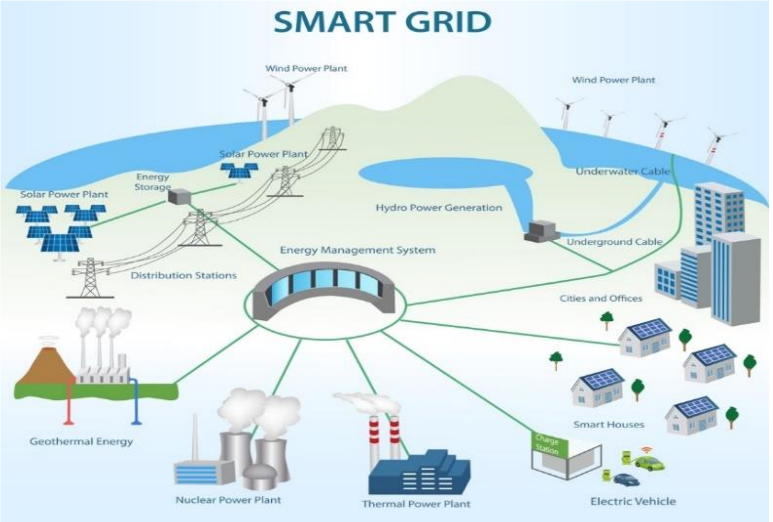
SMART GRIDS AND CYBER SECURITY



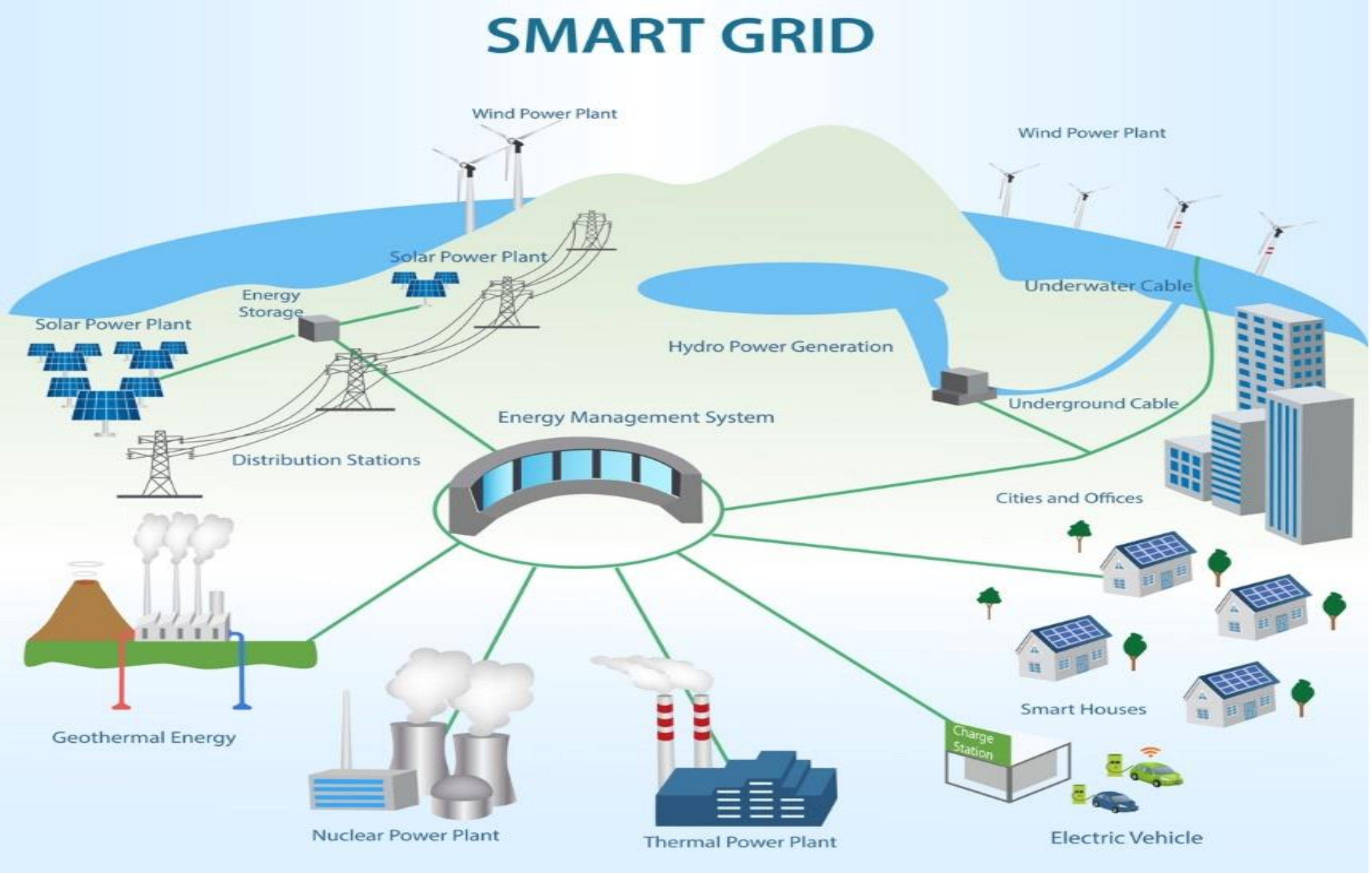
CYBER SECURITY

Sushil Kumar
Dy. General Manager
GAIL(India) Limited, New Delhi

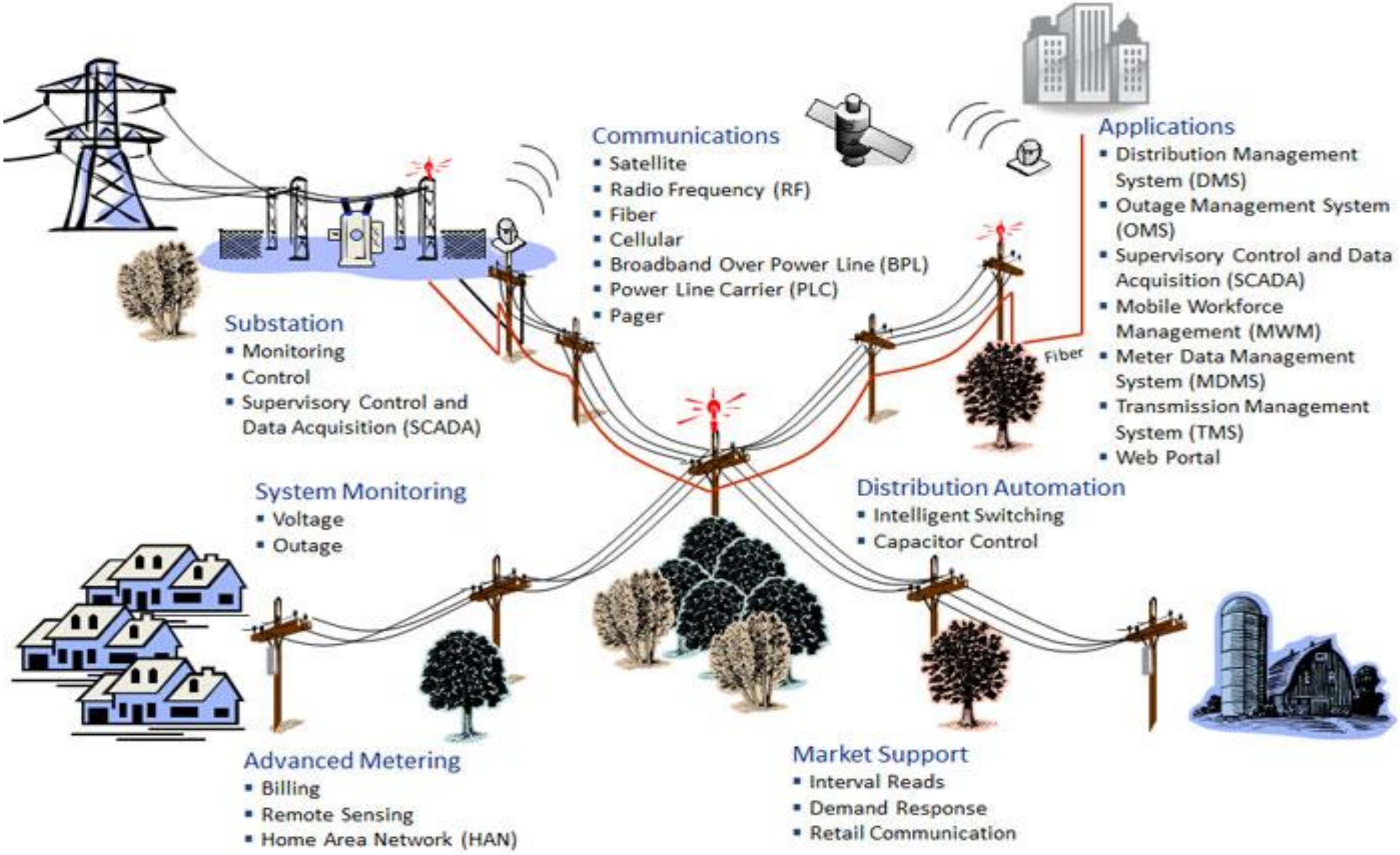
SMART GRID

A smart grid is an evolved grid system that manages electricity/gas/ water demand and supply in a sustainable, reliable and economic manner, built on advanced infrastructure and tuned to facilitate the integration of information and communication technologies (ICT) to gather and act on information about components, systems, suppliers and consumers, in an automated fashion .

SMART GRID-ECTRICAL



VARIOUS COMPONENTS OF SMART GRID



Communications
- Satellite
- Radio Frequency (RF)
- Fiber
- Cellular
- Broadband Over Power Line (BPL)
- Power Line Carrier (PLC)
- Pager

Applications
- Distribution Management System (DMS)
- Outage Management System (OMS)
- Supervisory Control and Data Acquisition (SCADA)
- Mobile Workforce Management (MWM)
- Meter Data Management System (MDMS)
- Transmission Management System (TMS)
- Web Portal

Substation
- Monitoring
- Control
- Supervisory Control and Data Acquisition (SCADA)

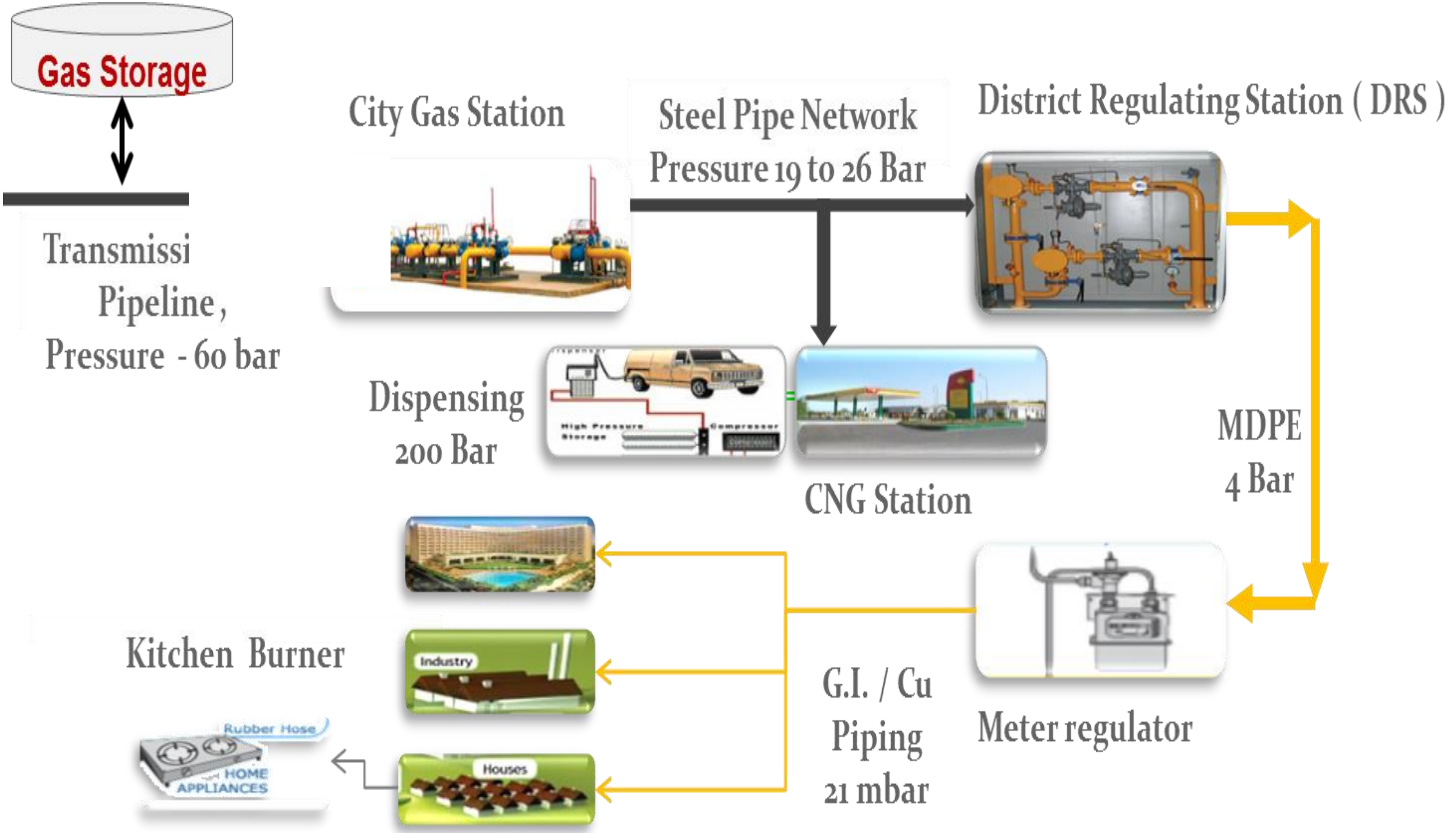
System Monitoring
- Voltage
- Outage

Distribution Automation
- Intelligent Switching
- Capacitor Control

Advanced Metering
- Billing
- Remote Sensing
- Home Area Network (HAN)

Market Support
- Interval Reads
- Demand Response
- Retail Communication

NATURAL GAS :CITY GAS DISTRIBUTION NETWORK



Gas Storage

Transmissi Pipeline , Pressure - 60 bar

City Gas Station

Steel Pipe Network Pressure 19 to 26 Bar

District Regulating Station (DRS)

Dispensing 200 Bar

CNG Station

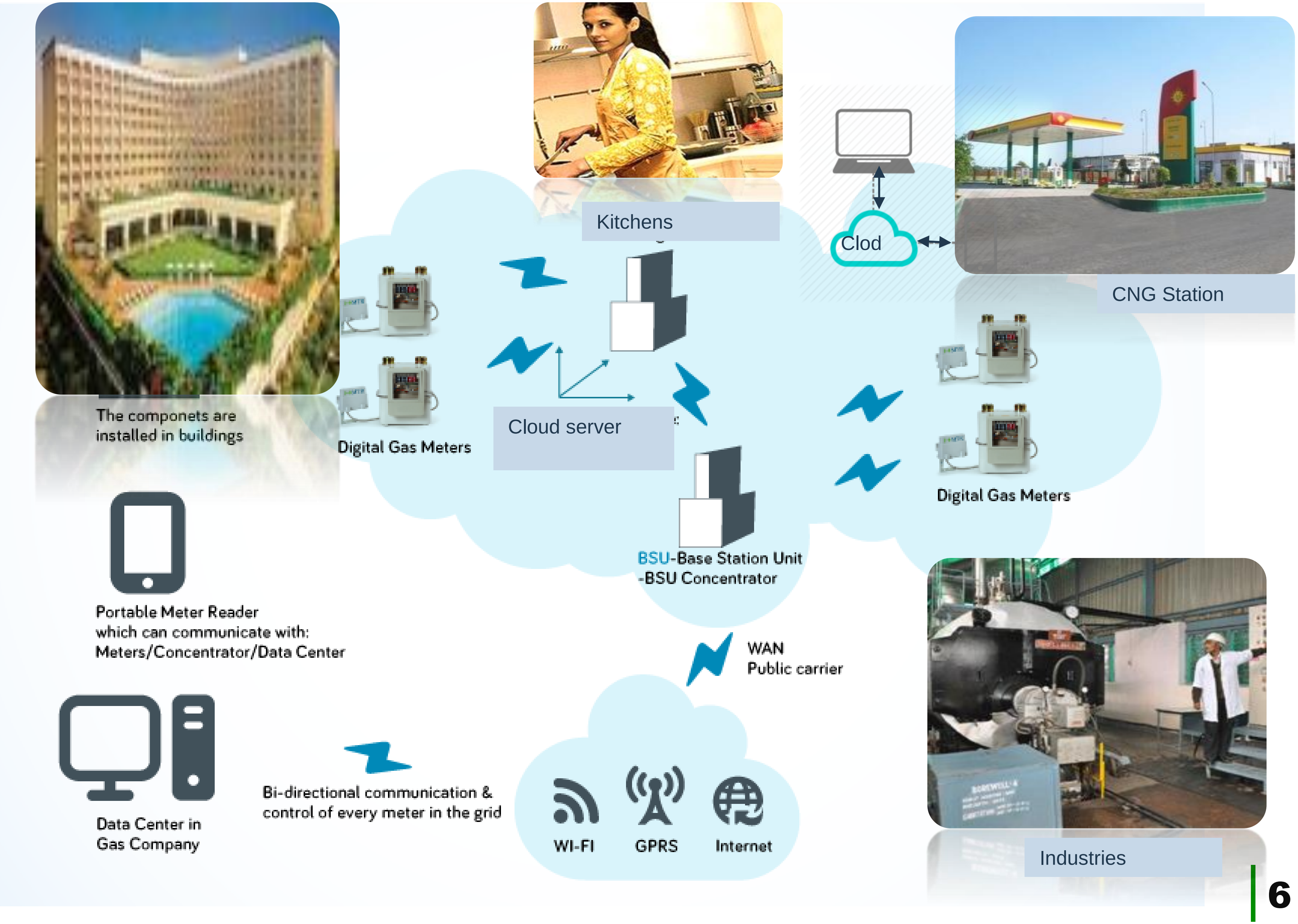
MDPE 4 Bar

Meter regulator

G.I. / Cu Piping 21 mbar

Kitchen Burner

SMART GRID: CITY GAS DISTRIBUTION TOPOLOGY



Kitchens

Clod

CNG Station

The componets are installed in buildings

Digital Gas Meters

Cloud server

Digital Gas Meters

BSU-Base Station Unit
-BSU Concentrator

Portable Meter Reader
which can communicate with:
Meters/Concentrator/Data Center

WAN
Public carrier

Data Center in
Gas Company

Bi-directional communication &
control of every meter in the grid

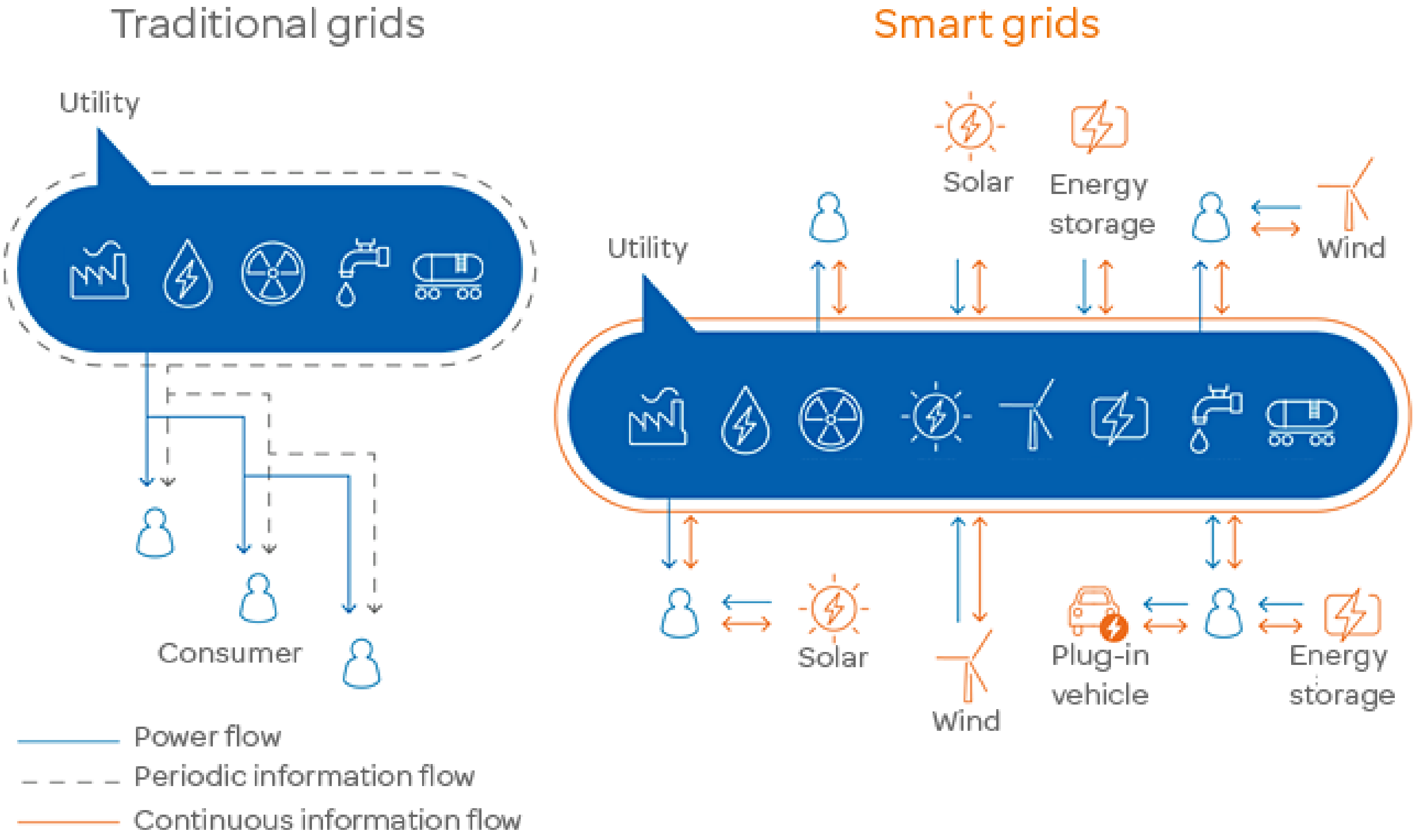
WI-FI

GPRS

Internet

Industries

TRADITIONAL & SMART GRIDS



FUNCTIONALTIES& COMPONENTS OF SMART GRID

- SCADA/EMS & SCADA/ DMS
- Substation & Distribution Automation
- Wide Area Monitoring System
- AMI (Smart Metering)
- Cyber Security
- Storage or water /gas storage in pipeline
- Electric Vehicle or NGVs in case of Gas
- Renewable Energy: wind/solar or biogas
- Power/ gas/ water Quality Management

FUNCTIONALTIES& COMPONENTS OF SMART GRID

- Common Command Control Room
- Enterprise IT System
- Application Integration & Analytics
- GIS (Digital) Map
- Customer Engagement Social Media for Utility
- Mobile Crew Management System
- Smart Street Lights
- Outage Management System

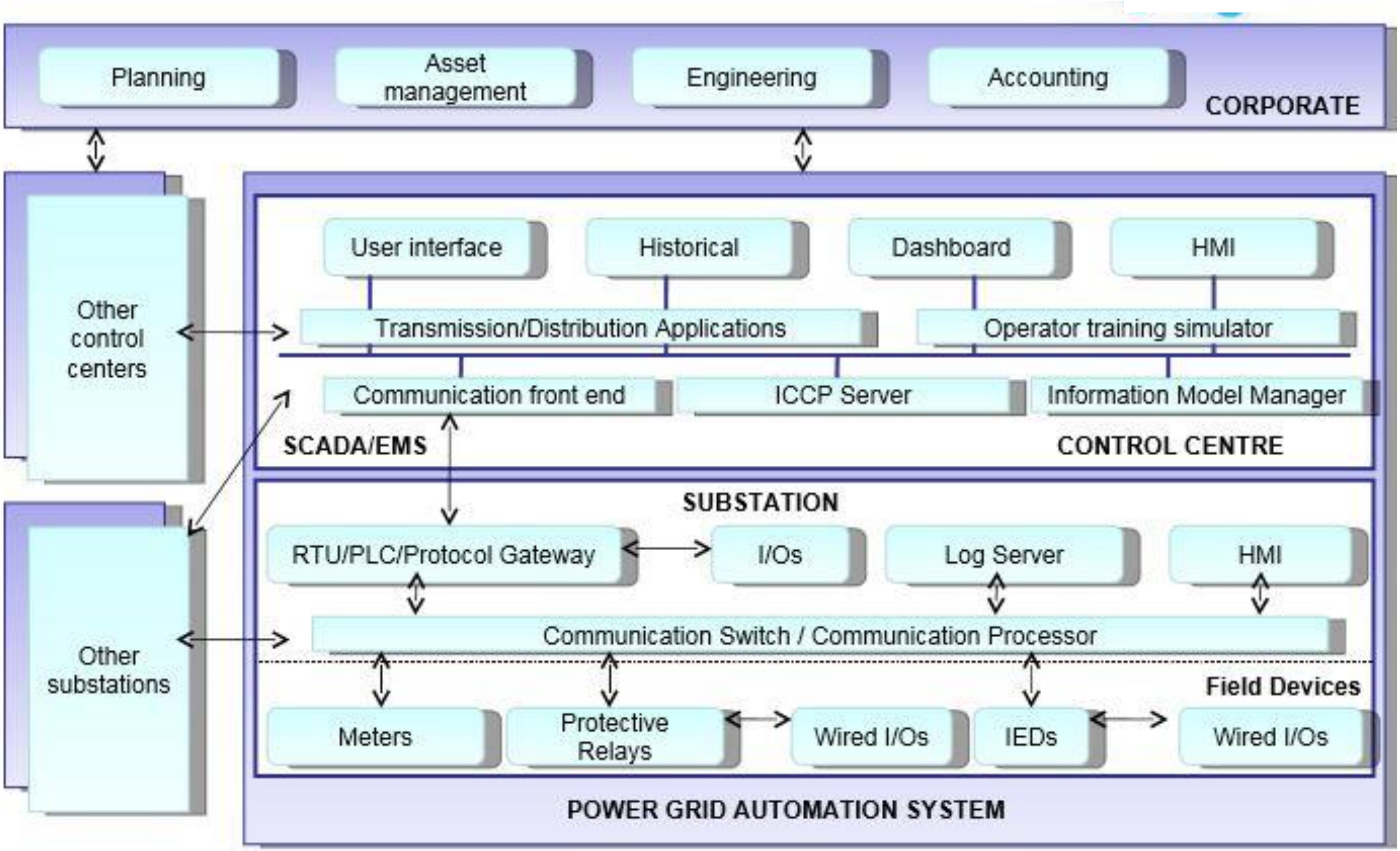
SMART GRID- BENEFITS OF AMR SYSTEM

- Promotes energy conservation
- Lowers significantly the cost of meter reading (manual versus automatic)
- Provides real time – on line billing info while reducing estimated inaccurate readings
- Reduces billing mistakes and conflicts and increases client's satisfaction
- Reduces the number of metering personnel on the streets and enhances safety by providing smart reading methods
- Provides flexibility in reading schedules and avoids delays
- Increases confidence in the service provider
- Exposure of usage information and promoting energy conservation
- Increases the cash flow

CYBER SECURITY

The Utility (Power/Gas/Water) sector is the critical infrastructure of a nation and other sectors depend directly and indirectly on them. Cyber-Physical Security is protection of the assets (both hardware and software) from natural and manmade disasters and intended and unintended activities. Since physical assets are associated with the cyber space of a utility, cyber-physical security completely defines the security paradigm of a utility. This dependency of the physical assets on the cyber assets (and vice versa), has prompted the utilities to inject resiliency and robustness into their grids.

SMART GRID- CORPORATE & OPERATIONAL N/W



SMART GRID- TYPES OF CYBER ATTACKS

- **Component wise:** Field components like RTUs are attached through remote access. Mislead data presented to control system operator which may lead to damage of filed equipment, If operation performed based on the mislead data. Loss of services due to intruder shutting down the devices.
- **Protocol wise**: Using the communication protocols available in the public domain, an intruder can reverse engineer the data acquisition protocols and exploit them. Financial loss if the attack leads to excess generation output. Safety vulnerability if a line is charged while lineman are in the filed servicing the line. Equipment damage if control commands are sent to filed resulting in overload conditions.
- **Topology wise**: Network topology vulnerability is exploited like DoS (Denial of Services). Delay or inhibition of real time data exchange. As a result, control center operator may fail to have complete view of grid system status which may lead to incorrect decision making.

SMART GRID- CYBER SECURITY SYSTEM

Smart Grid Cyber Security Platform must be designed to address the following requirements:

- Data security
- Application security
- Sensor/device security
- Sensitive data handling
- Security administration

SMART GRID- CYBER SECURITY THREATS

The Global Business Reality

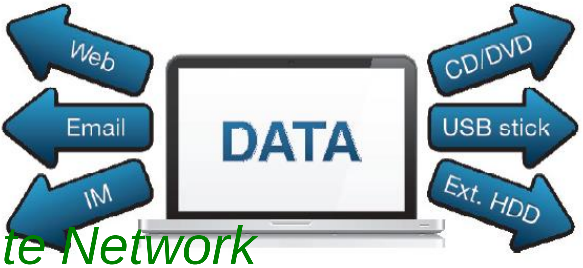
- Advanced technology - New form of attacks
- Open Plan – Office Culture
- Misuse of Resources
- Multiple ways to connect to Office networks
- Dynamic business environment

Increased threat to Information Security! !

How Data Leakage Happens in Corporate ?

What is Data Leakage ?

- Disclosure of sensitive data to unauthorized personnel either by malicious intent or inadvertent mistake.
- Sensitive data - Private or company information , Intellectual property (IP), Financial ,Patient information ,Credit-card data and other information depending on the business and the industry.



Ways for data leakage by users in Corporate Network

- Copying of Data to External Media (CD, DVD, Pen drive, Portable HDD.
- Photo-copying and printing of sensitive information and its distribution.
- Sending emails through Corporate Email and free webmail systems (Google, Yahoo etc.).

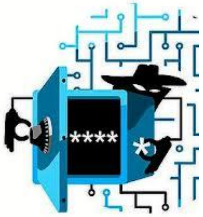
How Data Leakage Happens in Corporate ?

Ways for data leakage by outsiders

- Theft of Laptop/Mobile of GAIL officials in public places / hotel.
- Advanced Targeted cyber-attacks by cyber-criminals.

Terminologies in Cyber Criminal World

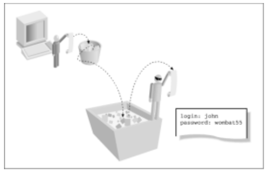
- Back Door - A point of entry used by a cracker to access a network or computer system.
- Black Hat – A Cracker who looks vulnerabilities in target systems for exploitation. They also share information about the vulnerabilities to other Black hats.
- Gray Hat – A cracker gains access to the targeted system/network illegally for exposing the security weaknesses and to notify the “victim” about their success.
- White Hat – Ethical cracker to prevent the black hat’s entry and secure the integrity of computer systems/networks of corporates/govt. organizations.
- Script Kiddie -An individual uses pre-written program to crack a computer/network.



```
class HelloScribes(object):

    def __init__(self):
        self.__appname = "Scribe
        self.__version = 0.4
        self.__status = "VAPORWARE
        print "%s - %d (%    " % (self.__                f.__

def main():
    HelloScribes()
    return

if __name__ == "__mai
    main()
```

Terminologies in Cyber Criminal World

- Bot/Zombie/Zombie Drone - A software “robot” used by black hat to take remote control of a system/network for further attacks.
- Botnet – A network of zombie drones under the control of a black hat.
- Denial of Service Attack (DOS) – An attack designed to overwhelm a targeted website to the point of crashing it or making it inaccessible.
- Distributed Denial of Service Attack (DDOS) - An attack launched with the help of zombie drones under the control of black hats using a master program.
- Dumpster Diving - Using trash of an individual or business to gather information for enabling cyber criminal to gain access to a systems.
- Keylogger – Anon-destructive program to log every keystroke made on a computer and saved in a remote computer for black hat.



Terminologies in Cyber Criminal World

- Logic Bomb – A malicious program designed remain dormant and to execute when a certain criterion is met.
- Malware – A malicious program causes damage(viruses, Trojans, worms, time bombs, logic bombs etc.).
- Master Program - A program used by black hat cracker to remotely transmit commands to infected zombie drones.
- Payload – A part of malware program that actually executes its designed task.
- Worm – A virus having destructive self-contained program that can replicate itself.
- Polymorphic Virus - A virus that changes its digital footprint every time it replicates.
- Trojan/Trojan horse - A non-self-replicating virus containing payload capable of data theft and system harm.

Terminologies in Cyber Criminal World

- Rootkit – The most lethal malware works at low system level (sometimes firmware) and almost impossible to remove. Sometimes, replacement of hardware is the only solution.
- Social Engineering – In the territory of black hats, it means to mislead someone for acquiring sensitive and personal information.
- Spoofing – Black hat often hide their tracks by spoofing (faking) an IP address or masking sender information in an email to convince recipient about the authenticity of domain.
- Zero Day Threat/Exploit – From the very first day a particular threat is ever deployed until noticed, reported, documented and added in definition is called Zero Day.
- Phishing – A form of social engineering done by black hats usually by email for gathering sensitive information.

What is Advanced Targeted Cyber-Attack ?

What is Advanced Targeted Cyber-Attack ?

- Advanced Targeted Cyber-attack is an offensive maneuver employed by individuals or organizations or states targeting Information Systems/Infrastructures/networks of other organizations or states or personal devices by various means of malicious acts originating from an anonymous source.
- Objectives -Stealing valuable data, Trade secrets , Intellectual Property, Reputational damage and access to internal systems.
- Advanced Targeted Attacks (ATAs)/Advanced Persistent Threats (APTs) new norm of cyber security.

What is Advanced Targeted Cyber-Attack ?

- According to ISACA study

✓ 21% respondents reported -> Their enterprises victimized by ATA

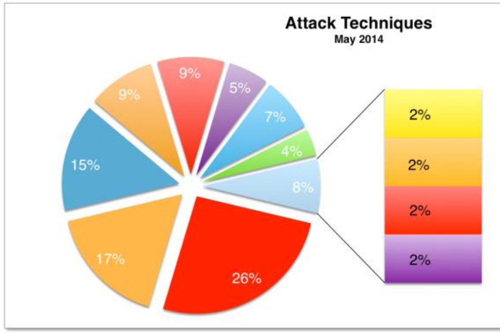
✓ 63% respondents reported -> Only a matter of time before their enterprises are targeted

✓16% - Not Aware

- Traditional security Solutions (Signature based)

✓ Defend against known vulnerabilities and malwares.

✓ Ineffective against ATAs.



- ATAs bypass traditional signature-based security controls and remains undetected in Victim’s systems for extended period of time.

Headlines of Advanced Targeted Cyber-Attacks

1. Headlines in Times of India (23.3.2015): Indian defense personnel continue to be targets of foreign intelligence espionage

- ✓ India’s Defense Ministry warned its personnel that they might become targets of foreign (China and Pakistan) spy agency web attacks, the Times of India reported on Monday.
- ✓ There have been cases of data leaks through pen-drives, portable hard drives and CDs, the International Business Times quoted an anonymous defense official as saying.
- ✓ The official added that China had hacker brigades undertaking cyber attacks.

2. Headlines in LA Times (14.11.2014): Sony Pictures Entertainment was targeted in a hack on 24th November’2014 that forced its employees to boot up fax machines and take calls on landline phones.

- ✓ Evidence suggests that the intrusion had been occurring for more than a year prior November 2014.
- ✓ The hackers called themselves the "Guardians of Peace" or "GOP“
- ✓ The leaked data included following :-
  - ▪ Personal information about Sony Pictures employees and their families
  - ▪ E-mails between employees
  - ▪ Information about executive salaries at the company
  - ▪ Copies of unreleased Sony films,.

Headlines of Advanced Targeted Cyber-Attacks

3.Headlines : Targeted Cyber Attack - Anthem Inc.

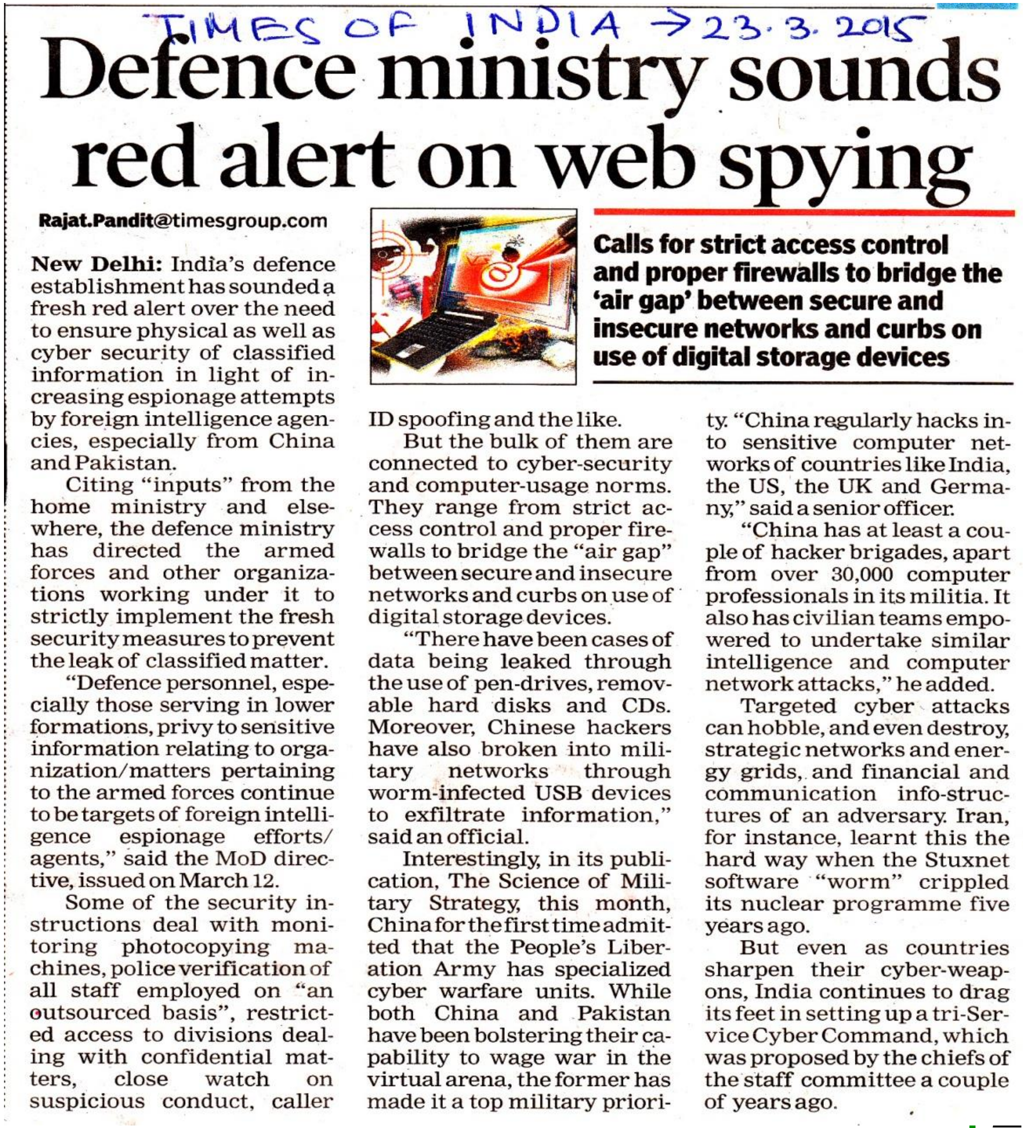
- ✓ Anthem Inc., the second largest U.S. health insurer, said on Feb 4 , 2015 that its computers were hacked and data on as many as 80 million customers and employees may have been exposed.
- ✓ Data leaked : Names, birthdays, medical **IDs/**social security numbers, street addresses, email addresses of current and former members.

4. Headlines, June 09, 2011 : Targeted Cyber Attack -City Bank Inc.

- ✓ Citibank disclosed that hackers broke into its systems and gained access to the personal information of hundreds of thousands of customers.
- ✓ Data leaked : Customer account numbers and contact information, including email addresses. SCMagazineUS.com on Thursday.
- ✓ The bank discovered the unauthorized access during routine monitoring.

Headlines of Advanced Targeted Cyber-Attacks

Headlines 1: State sponsored Cyber Espionage



TIMES OF INDIA → 23.3.2015

Defence ministry sounds red alert on web spying

Rajat.Pandit@timesgroup.com

Calls for strict access control and proper firewalls to bridge the 'air gap' between secure and insecure networks and curbs on use of digital storage devices

New Delhi: India's defence establishment has sounded a fresh red alert over the need to ensure physical as well as cyber security of classified information in light of increasing espionage attempts by foreign intelligence agencies, especially from China and Pakistan.

Citing "inputs" from the home ministry and elsewhere, the defence ministry has directed the armed forces and other organizations working under it to strictly implement the fresh security measures to prevent the leak of classified matter.

"Defence personnel, especially those serving in lower formations, privy to sensitive information relating to organization/matters pertaining to the armed forces continue to be targets of foreign intelligence espionage efforts/agents," said the MoD directive, issued on March 12.

Some of the security instructions deal with monitoring photocopying machines, police verification of all staff employed on "an outsourced basis", restricted access to divisions dealing with confidential matters, close watch on suspicious conduct, caller ID spoofing and the like.

But the bulk of them are connected to cyber-security and computer-usage norms. They range from strict access control and proper firewalls to bridge the "air gap" between secure and insecure networks and curbs on use of digital storage devices.

"There have been cases of data being leaked through the use of pen-drives, removable hard disks and CDs. Moreover, Chinese hackers have also broken into military networks through worm-infected USB devices to exfiltrate information," said an official.

Interestingly, in its publication, The Science of Military Strategy, this month, China for the first time admitted that the People's Liberation Army has specialized cyber warfare units. While both China and Pakistan have been bolstering their capability to wage war in the virtual arena, the former has made it a top military priority. "China regularly hacks into sensitive computer networks of countries like India, the US, the UK and Germany," said a senior officer.

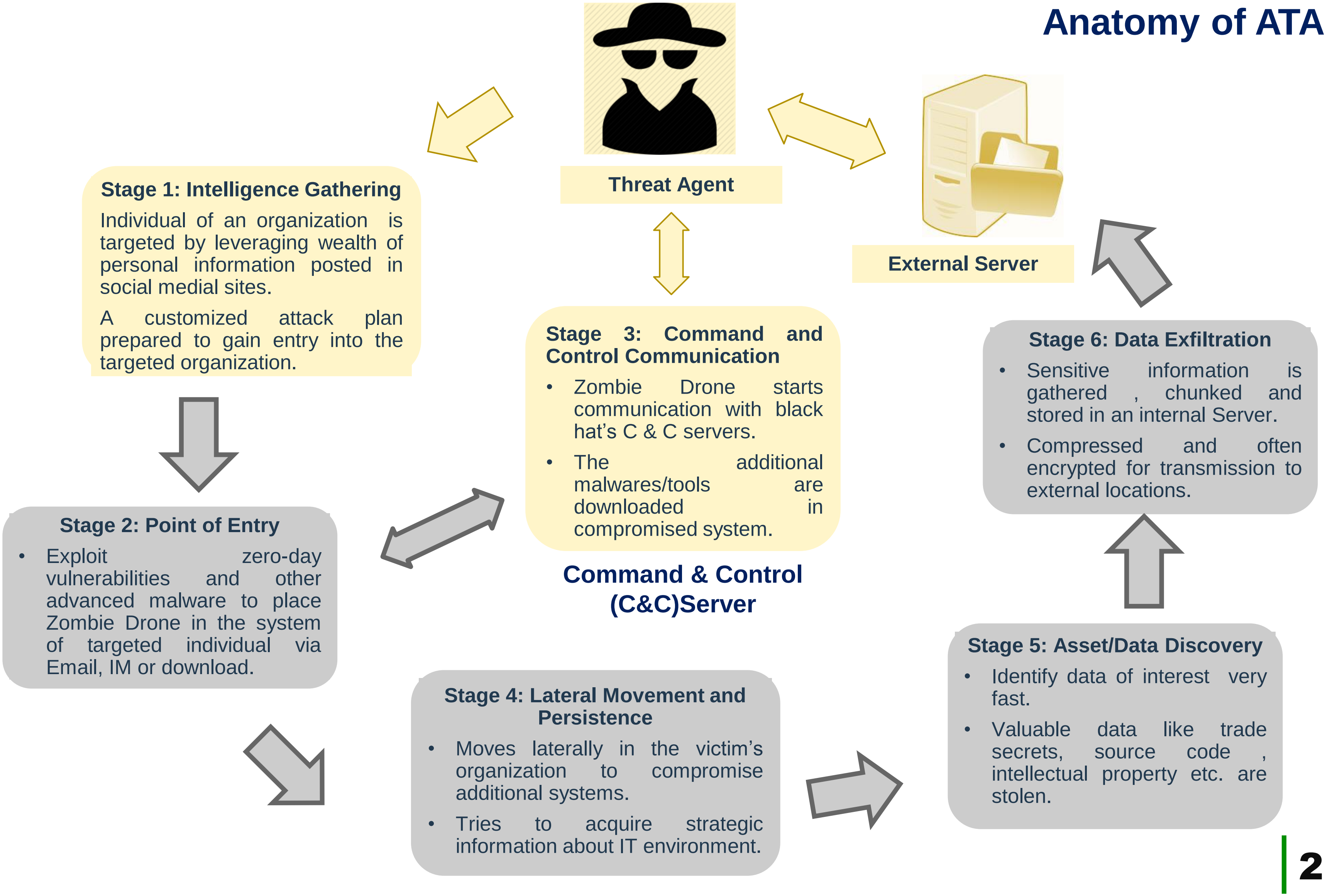
"China has at least a couple of hacker brigades, apart from over 30,000 computer professionals in its militia. It also has civilian teams empowered to undertake similar intelligence and computer network attacks," he added.

Targeted cyber attacks can hobble, and even destroy, strategic networks and energy grids, and financial and communication info-structures of an adversary. Iran, for instance, learnt this the hard way when the Stuxnet software "worm" crippled its nuclear programme five years ago.

But even as countries sharpen their cyber-weapons, India continues to drag its feet in setting up a tri-Service Cyber Command, which was proposed by the chiefs of the staff committee a couple of years ago.

How Advanced Targeted Attacks (ATA) Works ?

Anatomy of ATA



Threat Agent

External Server

Stage 1: Intelligence Gathering

Individual of an organization is targeted by leveraging wealth of personal information posted in social medial sites.

A customized attack plan prepared to gain entry into the targeted organization.

Stage 2: Point of Entry

- Exploit zero-day vulnerabilities and other advanced malware to place Zombie Drone in the system of targeted individual via Email, IM or download.

Stage 3: Command and Control Communication

- Zombie Drone starts communication with black hat's C & C servers.
- The additional malwares/tools are downloaded in compromised system.

Command & Control (C&C)Server

Stage 4: Lateral Movement and Persistence

- Moves laterally in the victim's organization to compromise additional systems.
- Tries to acquire strategic information about IT environment.

Stage 5: Asset/Data Discovery

- Identify data of interest very fast.
- Valuable data like trade secrets, source code , intellectual property etc. are stolen.

Stage 6: Data Exfiltration

- Sensitive information is gathered , chunked and stored in an internal Server.
- Compressed and often encrypted for transmission to external locations.

SMART GRID- CYBER SECURITY FEATURES

Scalability: security performance remain unabated with increase in load and system volume.

Extendibility: able to handle any future state of power grid.

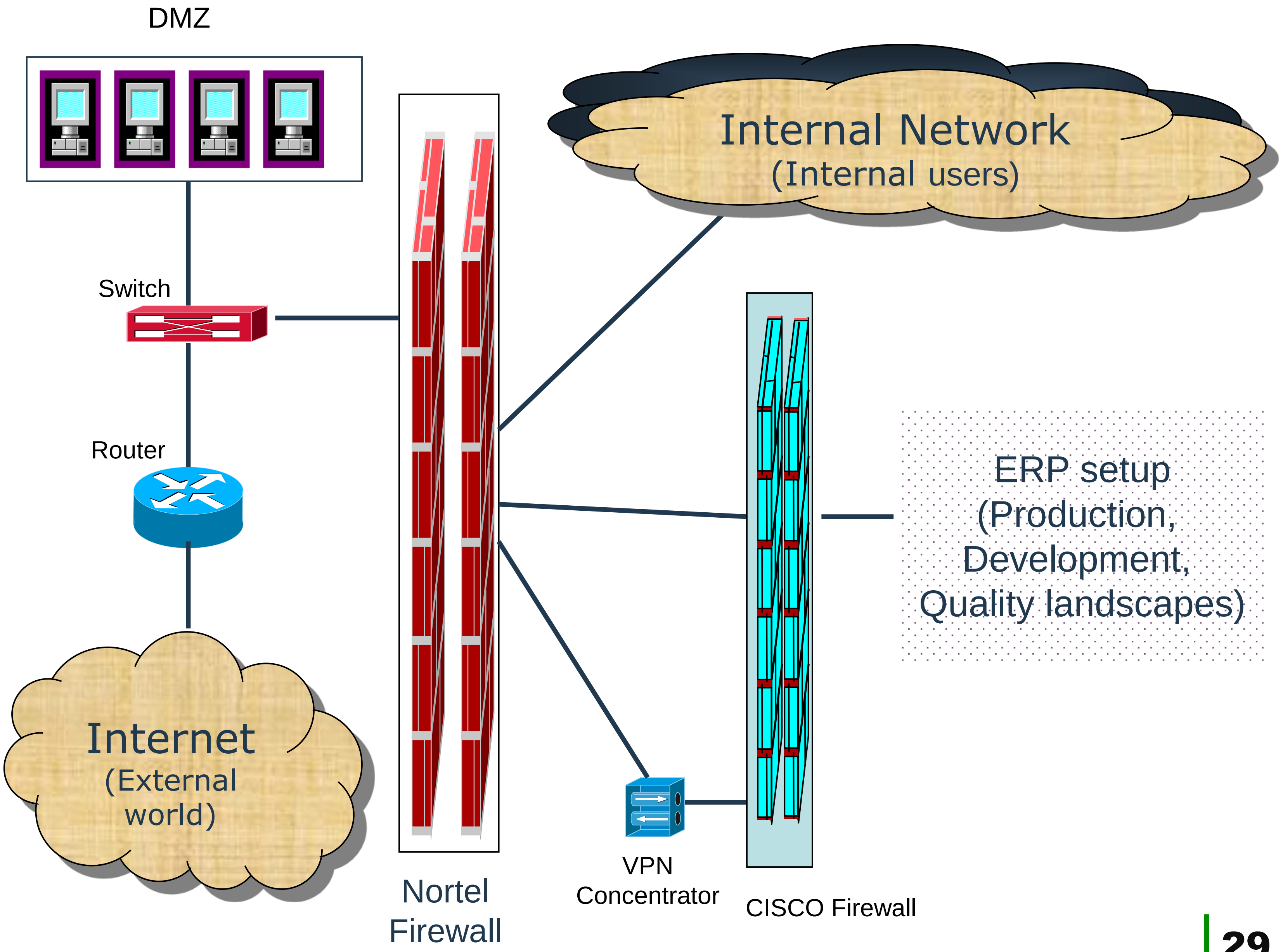
Integral: Can be integrated into the existing, legacy systems into a non-intrusive fashion.

Intrusion Detection System:
a. Anomaly based intrusion detection system.

b. Sound alarms when observed behavior is outside baseline parameters.

Intrusion detection at three levels: **Security agent** performs intrusion detection based on the CPU and memory utilization of the protected device (such as RTU/PLC), scan time, protocol pattern, communication partners, etc. **Managed security switch** performs intrusion detection function based on the delay of data packet, the allocated bandwidth profile, protocol pattern, etc.• **Security manager** performs intrusion detection at the highest level, by monitoring complete grid system and its automation stage.

SMART GRID- CYBER SECURITY MEASURES



SMART GRID- CYBER SECURITY FEATURES

- Single Gateway to External World
- Two Level Firewall
- Intrusion Detection System
- Internet Content Filtering
- Antispam Solution
- Centralized Antivirus/Anti-spam Solution
- VPN for access to SAP from Internet
- Digital Signatures & Certificates
- Information Security Audit

SMART GRID AND CYBER SECURITY

Key points:

Cyber security of the Smart Grid System is not only responsibility of IT department now it’s the responsibility of operation and other departments also.

Grids have develop mechanism to monitor your employees, internal and external customers and other stake holders.

Role based access control to be strictly defined and administered

Periodical audit of the IT and IT-OT infrastructure to be carried out based on the risk involved.

Trainings on latest security issues and their mitigation must be given to concerned persons who are directly involved in cyber security.

Thanks