ISA Delhi Section

A Maharatna Company

"CYBER SECURITY STANDARDS for IACS - Trends, Issues and Challenges"

Technical Presentation

by

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

ISA Delhi Section

A Maharatna Company

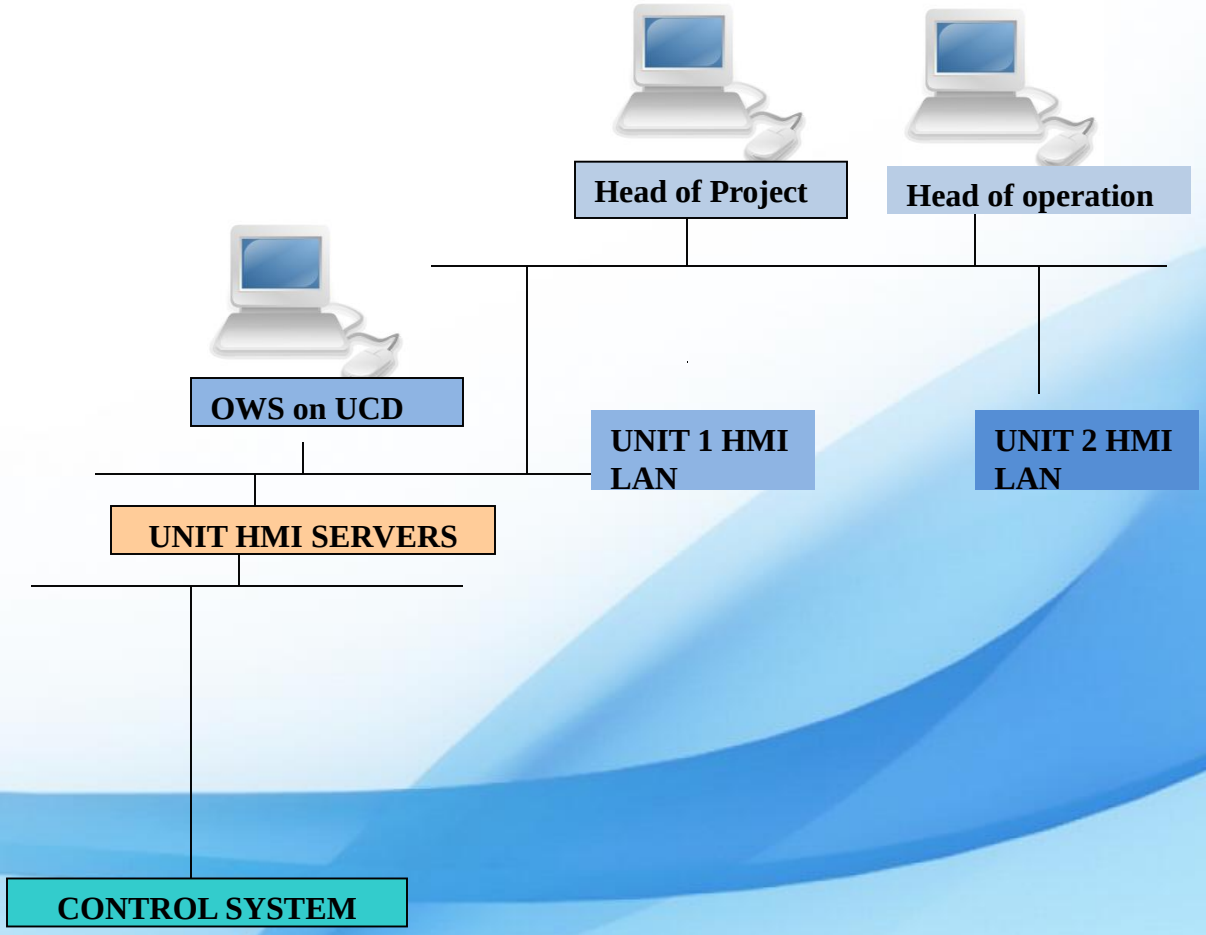
Presentation Agenda

- 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

ISA Delhi Section

एनटीपीसी NTPC A Maharatna Company

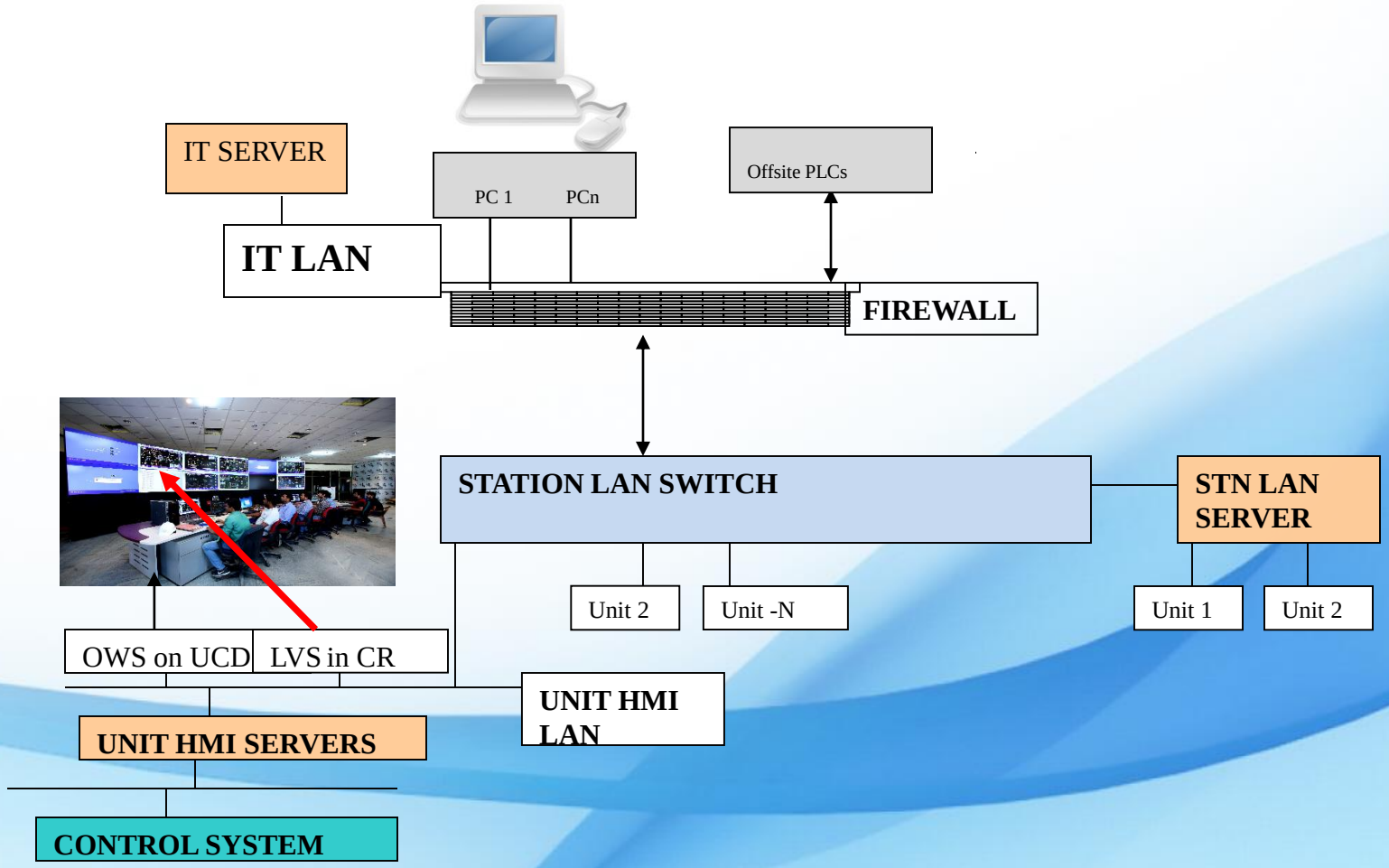
Networking in DCS- The scenario before….



ISA Delhi Section

एनटीपीसी NTPC
A Maharatna Company

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

By 2020, spending on OT security will double due to increasing attacks on critical industrial infrastructure and subsequent regulatory responses.

-Gartner, Market Guide for Operational Technology Security, May 2016.

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

It is important to recognize that while breaches to IT systems raise financial and reputational risk, OT system breaches represent safety and operational risk.

Some major Cyber security incidents

- 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
- Ukraine Power grid was shutdown due to Black energy Malware
- WannaCry, Locky,Petya- Ransomware
- And many more….

ISA Delhi Section

एनटीपीसी NTPC A Maharatna Company

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)

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

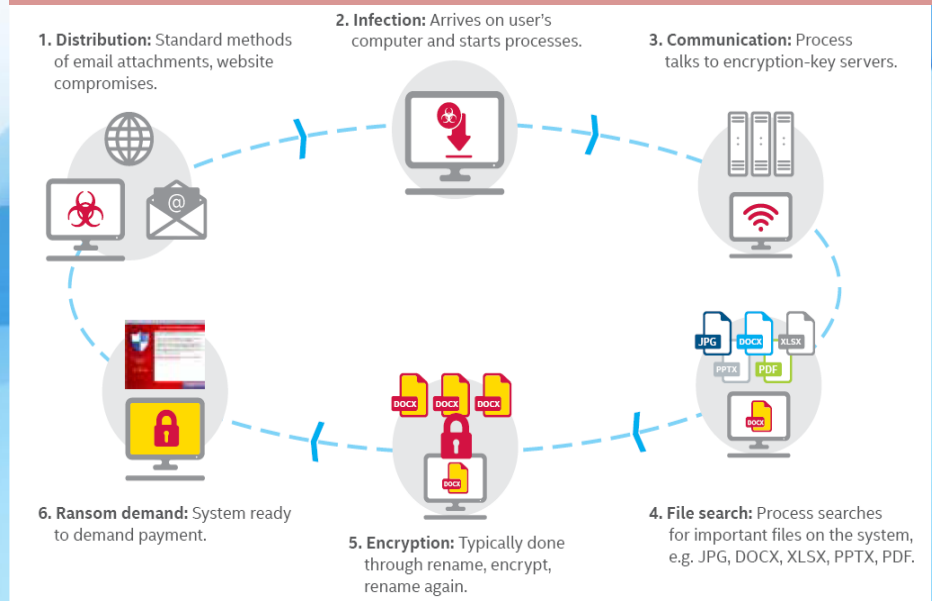
Destroy the intended target

Ransomware: WannaCry

- Ransomware is a malware that encrypts contents on infected systems and demands payment in bit coins.
- Worldwide cyber attack by the **WannaCry**- ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system
- 2 key components – a worm and a ransomware package
- •It spreads laterally between computers on the same LAN by using a vulnerability in implementations of Server Message Block (SMB).
- •This exploit is named as

  ETERNALBLUE.

How Ransomware works



ISA Delhi Section

A Maharatna Company

Ransomware: Locky

- Locky is ransomware malware released in 2016 & was active in 2017, it is delivered by email with an attached Microsoft Word document that contains malicious macros.

Malicious Email with MS word attachment sent to targeted user

↓

On Opening Document it appears Gibberish

↓

Asks User to enable Macro (Which most users do)

↓

Macros then save and run a binary file that downloads the actual Encryption TROJAN

↓

It encrypt files with .locky extension & ask for Ransom in Bitcoin

Measures to prevent Wannacry

- Apply patches to Windows systems as mentioned in Microsoft Security Bulletin MS17-010. For Unsupported Versions such as Windows XP,Vista,Server 2003 etc. patch also available on Microsoft website
- Take Regular backup of Critical Data
- Block SMB ports on Enterprise Edge/perimeter network devices [UDP 137, 138 and TCP 139, 445] or Disable SMBv1.
- Restrict TCP port 445 traffic to where it is absolutely needed using router ACLs
- Use private VLANs if your edge switches support this feature
- Use host based firewalls to limit communication on TCP 445
- Deploy antivirus protection, Block spam
- •Don't open attachments in unsolicited e-mails
- Disable macros in Microsoft Office products.
- •Deploy Application whitelisting.
- •Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses; block these before receiving and downloading messages.

Other Recent incidents

Meltdown and Spectre- January 5, 2018

- Modern computers CPU Vulnerability. It may leak passwords and sensitive data.
- AMD,ARM Intel etc. microprocessor hardware vulnerabilities allow programs to steal data which is currently processed on the computer.
- While programs are typically not permitted to read data from other programs, a malicious program can exploit Meltdown and Spectre to get hold of secrets stored in the memory of other running programs.

Rockwell Automation FactoryTalk Alarms and Events Denial of Service Vulnerability

- CERTIn Vulnerability Note CIVN20180009
- Original Issue Date: **January 15, 2018**
- A vulnerability has been reported in Rockwell Automation Alarms and Events
- An unauthenticated, remote attacker could exploit this vulnerability by submitting specially crafted packets to TCP port 403 to cause the system to crash, resulting in denial of service (DoS) condition.
- Details of above vulnerability & mitigation measures available on CERT-IN website.

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

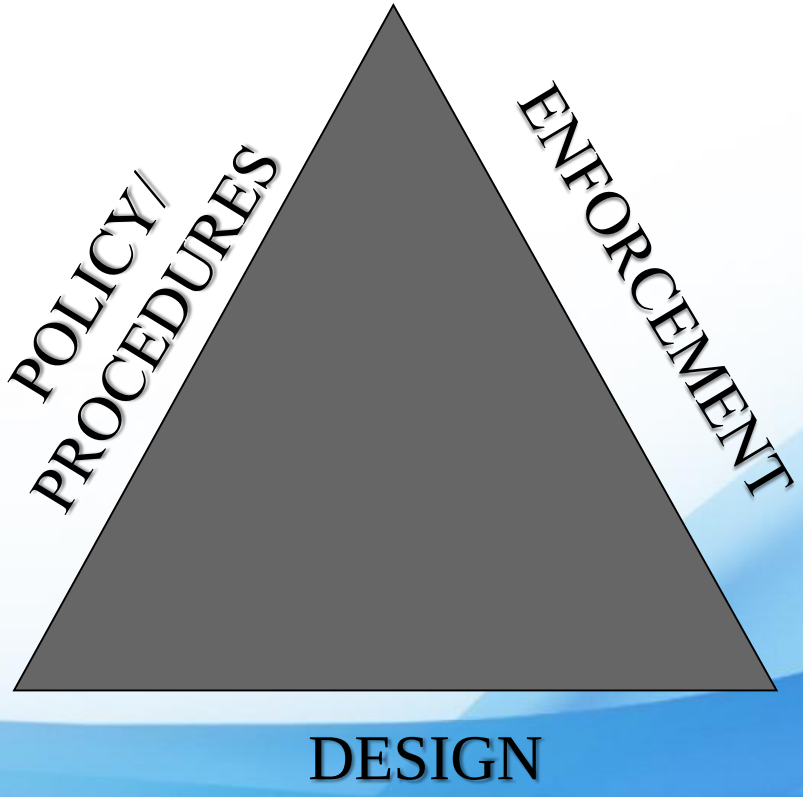
Cyber Security of DCS in NTPC

- 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

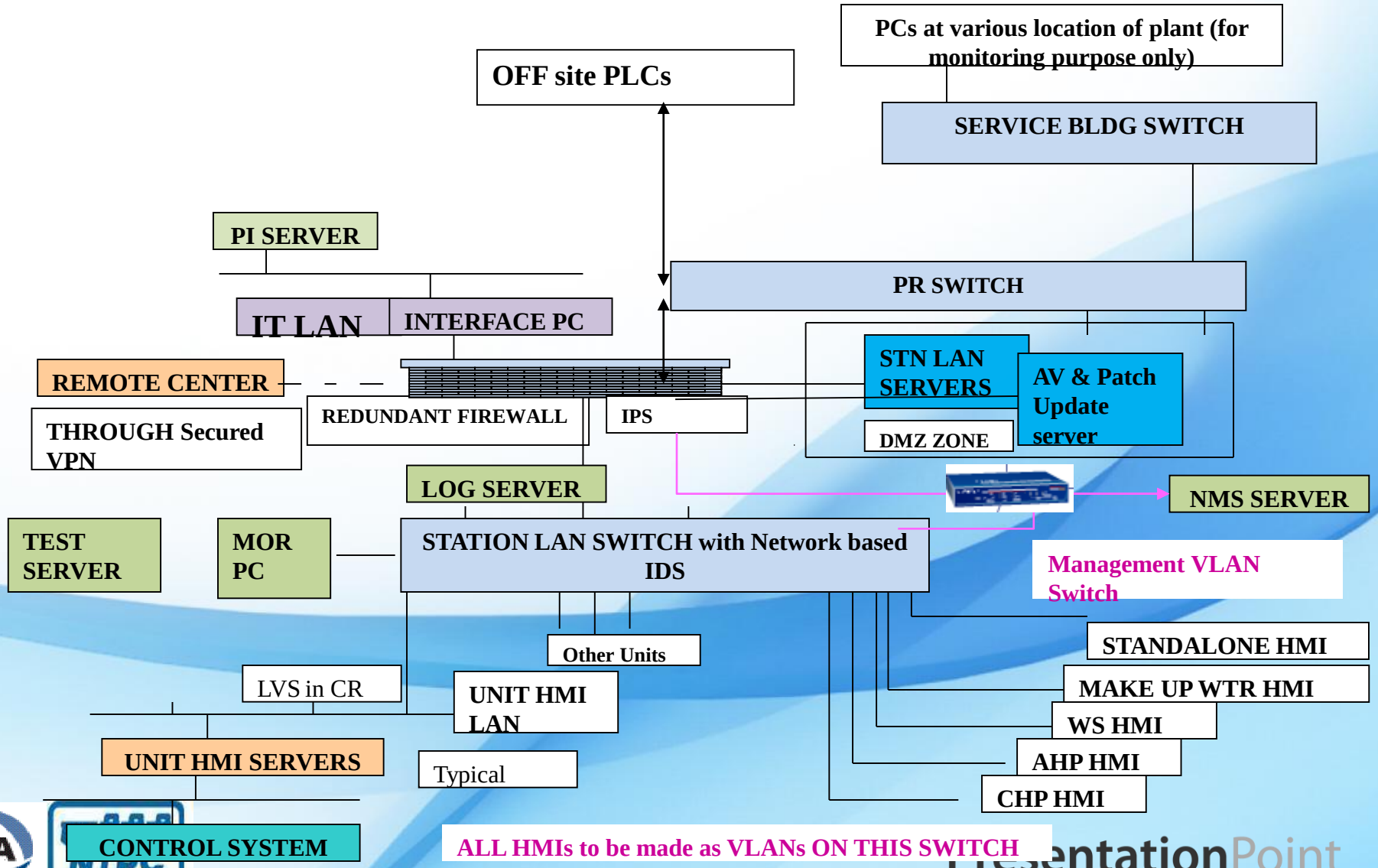
Cyber Security of DCS in NTPC:Contd.

- **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



ISA Delhi Section

A Maharatna Company

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 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

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

एनटीपीसी NTPC A Maharatna Company

DCS Security- now a “MUST HAVE” !!

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

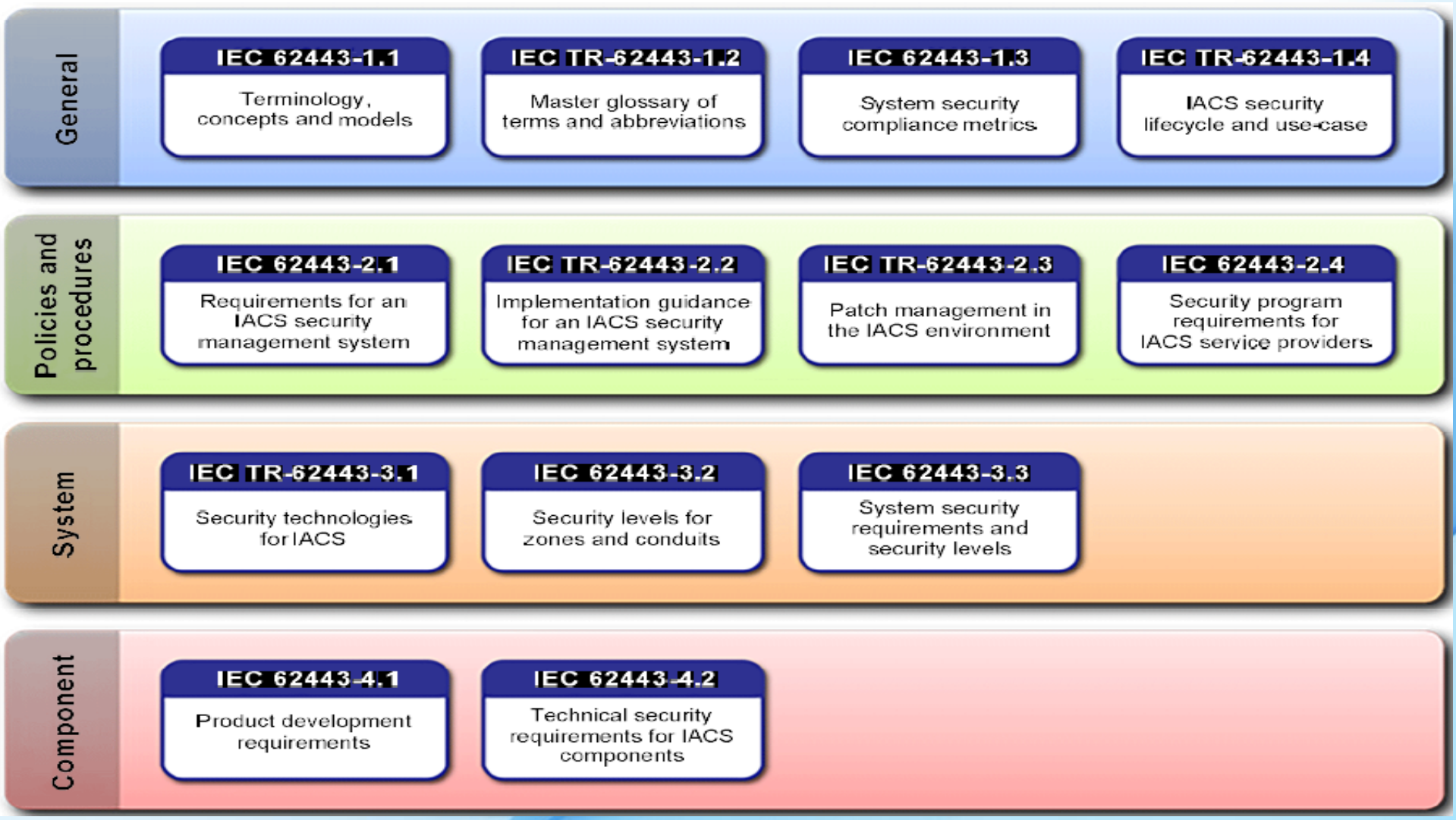
- Security of DCS Mandated by Standards
  - IEC 62443 –Specific standard for IACS (Industrial Automation & Control System)

- 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

IEC 62443-2.4 Standards- Details

- Requirement ID
  - SP.XX.YY
  - SP indicates Security Program
  - XX indicates functional area
  - YY is two digit identifier for the requirement
  - Base Requirement (BR) and their Requirement Enhancements (RE) all have the same SP requirement identifier
  - Requirement enhancements Sequence number is placed in parentheses following the “RE” starting at “1” for each BR
  - RE(#), where # is the sequence number of the enhancement.

IEC 62443-2.4 Standards- Details

Solution staffing	SP.01.XX	**Assignment of personnel by the service provider to Automation Solution related activities**
Assurance	SP.02.XX	**Providing confidence that the Automation Solution security policy is enforced**
Architecture	SP.03.XX	**Design of the Automation Solution**
Wireless	SP.04.XX	**Use of wireless in the Automation Solution**
SIS	SP.05.XX	**integration of SIS into the Automation Solution**
Configuration management	SP.06.XX	**Configuration control of the Automation Solution**
Remote access	SP.07.XX	**Remote access to the Automation Solution**
Event management	SP.08.XX	**Event handling in the Automation Solution**
Account management	SP.09.XX	**Administration of user accounts in the Automation Solution**
Malware protection	SP.10.XX	**Use of anti-malware software in the Automation Solution**
Patch Management	SP.11.XX	**Security aspects of approving and installing software patches**
Backup/Restore	SP.12.XX	**Security aspects of backup and restore**

IEC 62443-2.4 Standards- Details

- EXAMPLE 1

  SP.01.02 BR - base requirement for assigning personnel to the Automation Solution who have been informed of the IEC 62443-2-4 security requirements

  RE(1) enhances that requirement by defining a requirement for background checks of service provider personnel assigned to the Automation Solution.

  EXAMPLE 2

  SP.01.02 RE(2) defines an enhancement for the RE(1) requirement by specializing the RE(1) requirement to apply to subcontractor personnel assigned to the Automation Solution.

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** !!

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

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)

Indian Manual for Cyber Security in Power Systems

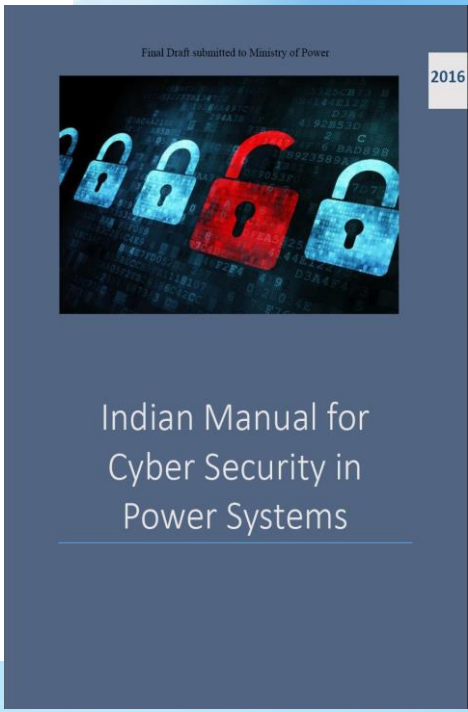
ISGF India Smart Grid Forum

GOVERNMENT OF INDIA
MINISTRY OF POWER

2. Acknowledgements

This manual is prepared by India Smart Grid Forum (Working Group 10 on Cyber Security) in coordination with National Critical Information Infrastructure Protection Center (NCIIPC). Following organisations contributed for the preparation of this Manual:

1. National Thermal Power Corporation (Mr R Sarangapani)
2. Tata Power Delhi Distribution Limited (Ms Satya Gupta)
3. Larsen & Toubro (Mr Abraham Samson & Ms Pallavi Mhatre)
4. Huawei (Dr Debu Nayak)
5. Schneider Electric (Mr Sandeep Pathak)
6. National Critical Information Infrastructure Protection Center (Mr Sachin Burman)
7. Microsoft (Mr Manish Tiwari)
8. Veermata Jijabai Technological Institute (Prof Faruk Kazi)
9. CESC, Kolkata (Mr Sumit Poddar and Ms Soma Basu)
10. Institute for Defence Studies and Analyses (Mr Munish Sharma)
11. Mr Arun Mane (in individual capacity)
12. ISGF (Mr Reji Kumar Pillai, Dr Shailendra Fuloria, Mr Samir Chaudhury, Mr Hem Thukral & Mr Sushant Chopra)



ISA Delhi Section

एनटीपीसी NTPC
A Maharatna Company

Indian Manual for Cyber Security in Power Systems

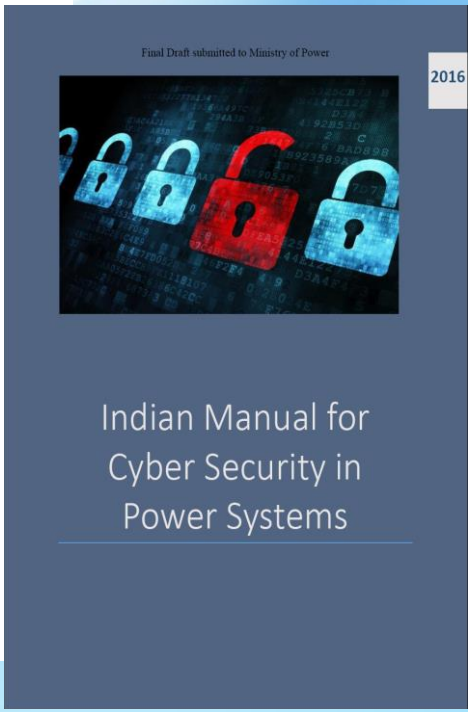
ISGF India Smart Grid Forum

GOVERNMENT OF INDIA
MINISTRY OF POWER

2. Acknowledgements

This manual is prepared by India Smart Grid Forum (Working Group 10 on Cyber Security) in coordination with National Critical Information Infrastructure Protection Center (NCIIPC). Following organisations contributed for the preparation of this Manual:

1. National Thermal Power Corporation (Mr R Sarangapani)
2. Tata Power Delhi Distribution Limited (Ms Satya Gupta)
3. Larsen & Toubro (Mr Abraham Samson & Ms Pallavi Mhatre)
4. Huawei (Dr Debu Nayak)
5. Schneider Electric (Mr Sandeep Pathak)
6. National Critical Information Infrastructure Protection Center (Mr Sachin Burman)
7. Microsoft (Mr Manish Tiwari)
8. Veermata Jijabai Technological Institute (Prof Faruk Kazi)
9. CESC, Kolkata (Mr Sumit Poddar and Ms Soma Basu)
10. Institute for Defence Studies and Analyses (Mr Munish Sharma)
11. Mr Arun Mane (in individual capacity)
12. ISGF (Mr Reji Kumar Pillai, Dr Shailendra Fuloria, Mr Samir Chaudhury, Mr Hem Thukral & Mr Sushant Chopra)



ISA Delhi Section

एनटीपीसी NTPC
A Maharatna Company

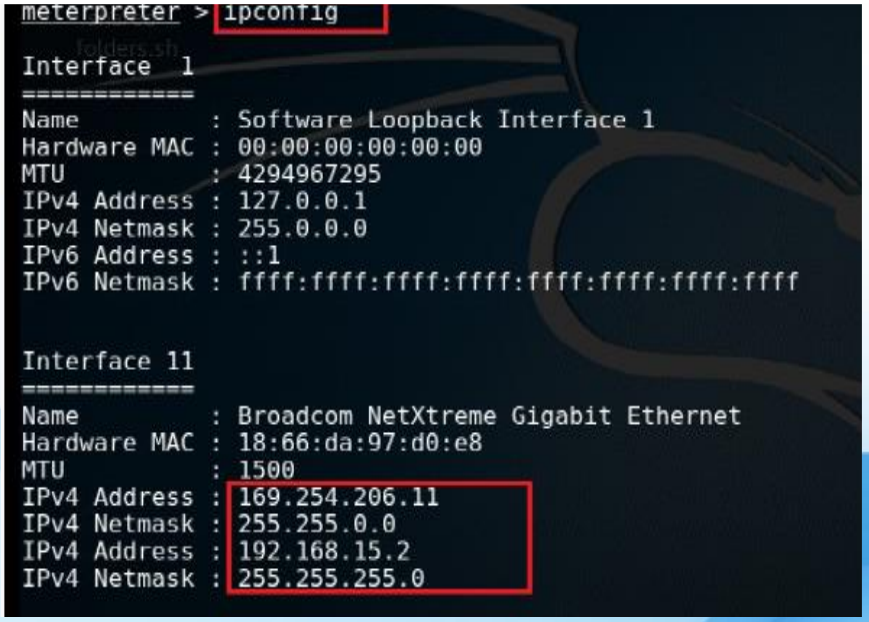
Best practices

- 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.

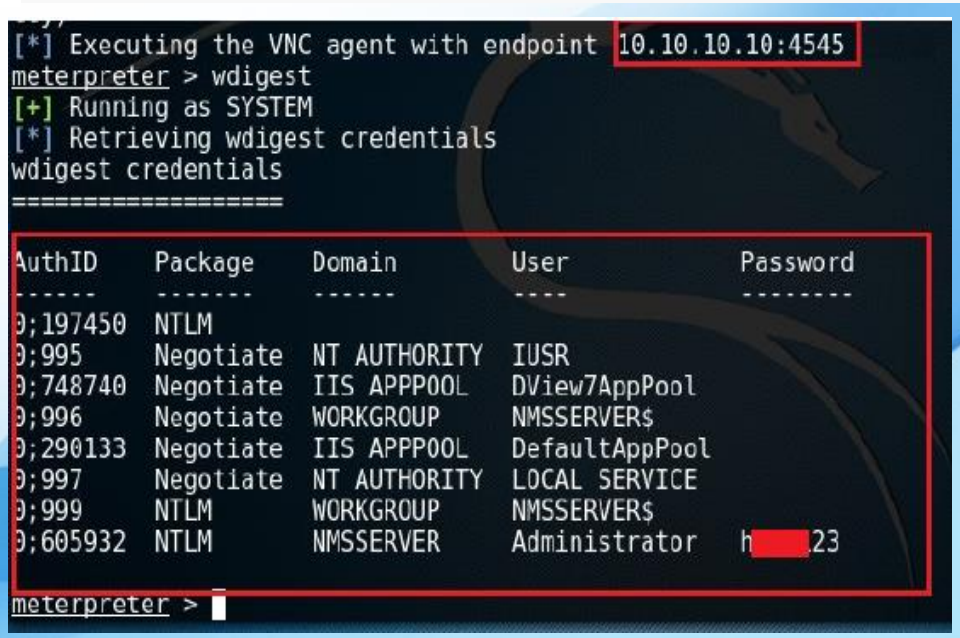
Practices Adopted in NTPC: Patching for Ransomware like WannaCry

- Critical vulnerability MS17-010 (ETERNALBLUE).
  - Server Message Block (SMB) is the transport protocol used by Windows machines for a wide variety of purposes such as file sharing, printer sharing, and access to remote Windows services.

The screenshot below shows the system has been compromised and we were able to execute the system level commands.



The following screenshot shows we have retrieved user's password.



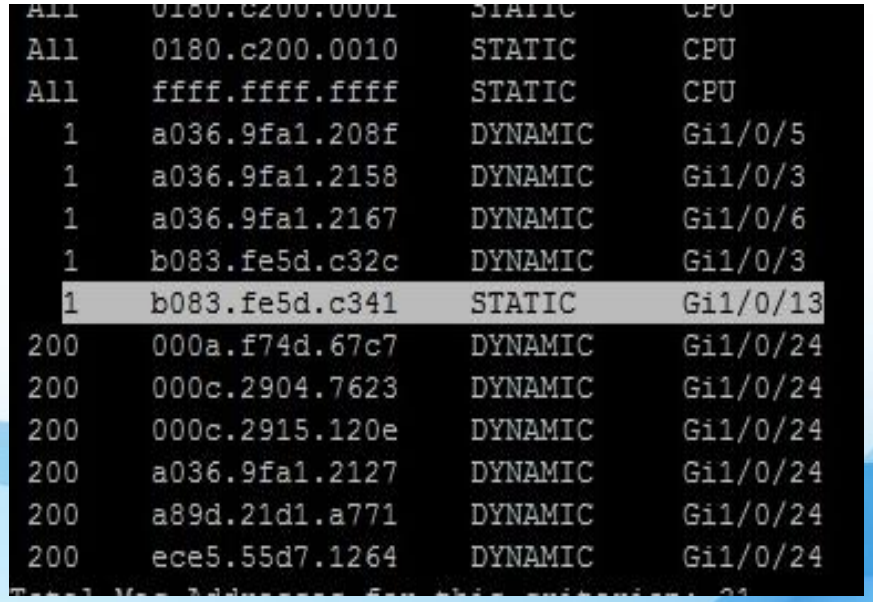
- ms 14-066, ms 11-030, MS 15-034 Microsoft Patches are applied.

ISA Delhi Section

A Maharatna Company

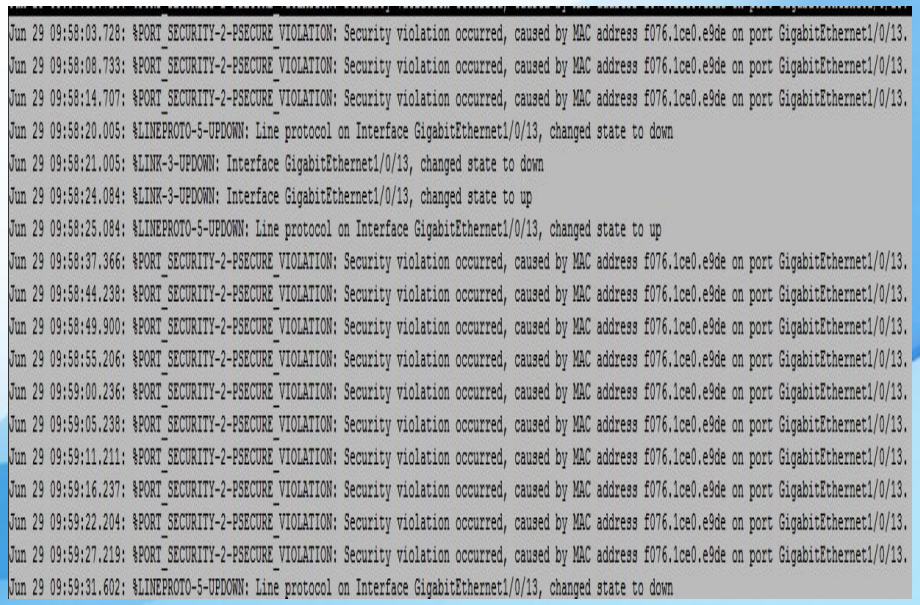
Practices Adopted in NTPC: Mac Binding

- 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.c200.0001	STATIC	CPU
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

Practices Adopted in NTPC: 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.

Practices Adopted in NTPC: 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 being ensured.

Practices Adopted in NTPC: Remote access

For getting Support from OEM through Secured VPN

a) Using **two factor authentication** (2FA)

- Provides an additional layer of security and makes it harder for attackers to gain access to a IACS, because knowing the victim's password alone is not enough to pass the authentication check.

- What are the two authentication factors?
- 1. Knowledge factors -- something the user knows, such as a password, PIN or shared secret.
- 2. Possession factors -- something the user has, such as an ID card, security token or a smartphone.

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

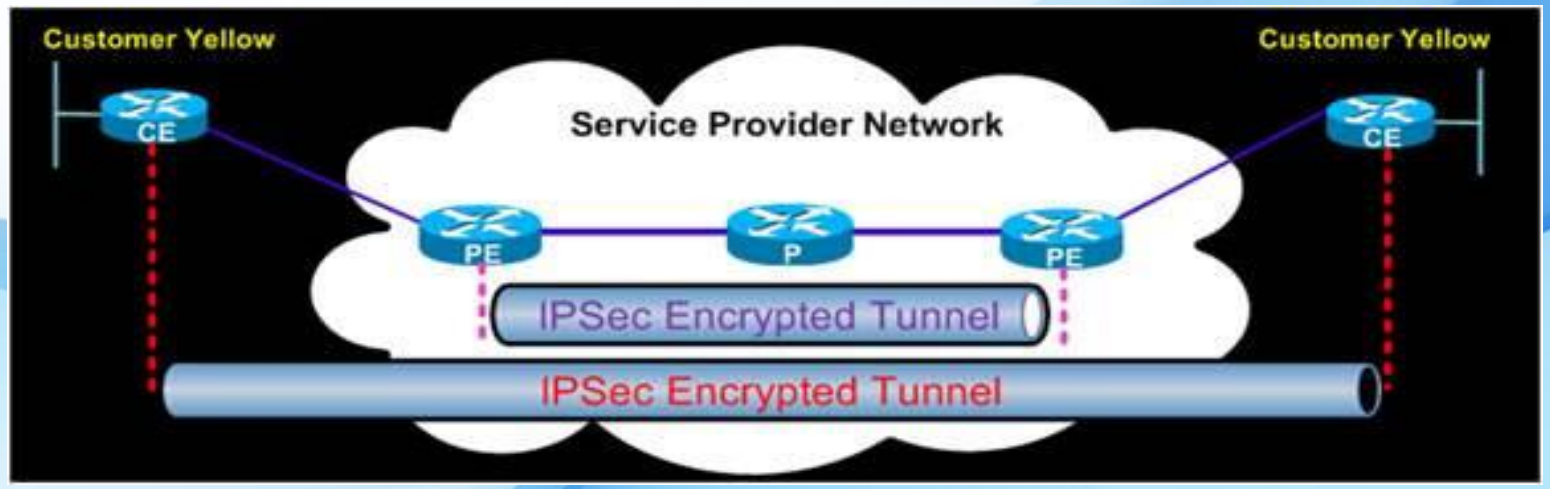
c) Using encryption technologies to protect the confidentiality and integrity of communications.

Practices Adopted in NTPC: Remote access

- **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



ISA Delhi Section

एनटीपीसी NTPC A Maharatna Company

Findings of Audit reports

Extract from a Security Audit of NTPC DCS

Vulnerability	Affected systems	Impact	Status	Clients Justification
NTP monlistCommand Enabled	[redacted]	Medium	Not Fixed	
OpenSSL 'ChangeCipherSpec' MiTM Vulnerability	[redacted]	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

एनटीपीसी NTPC A Maharatna Company

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.

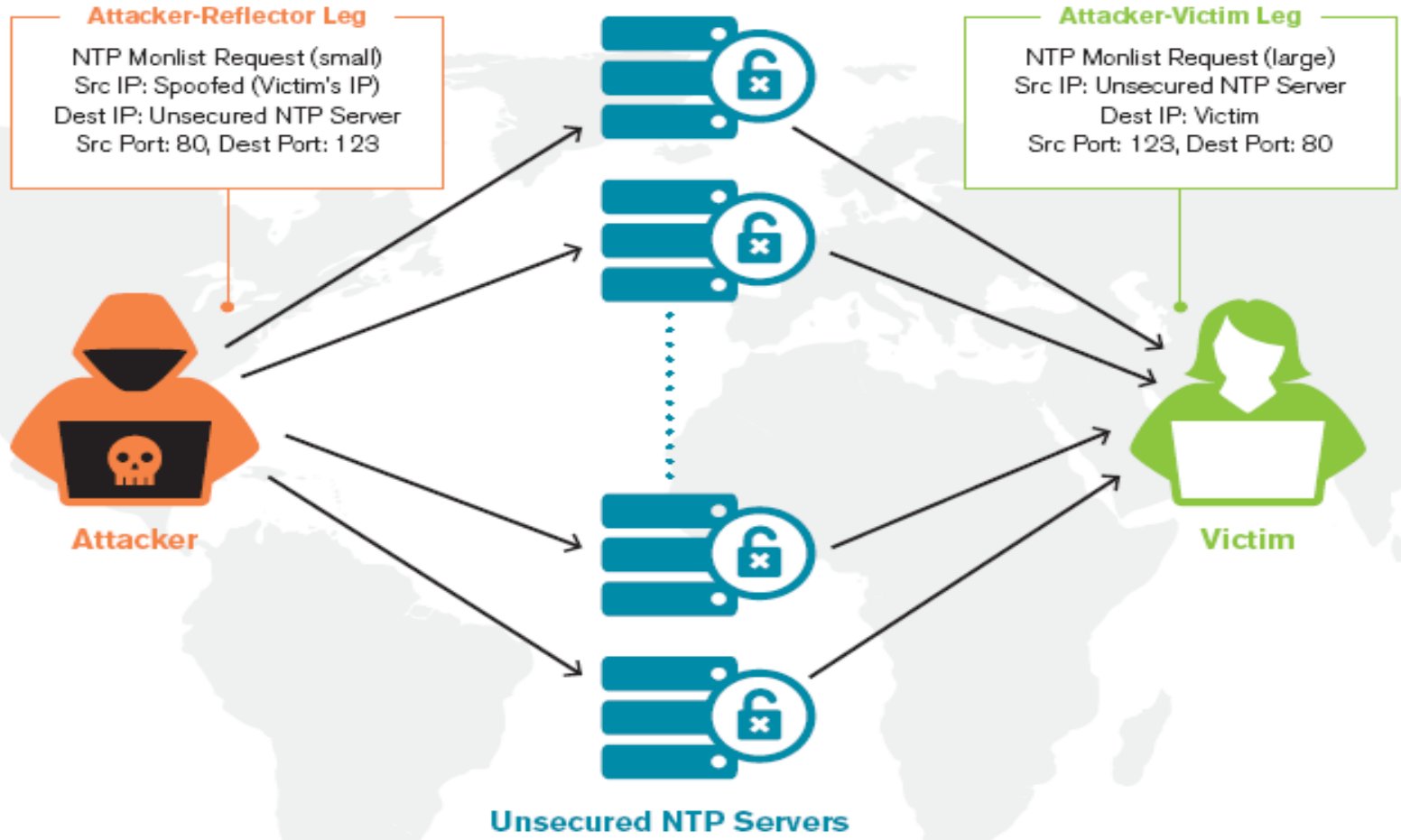
Solution

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



CERT sites


US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM
HOME
ABOUT US
CAREERS
PUBLICATIONS
ALERTS AND TIPS
RELATED RESOURCES
C³ VP
Current Activity
The US-CERT Current Activity web page is a regularly updated summary of the most frequent, high-impact types of security incidents currently being reported to the US-CERT.
Cisco Releases Security Updates
Published January 17, 2018
Cisco has released security updates to address vulnerabilities affecting multiple products. An attacker could exploit one of these vulnerabilities to take control of an affected system.
NCCIC/US-CERT encourages users and administrators to review the following Cisco Security Advisories and apply the necessary updates:
Email Security and Content Security Management Appliance Privilege Escalation Vulnerability cisco-sa-20180117-esasma
NX-OS Software Pong Packet Denial of Service Vulnerability cisco-sa-20180117-nx-os
Unified Customer Voice Portal Denial of Service Vulnerability cisco-sa-20180117-cv
Read Full Entry »
ISC Releases Security Advisories for DHCP, BIND
Published January 16, 2018
The Internet Systems Consortium (ISC) has released updates or workarounds that address vulnerabilities in versions of ISC Dynamic Host Configuration Protocol (DHCP) and Berkeley Internet Name Domain (BIND). A remote attacker could exploit these vulnerabilities to cause a denial-of-service condition.
NCCIC/US-CERT encourages users and administrators to review ISC Knowledge Base Articles AA-01541 and AA-01542 and apply the necessary updates or workarounds.
Read Full Entry »
Oracle Releases January 2018 Security Bulletin
Published January 16, 2018
Oracle has released its Critical Patch Update for January 2018 to address 237 vulnerabilities across multiple products. A remote attacker could exploit some of these vulnerabilities to obtain access to sensitive information.
NCCIC/US-CERT encourages users and administrators to review the Oracle January 2018 Critical Patch Update and apply the necessary updates.
Read Full Entry »
VMware Releases Security Updates for Workstation, Fusion
Published January 11, 2018
VMware has released security updates to address vulnerabilities in VMware Workstation and Fusion. An attacker could exploit these vulnerabilities to take control of an affected system.
NCCIC/US-CERT encourages users and administrators to review the VMware Security Advisory VMSA-2018-0005 and apply the necessary updates.
Read Full Entry »
Juniper Networks Releases Security Updates
Published January 11, 2018
Juniper Networks has released security updates to address vulnerabilities affecting multiple products. An attacker could
Latest Alerts
Meltdown and Spectre Side-Channel Vulnerability Guidance
Thursday, January 4, 2018
HIDDEN COBRA – North Korean Trojan: Volgmer
Tuesday, November 14, 2017
HIDDEN COBRA – North Korean Remote Administration Tool: FALLCHILL
Tuesday, November 14, 2017
More Alerts »
Recent Vulnerabilities
VU#584653: CPU hardware vulnerable to side-channel attacks
Wednesday, January 3, 2018
VU#144389: TLS implementations may disclose side channel information via discrepencies between valid and invalid PKCS#1 padding
Tuesday, December 12, 2017
VU#113765: Apple MacOS High Sierra root authentication bypass
Wednesday, November 29, 2017
VU#681983: Install Norton Security for Mac does not verify SSL certificates
Tuesday, November 21, 2017
VU#817544: Windows 8.0 and later fail to properly randomize all applications if system-wide mandatory ASLR is enabled via EMET or Windows Defender Exploit Guard
Friday, November 17, 2017
More Vulnerability Notes »

CERT sites

Industrial Security ▸ Deutsch ▸ Contact ▸ Site Explorer Search

› Home › Industrial Security › Alerts and updates › Alerts

- › Plant security
- › Network security
- › System integrity
- › Always active
- › Alerts and updates
- › Support

Industri

Take adv er to obtain an overview of current developments in the area of industrial

Categ

- ☐ General
- ☐ Network components
- ☐ PC-based
- ☐ Software
- ☐ Controller/Control systems
- ☐ HMI
- ☐ Motion Control and Drives

Reset

Overview

- General customer information for vulnerabilities Meltdown and Spectre (January 11th 2018)
- Security Information for LOGO! Soft Comfort (December 18th 2017)
- Updates for SIMATIC RF350M and SIMATIC RF360M (December 18th 2017)
- Updates for Industrial Products (November 23rd 2017)
- Update on DROWN vulnerability (November 23rd 2017)
- Vulnerabilities in SCALANCE W1750D, SCALANCE M800, and SCALANCE S615 (November 17th 2017)
- Additional Information on "KRACK Attacks" Vulnerabilities in WPA/WPA2 (November 9th 2017)
- Vulnerabilities in WPA/WPA2 reported as "KRACK Attacks" (October 18th 2017)
- Industrial Security Alert - 10/18/2017 (second publication) (October 18th 2017)
- Update for Ruggedcom ROS and SCALANCE X devices (October 12th 2017)
- Release of LOGO!8 BM FS-05 with firmware V1.81.2 (August 30th 2017)
- OPC UA vulnerability in Industrial Products (August 30th 2017)
- Update for SIMATIC Sm@rtClient App (July 13th 2017)
- Update for SIMATIC Logon (July 6th 2017)
- Update for Industrial PCs (June 26th 2017)
- Update for XHQ (June 22nd 2017)
- Update for SIMATIC CP 44x-1 RNA (June 20th 2017)
- Updates for Industrial Products (May 8th 2017)
- Vulnerabilities in RUGGEDCOM ROX I-based Devices (March 28th 2017)

Text Size

Share this Page:

Keep up-to-date

Subscribe to the RSS Feed of the latest news on Industrial Security

Subscribe now

Have an incident or found a vulnerability?

Please contact the Siemens Cyber Emergency Readiness Team (CERT)

Siemens CERT

Do you have questions on industrial security or do you need one-on-one support? Contact us!

industrialsecurity.i@siemens.com

More information

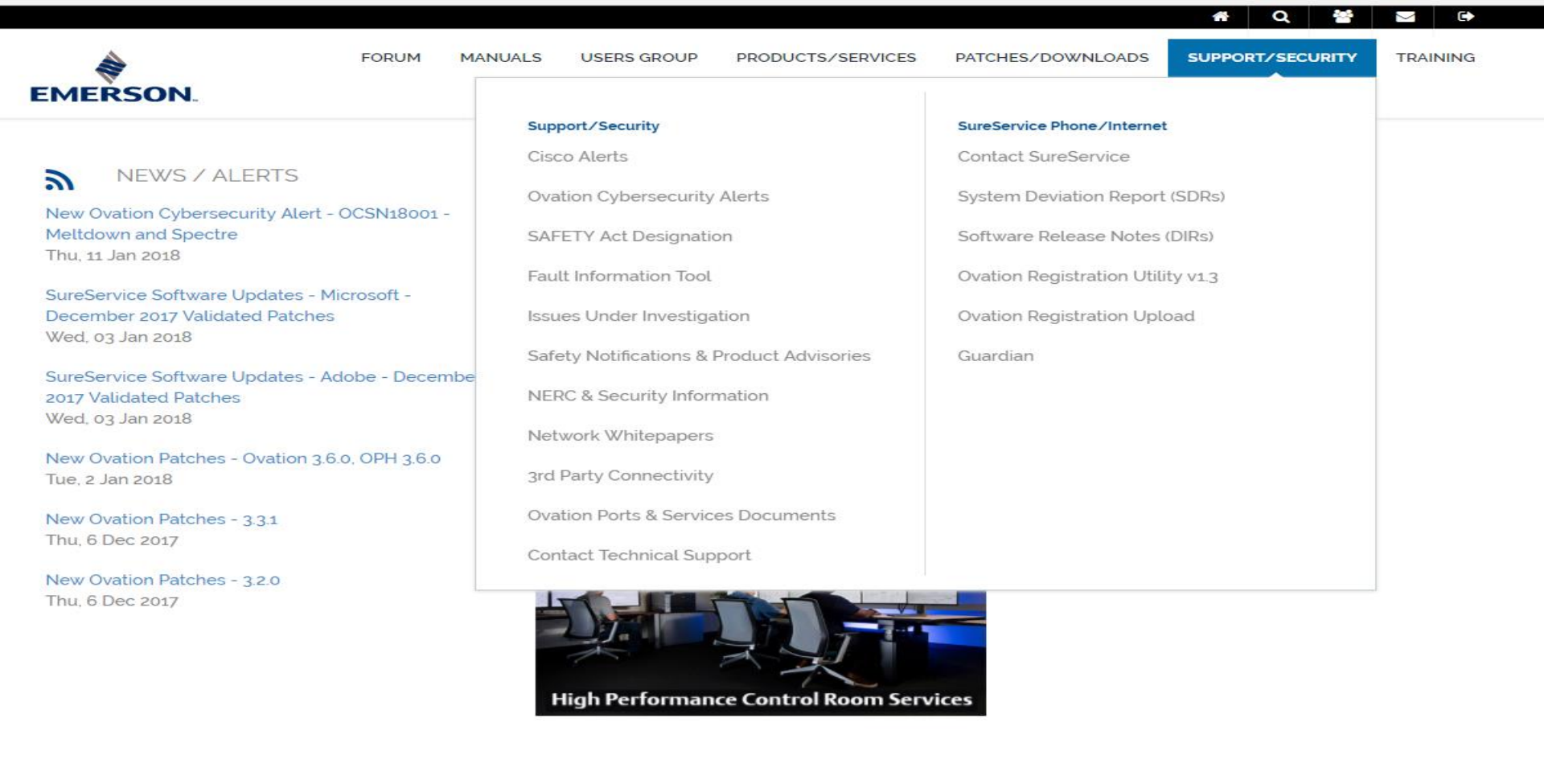
- Siemens Industry Online Support
- Compatibility information SIMATIC WinCC
- Compatibility information SIMATIC PCS 7

- Support information
- Brochures and downloads
- Press releases
- Related topics

ISA Delhi Section

एनटीपीसी NTPC A Maharatna Company

CERT sites



ISA Delhi Section

A Maharatna Company

MOM excerpt

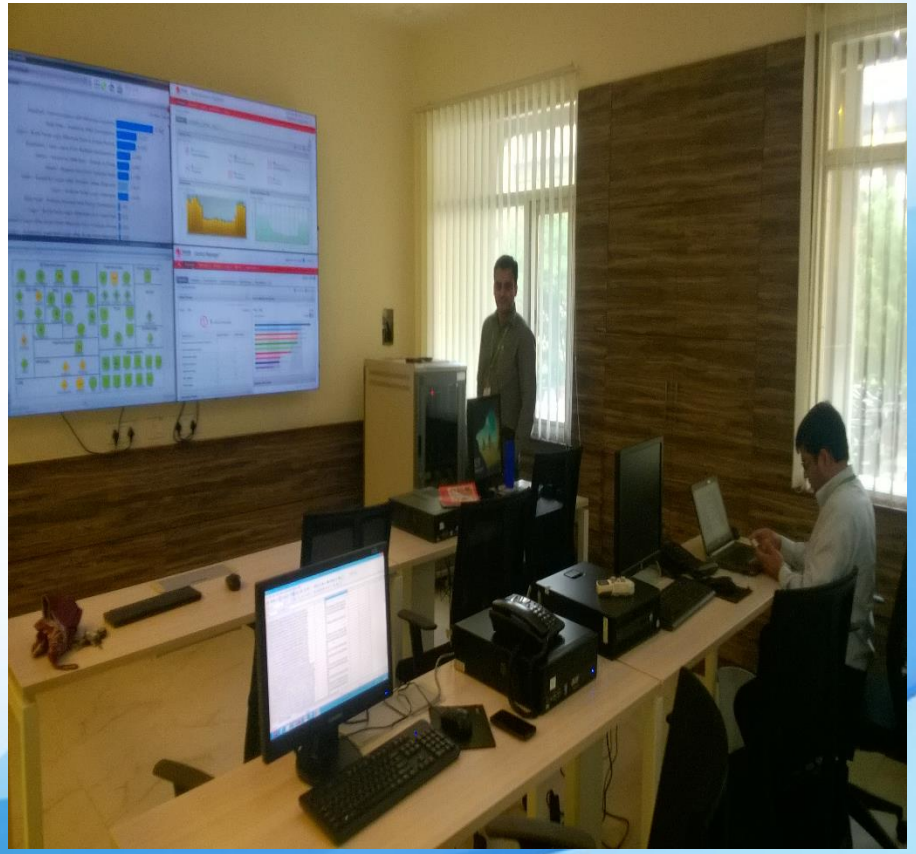
S.No.	Description	Status/Commitment
1	**Initial Checks and updation of Ovation application**	
	The patches of Release Ovation [redacted] used in [redacted] station C&I package were checked and compared with the released Patch list available in Ovation website for the same. It was found that patches OVA351128, OVA351127 and OVA351124 released in July 2017 were not installed in the system. In addition to this, NTPC further enquired if Ovation Cyber Security Alerts OCSN17002, OCSN17001 (related to Petya and WannaCry Ransomware) and OCSN16001 are required to be patched. M/s EPMI stated that the Ovation [redacted] patches released in July 2017 are to be installed in the system. Regarding Cybersecurity Alerts M/s EPMI stated that Vulnerabilities w.r.t Petya and WannaCry ransomware are already mitigated in the presen[redacted] systems using Windows 7 and Windows 2008 R2 OS. W.r.t OCSN16001, M/s EPMI stated that this vulnerability is mitigated through Ovation[redacted] patch OVA351054.	OVA351124, OVA351127 and OVA351128 patches installed in Unit 1 and SAC DDCMIS. OVA351054 demonstrated in both this DDCMIS. M/s EPMI confirmed that these patches will be installed in Unit#2, AHP, CHP (before FAT) and in MUWS DDCMIS before start of commissioning activity. Versions of all the softwares and firmwares are attached as Annexure II.
2	**Initial Checks and updation of Cisco Switches, Firewall and IPS**	
	NTPC enquired if all the security alerts mentioned in Cisco Alerts Spreadsheet (Mar 2017) are addressed in the different Cisco switches, firewall and IPS models used in this project. M/s EPMI stated that the latest Ovation Validated Cisco IOS is being used in this project for all the Cisco Switches. However based on the spread sheet information, NTPC stated that the following vulnerabilities are to be addressed: i) Present IOS version 15.2(1)E2 for switch type WS-[redacted] and IOS version [redacted] for switch type [redacted]24TS-E are vulnerable to ntp Subsystem Unauthorised Access Vulnerability. ii) Present IOS version 15.2(1)E2 for switch type WS-[redacted]C-L and IOS version [redacted] for switch type WS-C3560V2-24TS-E are vulnerable to IKEv1 information Disclosure Vulnerability. For Cisco Firewall and IPS, M/s EPMI stated that the ASA Software version and ASA Firepower Software versions used in this project are the latest and all the vulnerabilities mentioned in the spreadsheet related to ASA are not applicable for these software versions.	M/s EPMI demonstrated the IOS versions of all Cisco products. Regarding NTP vulnerability, M/s EPMI Stated that authentications and ACLs shall be added as a work around at site (as target Master Clock is required) until permanent fix has been released by CISCO. Regarding IKEv1 vulnerability, M/s EPMI stated that the same is not applicable as it is not used in Ovation network.

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

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

ISA Delhi Section

A Maharatna Company

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

ISA Delhi Section

एनटीपीसी NTPC
A Maharatna Company