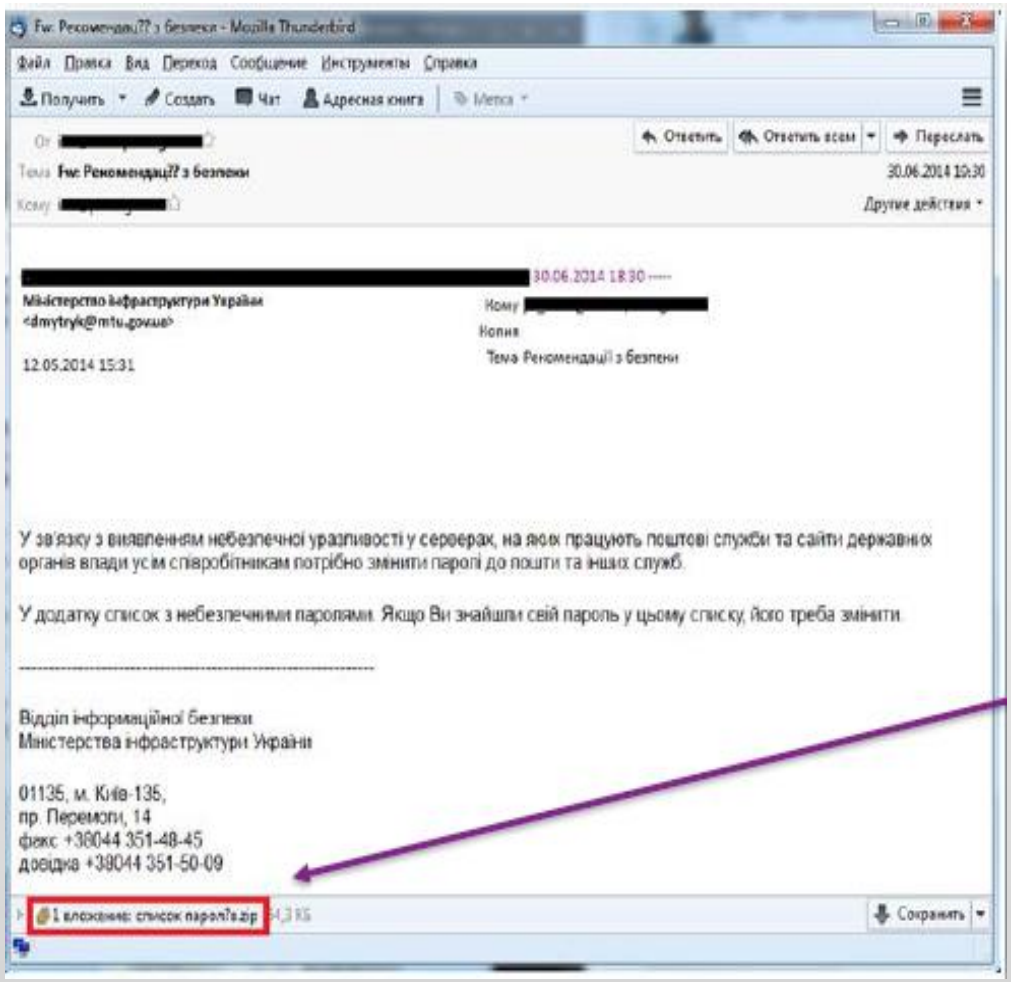
- In 2013, Attackers of BE began deploying SCADA-related plugins to victims in the ICS and energy sectors around the World
- Since middle of 2014, one of the preferred attack vectors for BE in Ukraine has been Excel documents with macros.
- 23 Dec 2015 –massive attack against Ukrainian Power Grid .Thousands of power substations were shutdown for up to 8 hours on West and Central Ukraine. On Dec. 23, 2015, three regional Ukrainian electricity distribution suffered power outages due to a cyber attack
- Hackers disabled operation remote control and switched power off Substation control was switched to manual for weeks.
- 80,000 consumers were w/o energy for at least 6 hours
- No SCADA control until January 9 2016.

Black Energy Malware Ukraine Attack Dec 2015:A Short case study

A Multi-vector attack

- Use of social engineering & spear-phishing to lure operator to open malicious Excel Macro on PC.
- Responders also found a wiper module called “Killdisk” that was used to disable computers.
- At the same time, the attackers overwhelmed utility call centers with automated telephone calls.

Black Energy Malware Ukraine Attack:A Short case study



Spread via Spear-phishing email

Infected attachment contained zip archive with exe file inside

ISA Delhi Section

A Maharatna Company

Can this happen in your plant…

ISA Delhi Section

एनटीपीसी NTPC
A Maharatna Company

Cyber Security of DCS in NTPC

- In terms of Cyber Security of DCS**, NTPC** was the **first company in India among** the **critical infrastructure** category to take Cyber security initiatives
- These initiatives were taken **in 2007** wherein consultancy project was awarded to M/s CMC in 2007-2008
- As part of this Consultancy project, **security audit** was conducted for Stg-II DCS at **Talcher Kaniha in 2007**
- Also **Secured Network Architecture** was evolved as part of this consultancy & incorporated in **specifications** from Bongaigoan onwards **in 2008**. Also, in the on going projects being engineered, this was implemented. This has become a defacto standard among DCS vendors

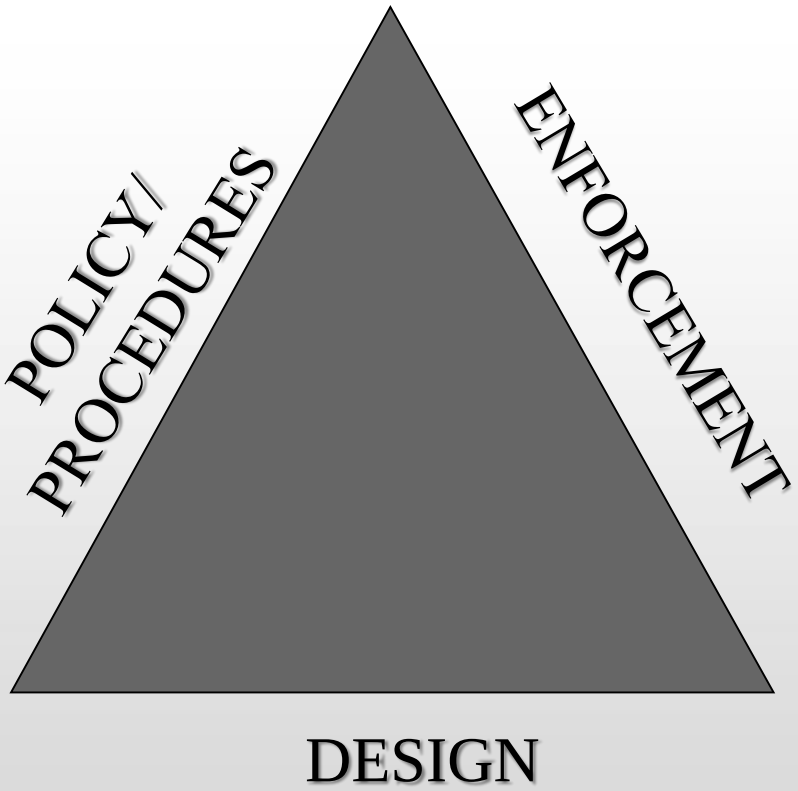
Cyber Security of DCS in NTPC

- Main features of this **architecture** was :
  - **Zone segmentation**- three zones, Internal zone- DCS, External zone- IT/Third party systems & DMZ zone- Station LAN server. Each zone separated through firewall. No communication directly with DCS- only through DMZ
  - **System hardening- No Internet** connection **in DCS, No USBs**, No unnecessary services
  - **Defense in depth** concept- Protocol from External to DMZ different from Protocol from Internal to DMZ. Cracking multiple protocol difficult
  - Firewall with IPS (Intrusion Protection System) at network perimeter & IDS (intrusion detection system) at Switch level

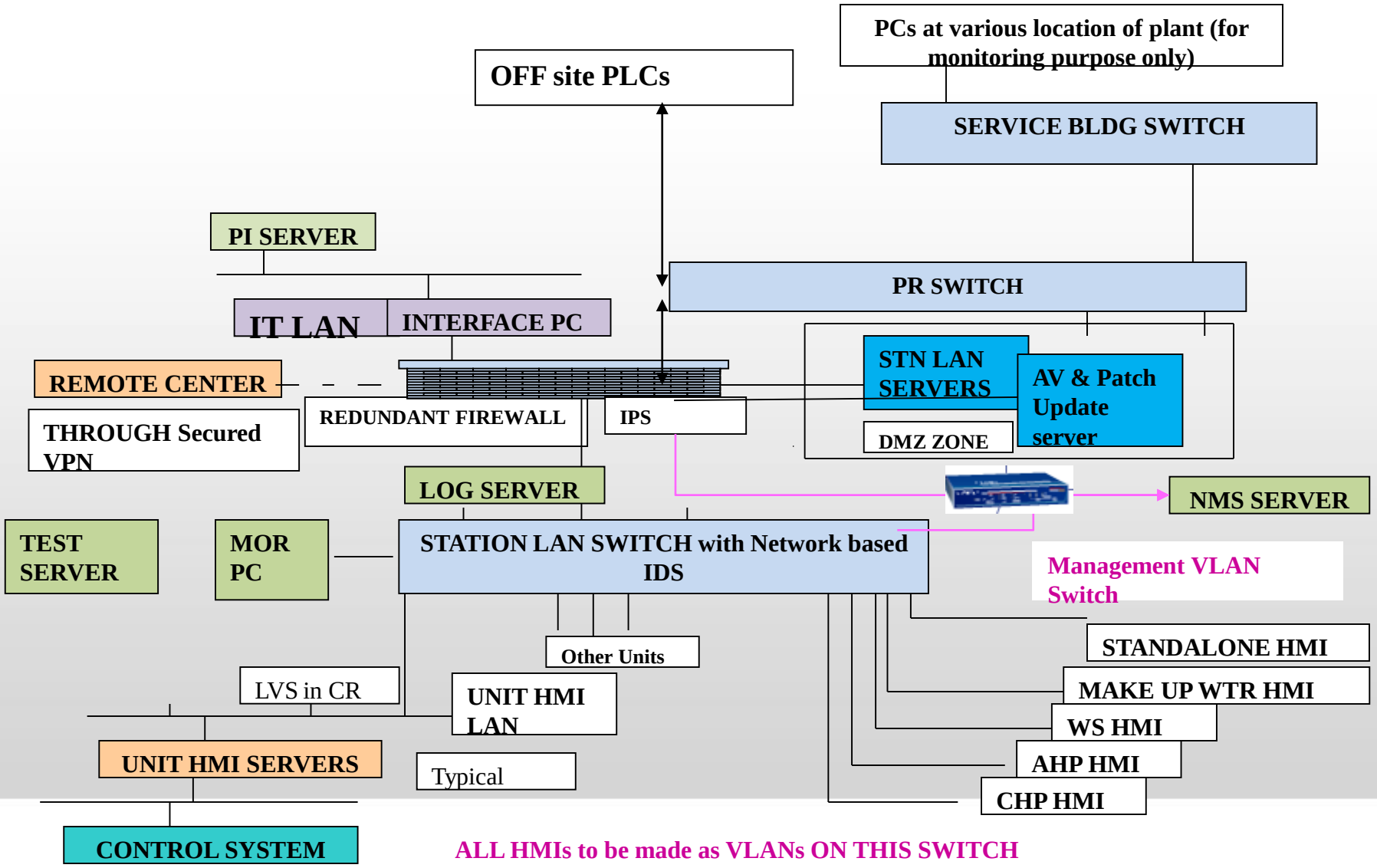
Cyber Security of DCS in NTPC:Contd.

- **Security Policies & procedures** evolved & incorporated in specifications in 2008
  - These policies & procedures **Issued as OGN(** Operation Guidance Note**) by Corp. OS in Dec 2008**
- **Security Audits**
  - Provision of Security audit by CERT-IN certified auditor for DCS introduced from Bongaigoan specs
  - **Security Audit in FAT** introduced from **2012** onwards. Vulnerability assessment & Penetration testing is done by CERT-In certified auditor. **Mitigation measures** suggested by auditor is generally done **before dispatch clearance**
- -Participation in framing of International standards (IEC 62443-2-4) & Indian manual for Cyber Security in Power Systems

Three pillars of DCS security program



Typical Secured System architecture



Components of a DCS security program

- A. ‘Defence in depth’ System architecture
- B. Policies & procedures
- C. Enforcement of A & B (Security Audit)

  -Vulnerability Assessment

  -Penetration testing
- D. Crisis management program
- E. Awareness, Knowledge & Skills

  (for the asset owner)
- F. 24 X 7 Assistance Desk (for large multiple installations)

Security Policies and Procedures

- Foundation of a security program
- Guide for Managers, Security Team & users to understand their specific role within the security framework
- Articulation of overall security objectives providing a management framework

Security Policies and Procedures

- Information Security Team Policy
- Firewall Policy
- Information Identification & Classification policy
- Security Policy Review Policy
- System Planning & Acceptance Policy
- Capacity Management Policy
- Media Handling policy
- Information Security Awareness Policy
- Third Party Access Policy

Security Policies and Procedures Contd..

- Change Control Policy
- Anti Virus Policy
- System Access Policy
- Monitoring Policy
- System Planning & Acceptance Policy
- Incident Handling policy
- Information Backup & Restoration Policy
- Network Access policy
- User access management Policy

Security Audit

- Done by CERT certified auditor as per approved Security Audit procedure.
- Envisaged during PG test & each year of AMC.

Vulnerability Assessment	Penetration Testing
• Identifies and reports noted vulnerabilities and security weaknesses in the target system • The assessment team generally reviews code, settings, etc. for known security weaknesses • The customer may specify the level of vulnerability verification	• A penetration test attempts to duplicate the actions of an attacker • The goal of external penetration testing is to find weaknesses in the company's network that could allow an attacker to access the enterprise environment from the Internet

Findings of Audit reports

Extract from a Security Audit of NTPC DCS

Vulnerability	Affected systems	Impact	Status	Clients Justification
NTP monlistCommand Enabled	10[redacted].51, [redacted].52, [redacted].53, 1[redacted].54,	Medium	Not Fixed	
OpenSSL 'ChangeCipherSpec' MiTM Vulnerability	1[redacted].0	High	Not Fixed	

Observation	Impact	Status	Clients Justification
Telnet service is enabled in IDS and IPS	Medium	Fixed	
Password Policy was not set in IDS and IPS	Medium	Fixed	
SNMP service weak community string in IDS and IPS	Medium	Fixed	
Weak filter rule (Any-Any) in Firewall	Medium	Fixed	
Maximum Password age is set 999 days in Application servers and Thin Clients	Medium	Not Fixed	
Account Lockout Threshold is set 0 invalid logon attempts in Application servers and Thin Clients	Medium	Not Fixed	
Antivirus is Outdated	Medium	Fixed	

CVSS score	NVD severity rating
0.0 – 3.9	Low
4.0 – 6.9	Medium
7.0 – 10.0	High

CVSS score determines level of severity

DCS vendor takes suitable action to remove risks & submit "Risk Mitigation Report"

Based on mitigation report Security Auditor issues certificate to DCS vendor for clearance of Audit

Based on above DCS system & Station LAN system is dispatched.

ISA Delhi Section

A Maharatna Company

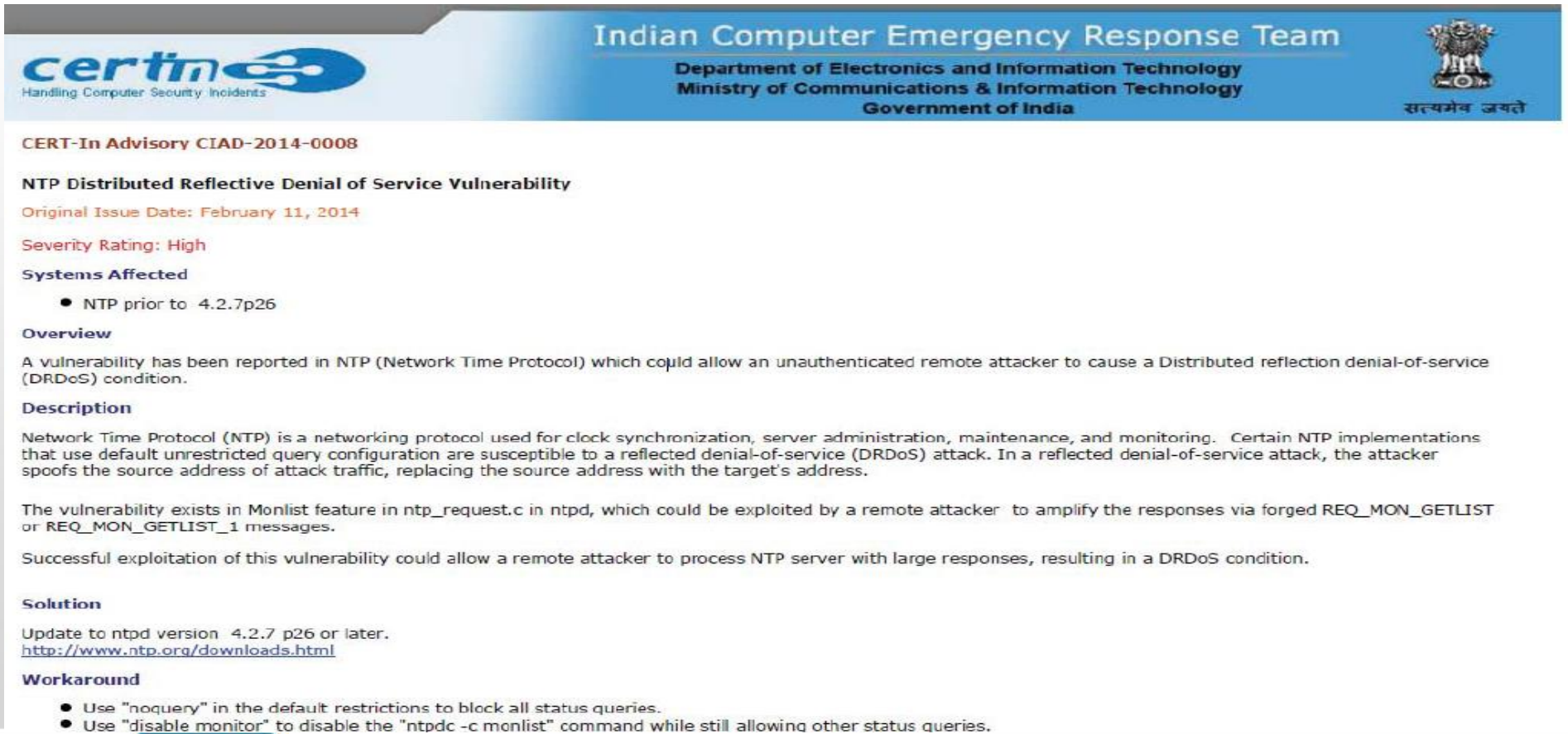
The Heartbleed Bug vulnerability (CVE-2014-0160)

- A serious vulnerability in the popular OpenSSL cryptographic software library.
- SSL/TLS provides communication security and privacy over the Internet for applications such as web, email,IM & VPNs.
- Bug is in the OpenSSL's implementation of the TLS/DTLS (transport layer security protocols).
- It allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. When it is exploited it leads to the leak of memory contents from the server to the client and from the client to
- the server.
- The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software.
- It compromises the secret keys used to identify the service providers and to encrypt
- the traffic, the names and passwords of the users and the actual content.
- This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

Solution: OpenSSL 1.0.1g released on 7th of April 2014 fixes the bug.

NTP Vulnerability

- NTP can be abused to amplify denial-of-service attack traffic.
- The attacker sends a packet with their source address being the IP of a victim. The NTP server replies to this request, but the number of bytes sent in the response is an amplified amount compared to the initial request, resulting in a denial-of-service on the victim.



certin
Handling Computer Security Incidents

Indian Computer Emergency Response Team
Department of Electronics and Information Technology
Ministry of Communications & Information Technology
Government of India

सत्यमेव जयते

CERT-In Advisory CIAD-2014-0008

NTP Distributed Reflective Denial of Service Vulnerability

Original Issue Date: February 11, 2014

Severity Rating: High

Systems Affected

- NTP prior to 4.2.7p26

Overview

A vulnerability has been reported in NTP (Network Time Protocol) which could allow an unauthenticated remote attacker to cause a Distributed reflection denial-of-service (DRDoS) condition.

Description

Network Time Protocol (NTP) is a networking protocol used for clock synchronization, server administration, maintenance, and monitoring. Certain NTP implementations that use default unrestricted query configuration are susceptible to a reflected denial-of-service (DRDoS) attack. In a reflected denial-of-service attack, the attacker spoofs the source address of attack traffic, replacing the source address with the target's address.

The vulnerability exists in Monlist feature in ntp_request.c in ntpd, which could be exploited by a remote attacker to amplify the responses via forged REQ_MON_GETLIST or REQ_MON_GETLIST_1 messages.

Successful exploitation of this vulnerability could allow a remote attacker to process NTP server with large responses, resulting in a DRDoS condition.

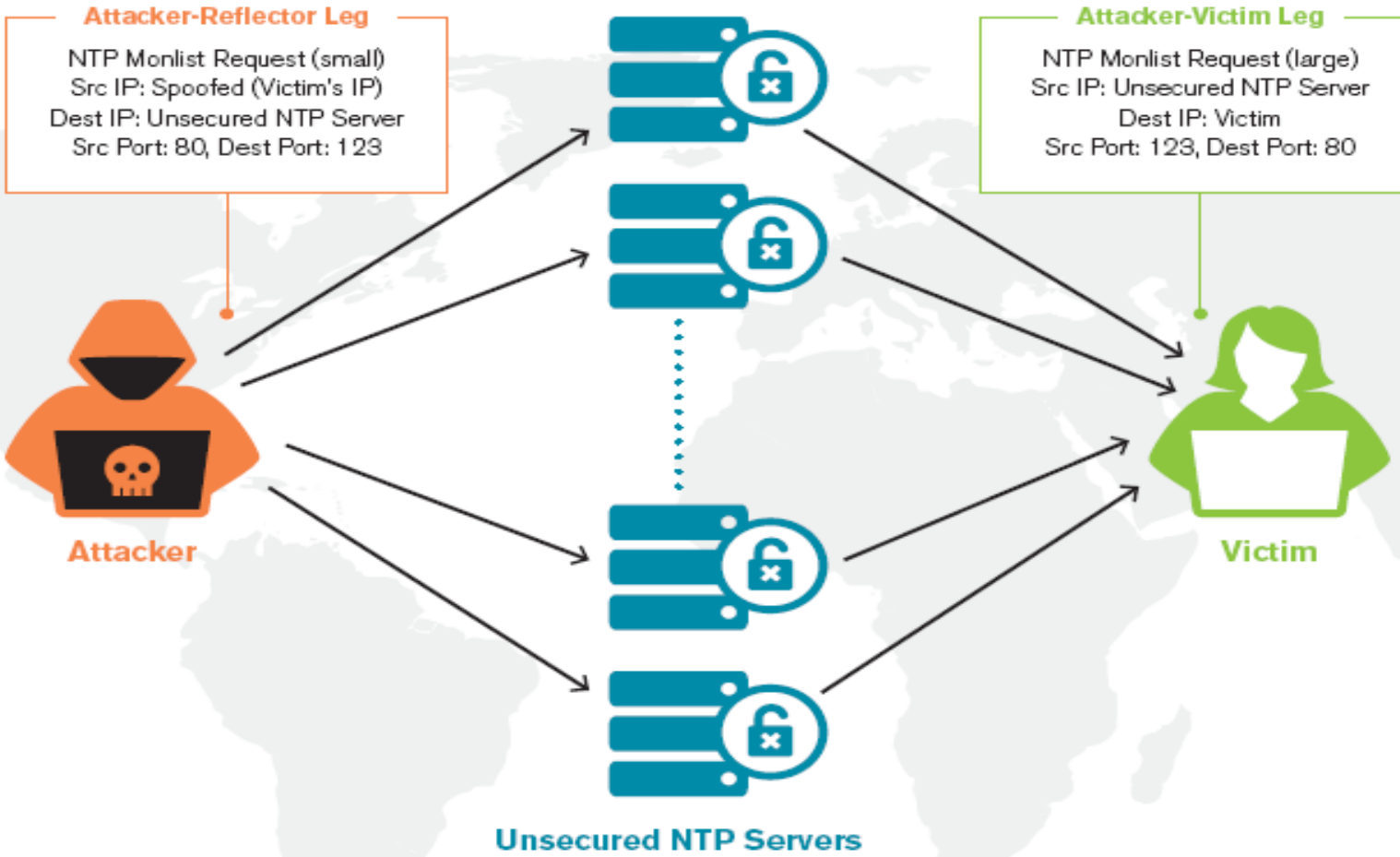
Solution

Update to ntpd version 4.2.7 p26 or later.
http://www.ntp.org/downloads.html

Workaround

- Use "noquery" in the default restrictions to block all status queries.
- Use "disable monitor" to disable the "ntpdc -c monlist" command while still allowing other status queries.

NTP Reflection/Amplification Attack



DCS Cyber Security Standards – How it evolved

- ISO 27000
  - For the information security of any organization
  - Used as a base for developing Cyber Security Standards for Automation Systems
- NERC CIP
  - Essentially for Power Systems
  - Applicable in US
  - SCADA/DCS vendor compliance
- WIB - Security Requirements for Vendors
  - First Standard exclusively for Automation Systems
  - Applicable in Netherlands/ Driven by Shell
  - Very comprehensive & structured

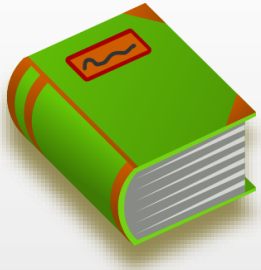
ISA Delhi Section

A Maharatna Company

DCS Security- now a “MUST HAVE” !!

- NIST
  - Framework to serve as guideline for organizations to start a Cyber security program

- Security of DCS Mandated by Standards
  - IEC 62443 –Specific standard for IACS (Industrial Automation & Control System)

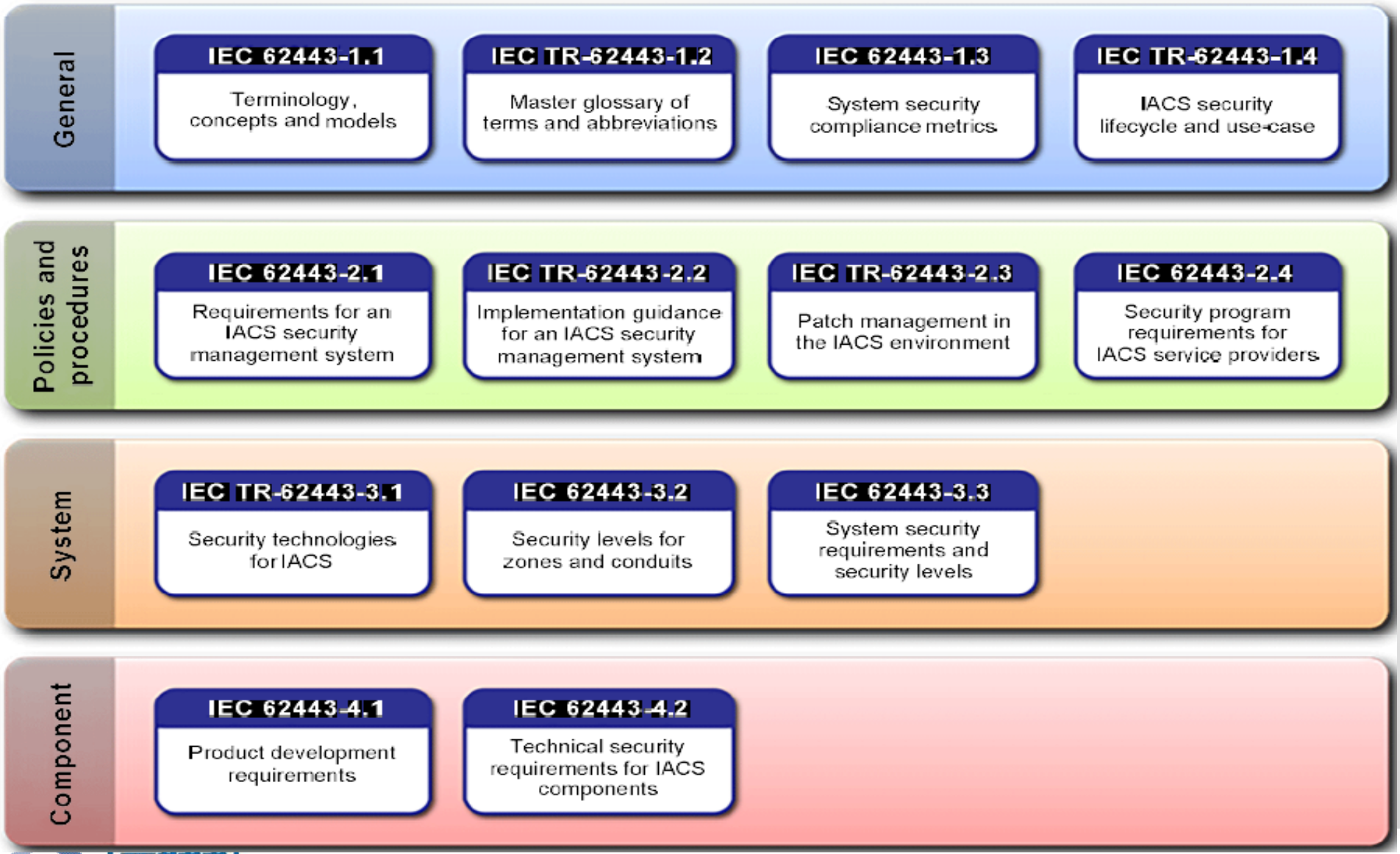


- Indian Manual for Cyber Security in Power Systems
  - Developed on the lines of NERC CIP
  - Final draft with CEA

NERC CIP Standards- Details

CIP-2	BES Cyber System Categorization
CIP-3	Security Management Controls
CIP-4	Personnel & Training
CIP-5	Electronic Security Perimeter
CIP-6	Physical Security
CIP-7	System Security Management
CIP-8	Incident Reporting and Response Planning
CIP-9	Recovery Plans
CIP-10	Conf. Change Mgmt & Vulnerability Assessments
CIP-11	Information Protection

ISA/IEC standards on security



ISA Delhi Section

एनटीपीसी NTPC
A Maharatna Company

Security assurance levels

1. Casual or Coincidental Violation
2. Intentional Violation Using Simple Means
3. Intentional Violation Using Sophisticated Means
4. Intentional Violation Using Sophisticated Means & Extended Resources

Security assurance levels initially proposed

1. LOD (LOSS of DATA)
2. LOV (LOSS of CONTROL)
3. LOV(LOSS of VIEW)
4. LOSS of PROTECTION

ISA Delhi Section

एनटीपीसी NTPC
A Maharatna Company

Some areas being addressed by standards

- SIS (Safety Instrumented system) as a separate entity
- Wireless Connectivity
- Patch management
- Account management
- Remote access
- Data encryption (Cryptography)

Vendor Certification

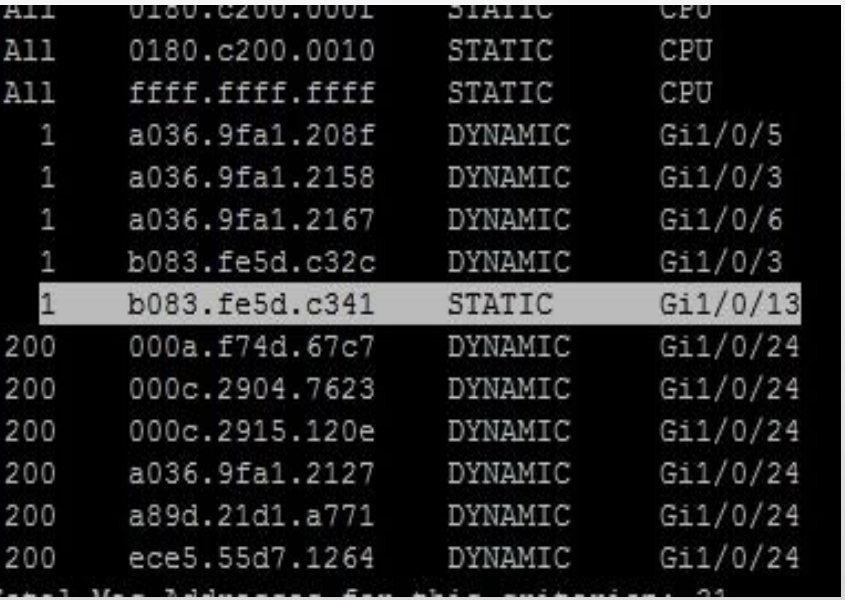
- A mechanism to enforce security in your system without knowing the details
- Best practices on one site gets embedded as system capabilities in the DCS/PLC
- Developments in security technology gets into the process control domain **faster** !!

Best practices

- Using Access Control systems to prevent unauthorized access to secure locations
- Deploy VLANs for traffic separation for coarse grained security
- Use Stateful firewall technology at the port level for fine-grained security
- Place encryption throughout the network to ensure privacy
- Detect threats to the integrity of the network and remediate them
- Applying application whitelisting throughout the ICS environment to prevent unauthorized applications from running
- Use safe browsing practices e.g. Disable Popups, Enable selected Plugins e.g. JS Guard, NoScript, Scriptsafe,
- Enabling a USB lockdown on all SCADA environments. This prevents malware from physically entering the environment
- SNMP should be disabled/blocked on public-facing infrastructure/servers.
- Use ACLs & BGP flowspec in Routers to mitigate DDOS.
- Deploy basic security measures in between network segments, such as firewalls/IPS, in between the business network, and the ICS network.

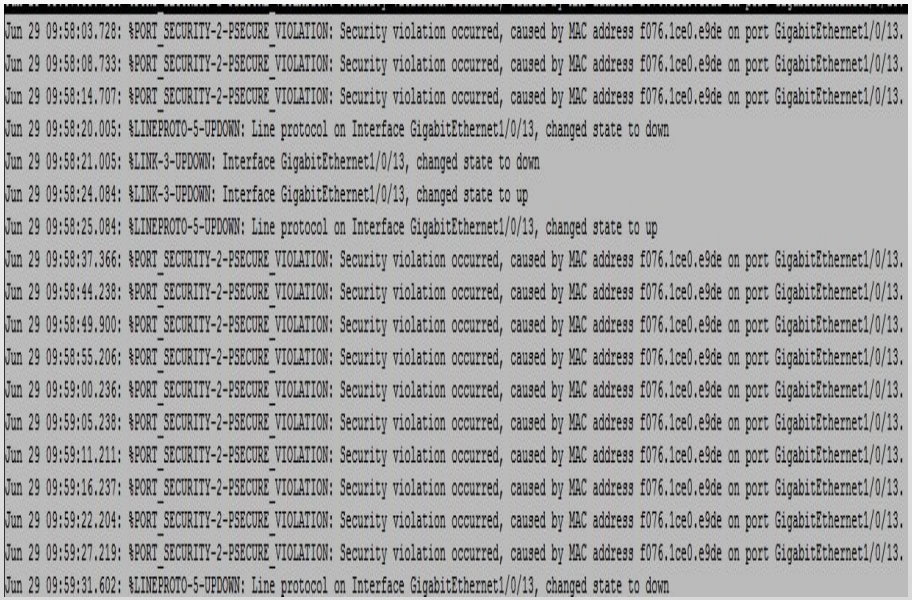
Practices Adopted in NTPC:Mac Binding

- A client IP address is mapped with a MAC address.
- A computer with a specified MAC address can send and receive information only if it uses the associated IP address.



All	0180.c200.0010	STATIC	CPU
All	ffff.ffff.ffff	STATIC	CPU
1	a036.9fa1.208f	DYNAMIC	Gi1/0/5
1	a036.9fa1.2158	DYNAMIC	Gi1/0/3
1	a036.9fa1.2167	DYNAMIC	Gi1/0/6
1	b083.fe5d.c32c	DYNAMIC	Gi1/0/3
1	b083.fe5d.c341	STATIC	Gi1/0/13
200	000a.f74d.67c7	DYNAMIC	Gi1/0/24
200	000c.2904.7623	DYNAMIC	Gi1/0/24
200	000c.2915.120e	DYNAMIC	Gi1/0/24
200	a036.9fa1.2127	DYNAMIC	Gi1/0/24
200	a89d.21d1.a771	DYNAMIC	Gi1/0/24
200	ece5.55d7.1264	DYNAMIC	Gi1/0/24

MAC Binding done on Port 13



```
Jun 29 09:58:03.728: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address f076.1ce0.e9de on port GigabitEthernet1/0/13.
Jun 29 09:58:08.733: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address f076.1ce0.e9de on port GigabitEthernet1/0/13.
Jun 29 09:58:14.707: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address f076.1ce0.e9de on port GigabitEthernet1/0/13.
Jun 29 09:58:20.005: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/13, changed state to down
Jun 29 09:58:21.005: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/13, changed state to down
Jun 29 09:58:24.084: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/13, changed state to up
Jun 29 09:58:25.084: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/13, changed state to up
Jun 29 09:58:37.366: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address f076.1ce0.e9de on port GigabitEthernet1/0/13.
Jun 29 09:58:44.238: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address f076.1ce0.e9de on port GigabitEthernet1/0/13.
Jun 29 09:58:49.900: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address f076.1ce0.e9de on port GigabitEthernet1/0/13.
Jun 29 09:58:55.206: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address f076.1ce0.e9de on port GigabitEthernet1/0/13.
Jun 29 09:59:00.236: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address f076.1ce0.e9de on port GigabitEthernet1/0/13.
Jun 29 09:59:05.238: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address f076.1ce0.e9de on port GigabitEthernet1/0/13.
Jun 29 09:59:11.211: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address f076.1ce0.e9de on port GigabitEthernet1/0/13.
Jun 29 09:59:16.237: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address f076.1ce0.e9de on port GigabitEthernet1/0/13.
Jun 29 09:59:22.204: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address f076.1ce0.e9de on port GigabitEthernet1/0/13.
Jun 29 09:59:27.219: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address f076.1ce0.e9de on port GigabitEthernet1/0/13.
Jun 29 09:59:31.602: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/13, changed state to down
```

Security Violation occurred & port went down when LAPTOP with different MAC connected on same port

ISA Delhi Section

A Maharatna Company

Remote support

For getting Support from OEM through Secured VPN

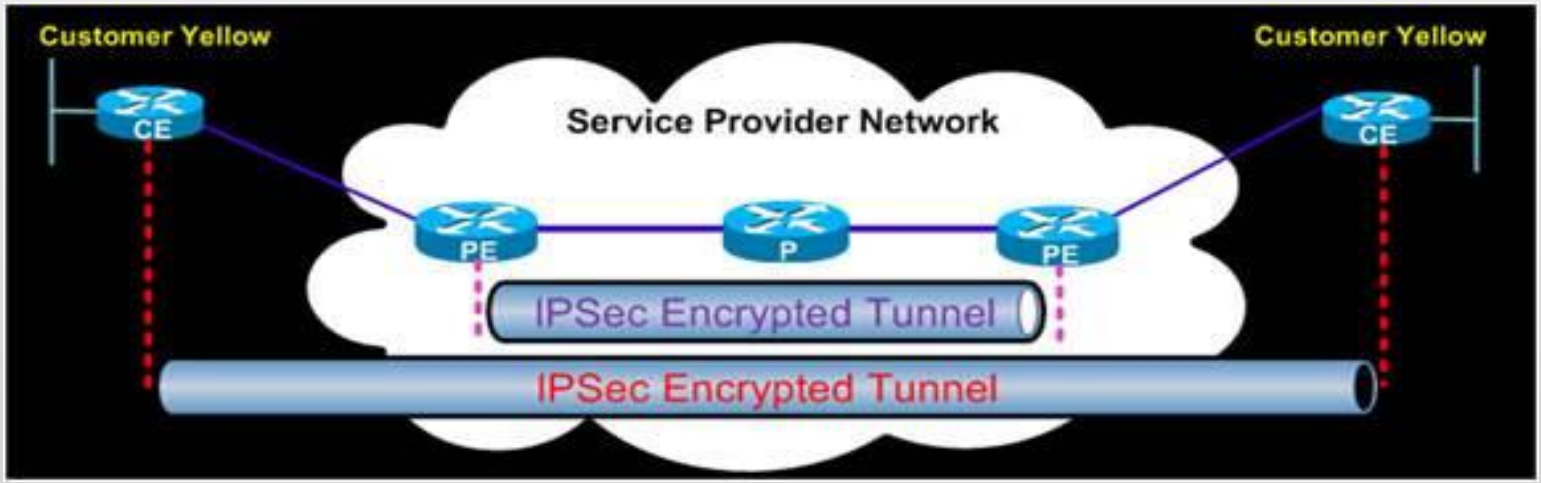
a)using encryption technologies to protect the confidentiality and integrity of communications.

b)using mutual authentication mechanisms to verify the identities of both endpoints.

- **Tunneling** :Secure communications tunnel through which information can be transmitted between networks are typically established through *virtual private network* (VPN) technologies.
- To use a VPN, users must either have the appropriate VPN software on their client devices or be on a network that has a VPN gateway system on it.
- Tunnels can do user authentication, access control (at the host, service, and application levels), and other security functions & it uses cryptography to protect the confidentiality and integrity of the transmitted information between the client device and the VPN gateway.

Security aspects of Communication Network

- Authentication :allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access
- Methods of Tunneling :Internet Protocol Security (IPsec) and Secure Sockets Layer (SSL) tunnels, using Secure Shell (SSH).
- IPsec meets most security goals: authentication, integrity, and confidentiality. IPsec uses encryption, encapsulating an IP packet inside an IPsec packet. De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination



SIS(Safety Instrumented System) Connectivity

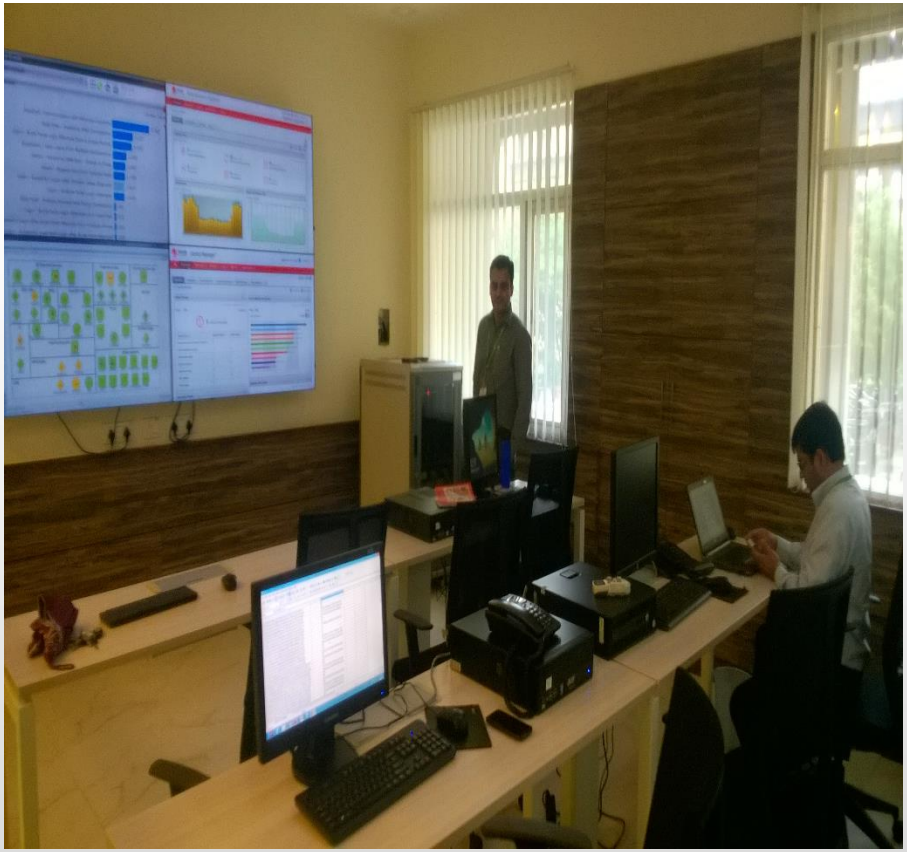
- As per International IEC standard , SIS (Safety Instrumented System) is not connected physically or logically to level 3 or above.
- Purdue reference model as standardized by ISA 95 & IEC 62264-1.
- Communication from level 3 or above to SIS shall pass through network security device.
- Accordingly, connection of SG DCS(having SIS) to BOP DCS is being done through Firewall.
- Further, risk assessment measure & philosophy to prevent Remote access to SIS is to be ensured.

Wireless Security methods

- Common types: Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA).
- WPA2 uses an encryption device that encrypts the network with a 256-bit key; the longer key length improves security over WEP. Replaces RC4 encryption with Advanced Encryption System (AES)
- To implement 802.11i, Router/AP as well as client must support network encryption which can be achieved by integration with RADIUS server.
- Remote Authentication Dial In User Service (RADIUS) is an AAA (authentication, authorization and accounting) protocol used for remote network access .
- Use of WIPS & WIDS is prevalent nowadays.
- However, a growing concept is to use wireless network in DCS in **air gap mode.**

Cyber Security Operation Center-NTPC

- Center for monitoring IT network of NTPC across India.
- All sites LOG server, Firewall, proxies server data is collected & analyzed
- All security violations are monitored & alerted & suitably mitigated by Security Team.
- Incident of Compromise (IOC) released by IN-CERT & NCIIPC are regularly being monitored & firewall rules & signatures (AV & IPS /IDS) are being updated accordingly.



ISA Delhi Section

एनटीपीसी NTPC A Maharatna Company

MACsec

- 802.1AE is the IEEE MAC Security standard (also known as MACsec) which defines connectionless data confidentiality and integrity for media access independent protocols. It is standardized by the IEEE 802.1 working group
- In common with IPsec and SSL, MACsec defines a security infrastructure to provide data confidentiality, Data integrity and Data Origin Authentication.
- By assuring that a frame comes from the station that claimed to send it, MACSec can mitigate attacks on Layer 2 protocols.
- MACsec frame format, which is similar to the Ethernet frame, but includes additional fields: Security Tag, Message Authentication Code, Security Connectivity associations, Security associations, Cipher suite of GCM-AES 128 or 256.

Takeaway Points for a secure ICS

Organizations can employ the following practices to help defend against ICS attacks :

- Review SCADA/ICS security architecture periodically.

- Enhance network security monitoring capability. Robust log collection and network traffic monitoring are the foundational components of a defensible ICS network.
- Search for Indicators of Compromise (IOC).
- Use of automated tools can alert security analysts and process operators when anomalous behavior or ICS-oriented malware.

- Review Incident Response plans.
- Security Audit to be conducted periodically.

Related Issues facing our industry

- Auditors not specialized in process control domain
- No distinction between IT security & process control security
- Interface to regulatory bodies by IT
- Lack of a comprehensive & uniform enforceable standard
- CERT-IN advisories also limited as many incidents are not reported
- Specialized/ Trained manpower

Distinction between IT security & Process Control security

IT Security	Process Control Security
System Response Importance ↓	System response ↑ Importance
Impact ↓	Impact (Can impact critical infrastructure; safety of equipment & personnel) ↑
Skill set ↑	Skill set ↓

End user concerns & Expectations from vendors

- New technology evolvement or new product development should take into account security vulnerabilities at the conceptual stage itself
- Assurance or certification for secure system should come from vendors
- Security of embedded devices should also be included in the above assurance
- High priority to critical infrastructure

Quote

"Security is a journey, not a destination. Peace of mind is the reward."

Source: 2007 Advantage Business Media

THANK YOU