 <a href="http://d2cigre.org">http://d2cigre.org</a>	CONSEIL INTERNATIONAL DES GRANDS RESEAUX ELECTRIQUES INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS
	<b>STUDY COMMITTEE D2</b> INFORMATION SYSTEMS AND TELECOMMUNICATION <b>2013 Colloquium</b> <b>November 13-15, 2013</b> <b>Mysore – KARNATAKA - INDIA</b>

## **Cyber Security in Implementing Modern Grid Automation Systems**

**(D2-02\_08)**

**By**

**S.R. Vijayan**  
**ABB Ltd.,**  
**Bangalore, India**  
**(91)**

### **SUMMARY**


The modern day power system is transforming over the recent years from the traditional top to bottom (Generation to Distribution to Consumers) power flow to an inter-connected grid, with distributed generation injecting power into the grid at different levels (sometimes even at the consumer point) within the system. It will not be an exaggeration to tell that today's power system network has to embrace the end consumer also into its grid operations. Not only the grid hierarchy has changed, but also the depth of visibility and monitoring the transmission and distribution sub-stations and the network to implement "Situational Awareness" tools for the system operators.

The paper will discuss how the utilities have recognized the need of building the security into their deployments and have started implementing solutions and execute operational practices towards addressing the Cyber Security aspect. It will be worthwhile to note that, addressing the Cyber Security is not limited to building different technical solutions but it is also as much important to have strong operational (or) IT policies within the utility organization. The standardization organizations are working to bring in standards which encompass both these aspects. The paper will highlight some of the standards that are available for deployment.

### **KEYWORDS**

Grid, Substation Automation, Control Systems, Smart Grid



 <a href="http://d2cigre.org">http://d2cigre.org</a>	CONSEIL INTERNATIONAL DES GRANDS RESEAUX ELECTRIQUES INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS
	<b>STUDY COMMITTEE D2</b> INFORMATION SYSTEMS AND TELECOMMUNICATION <b>2013 Colloquium</b> <b>November 13-15, 2013</b> <b>Mysore – KARNATAKA - INDIA</b>

## 1. INTRODUCTION – EVOLUTION OF MODERN DAY GRID

The traditional grids used to be vertically aligned from the source point to the consumption point. The power generation was centralized and the power flow was uni-directional - Generation to Transmission, Transmission to Distribution, as shown in figure 1.

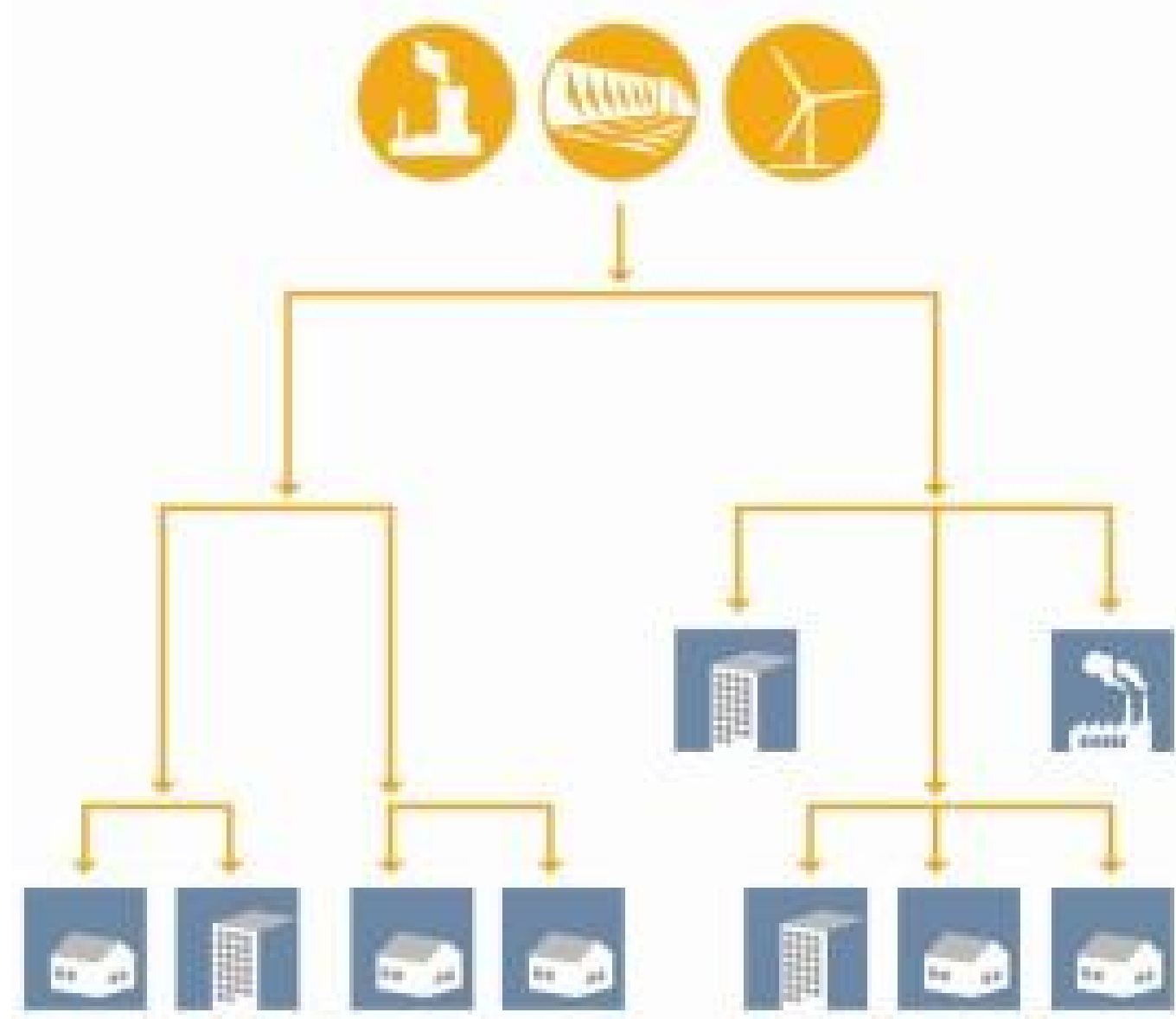


Figure 1 - Traditional Grid

With the power generation through renewable resources (Solar, Wind etc.) becoming more and more prominent to meet sustainability and environmental conditions, the grid connectivity is becoming more complex. It is no more hierarchical and the power flow has become bi-directional. Meaning, the injection points are at the Distribution Network also. A typical diagram depicting the modern day grid connectivity is as shown in figure 2.



Figure 2 – Modern Grid Connectivity

The Power Generation is transforming over the years from the bulk generation to medium and small distributed generation from renewable resources (DERs). This transformation in generation induces new operating grid conditions with increased responsibilities on the grid operators.

The transmission and the distribution sectors too are undergoing through this phase with implementations like

- Wide Area Monitoring (WAMs) applications with Phasor Measurement Units (PMUs), Phasor Data Concentrators (PDCs), Stability analysis tools, SCADA/EMS systems for the transmission network.



□ Distribution Automation Systems like SCADA/DMS, Geographical Information System (GIS), Automated Meter Reading (AMR) (or) Smart Metering. There are also advanced Distribution Automation applications like the Demand Response and the Demand Side Management that are being looked into by many utilities.

This change in the grid inter-connectivity has not only made the electrical connectivity complex, the information exchange between these different systems is also getting complex. The devices and systems that are connected together to exchange data, are moving from serial to IP (Ethernet) based interfaces.

## 2. SUB-STATION AUTOMATION SYSTEMS

Sub-Station automation and protection systems have changed significantly and will continue to change with technology advancements (Figure 3). The devices within the substations are not only connected to controlling system at the higher level but are also getting more inter-connected for implementing interlocks and controls.

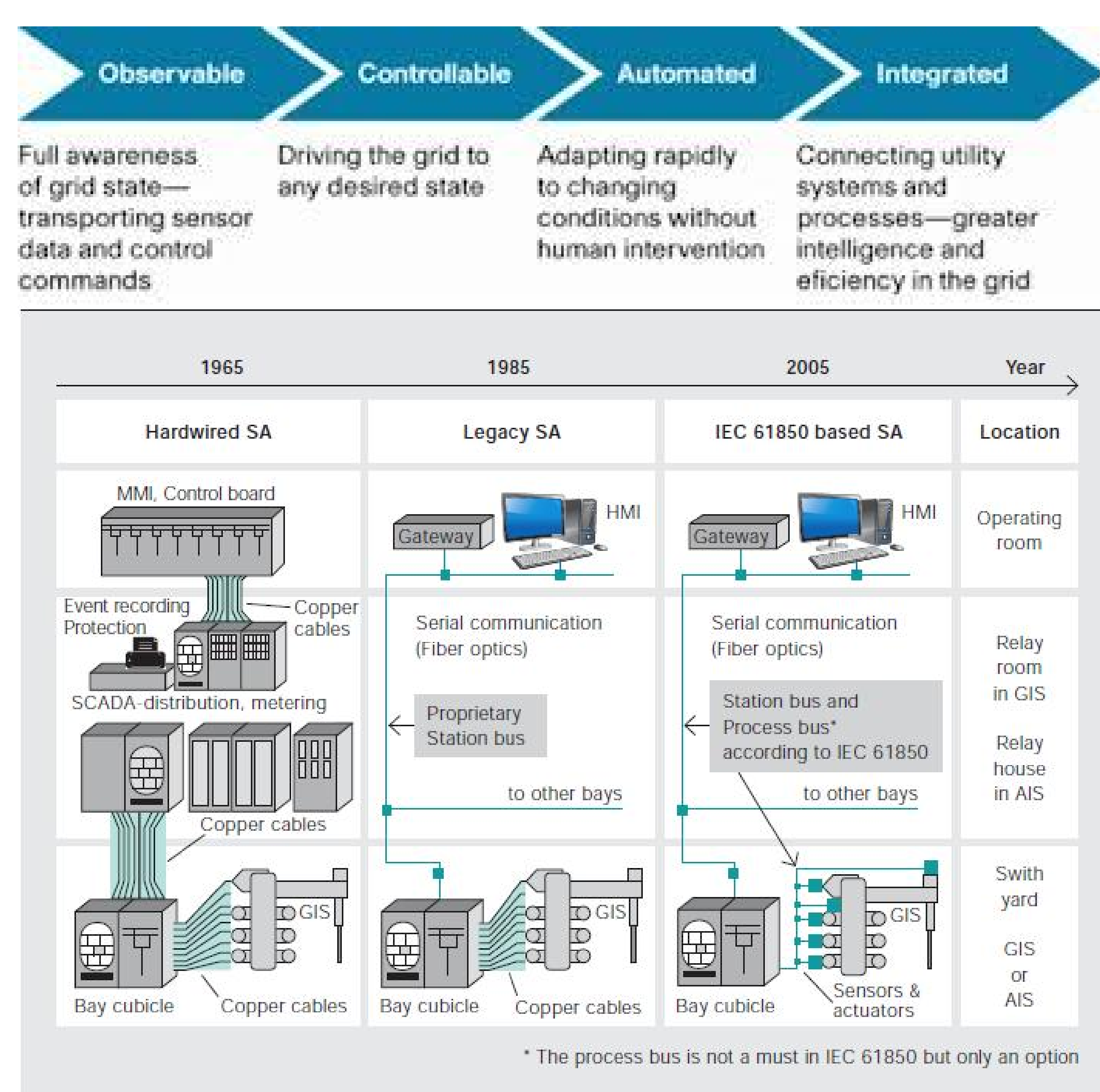


Figure 3 - Evolution of Sub Station Automation

To achieve the level of device and system inter-connections, using the Ethernet/TCP/IP based technology makes systems more inter-operable and the data exchange much faster. Substation with conventional control and relay panels had limitation in control and monitoring of the substation due to the non-communicable relays, centralized architecture and more of manual work for almost every action.

The advancements in the communication and Information technology such as switched Ethernet network, High speed wide area network, TCP/IP leads to the development of IEC 61850 standard based substation automation system. IEC 61850 standard based substation automation system overcomes the limitations of conventional and legacy protocol based substation automation system. Accordingly, the utilities are not only implementing 61850 based systems in the new stations, but are also looking at migration of their old/existing stations to the newer technologies.

While using the Ethernet based technology in the Sub-Station Automation Systems, gives tremendous benefits to the grid operations, they also bring in the threat of viruses, internet based attacks etc.



### 3. SCADA CONTROL SYSTEMS

SCADA systems have been implemented even during the period when the utilities were operating on a traditional grid. However, the changes in the grid connectivity and operations, has made it essential for deployment of various other solutions, to improve the efficiency and increase the Operational Excellence.

As mentioned above there are solutions of WAMS, tools for System Stability Analysis for the transmission network and solutions like Outage Management, Demand Management, Volt-Var Optimization etc for the distribution network being implemented, to make the grid more “Smart” and reliable. As these enhance the operational excellence of the grid operations, these solutions are called the “Operation Technologies”.

With the ever increasing assets, which the utilities own and operate to meet the energy demands, there are IT solutions like Asset Management, Crew or Service Management, Digitization of the network using GIS etc. also being implemented to enhance the planning and decision making capabilities of the utilities.

Further, the need of Data Exchanges between these different system applications makes it necessary to inter-connect them. Now, these systems need not be at the same location (or) even on the same network (Refer to Figure 4).

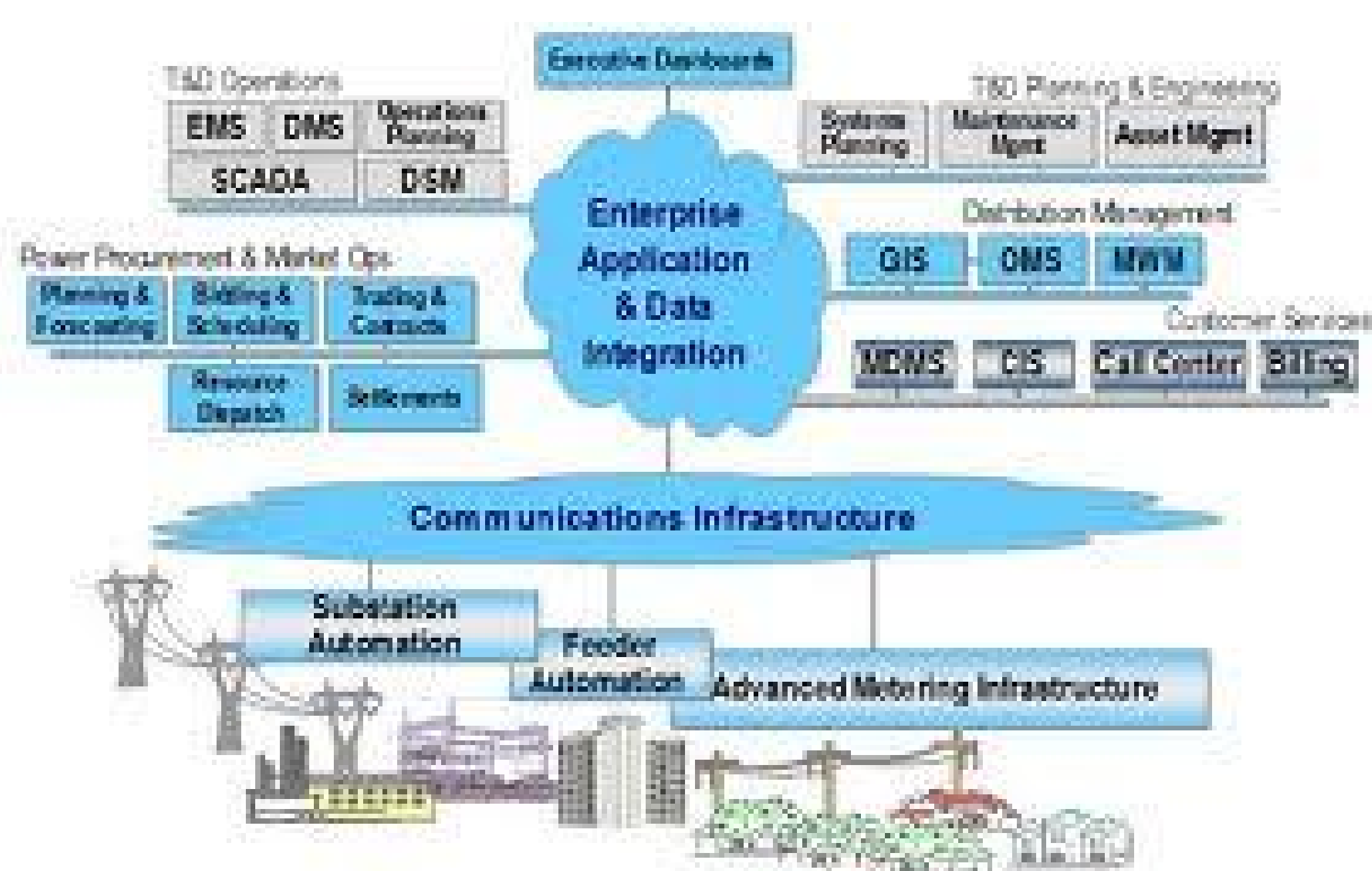


Figure 4 – Inter-Connected System Applications

Hence, the SCADA system stands exposed to the outside world, which makes it vulnerable. This makes the protection of SCADA systems a very critical requirement.

### 4. SMART GRIDS

While the various grid transformations discussed above and the solutions implemented at various levels form a part of smart grid, the smartness extends beyond the assets owned by the utilities to the end-consumer appliances. Applications like Demand Response and Demand Side Management, involves operating the home appliances based on the Time of Day (or) the loading conditions of the grid. This calls for an equal or more participation from the end consumers and an enormous effort by the utilities to have this participation. Hence, the grid operations have to now embrace the end consumers, and cannot be isolated for a successful and effective implementation of such solutions.





Figure 5 - Smart Grid - Connecting Utilities with the consumer

With the evolution of the smart grid, the devices which are neither owned nor controlled by the utilities have to be integrated into the utilities automation system. This creates a new network terminology – Home Area Network (HAN) using the SMART meters and the SMART appliances (refer figure 5).

## 5. CYBER SECURITY – DRIVERS & TRENDS

With the urgent need of making the grid “SMART” to improve its reliability, availability and efficiency, the utilities are facing the challenges of increased necessity of integration between the Information Technology (IT) and the Operational Technology (OT) aspects of the solution deployments. This has made the OT systems which were otherwise in a secure perimeter (physical and electronic) to hand-shake with the external world, thereby inducing a sense of insecurity to the operational assets of the utilities. Thus, when a utility is implementing various solutions and integrating these systems for data exchanges, the systems need not only be interoperable but also need to be secure.

With this backdrop, the cyber security for automation in electric utilities has gained a lot of importance and attention in the recent years. Cyber Security has transformed from a nice-to-have to a must-have for the utilities world over.

While the need and the importance are felt across the utilities, the drivers and the level of implementation may differ. However, the demand for cyber security solutions will increase and become mandatory requirements as part of solutions and products. Accordingly, the standards organizations are also taking up the standard’s development activities on priority. We will see some of such standards in the coming sections of this paper.

## 6. CRITICAL FACTORS SURROUNDING CYBER SECURITY SOLUTIONS/FEATURES AND ITS MITIGATION TECHNIQUES

Deploying security measures / solutions for protecting the automation systems is neither an off-the-shelf product nor a one-time investment. The solution is not limited to deploying a very high end technology alone. It involves people at various levels and the processes in place, within an organization. Hence, the process of having a secured system should be a continuous one.

There are different aspects that have to be taken into consideration for a secured system. Some of them are as listed below

- People and Identity
- Data and Information
- Application and Process
- Physical Infrastructure



*People and Identity:* The user who logs in and operates the system has to be properly identified with a username and password. This login authentication has to be combined with Role Based Access Control (RBAC), so that even authorized personnel can operate only the area/zone that he is responsible for. Here, it will be good to note that, though the solutions around restricting the people access with role based authentication is a natural requirement in any security architecture but is never stronger than implementation itself.

*Data and Information:* Another most important factor is protection of data and information. There are various types of data and information.

System Related: System Architecture, Computer Names, IP Addresses.

Operation Related: Cost, planning data, system operation data.

Data Pertaining to Security Mechanism itself: Username/Passwords, Encryption keys, Quality of Service and Access Policies defined in firewall.

Network Partitioning is implemented to fence the secured zone (real time operational systems like servers, operator work stations etc.) from the unsecured zone (systems in the external network). A de-militarized zone (DMZ) is created by using replica servers, which has upstream and downstream firewalls to give access to external systems for monitoring purposes. A typical diagram depicting the network partitioning for a control center system is shown in Figure 6.

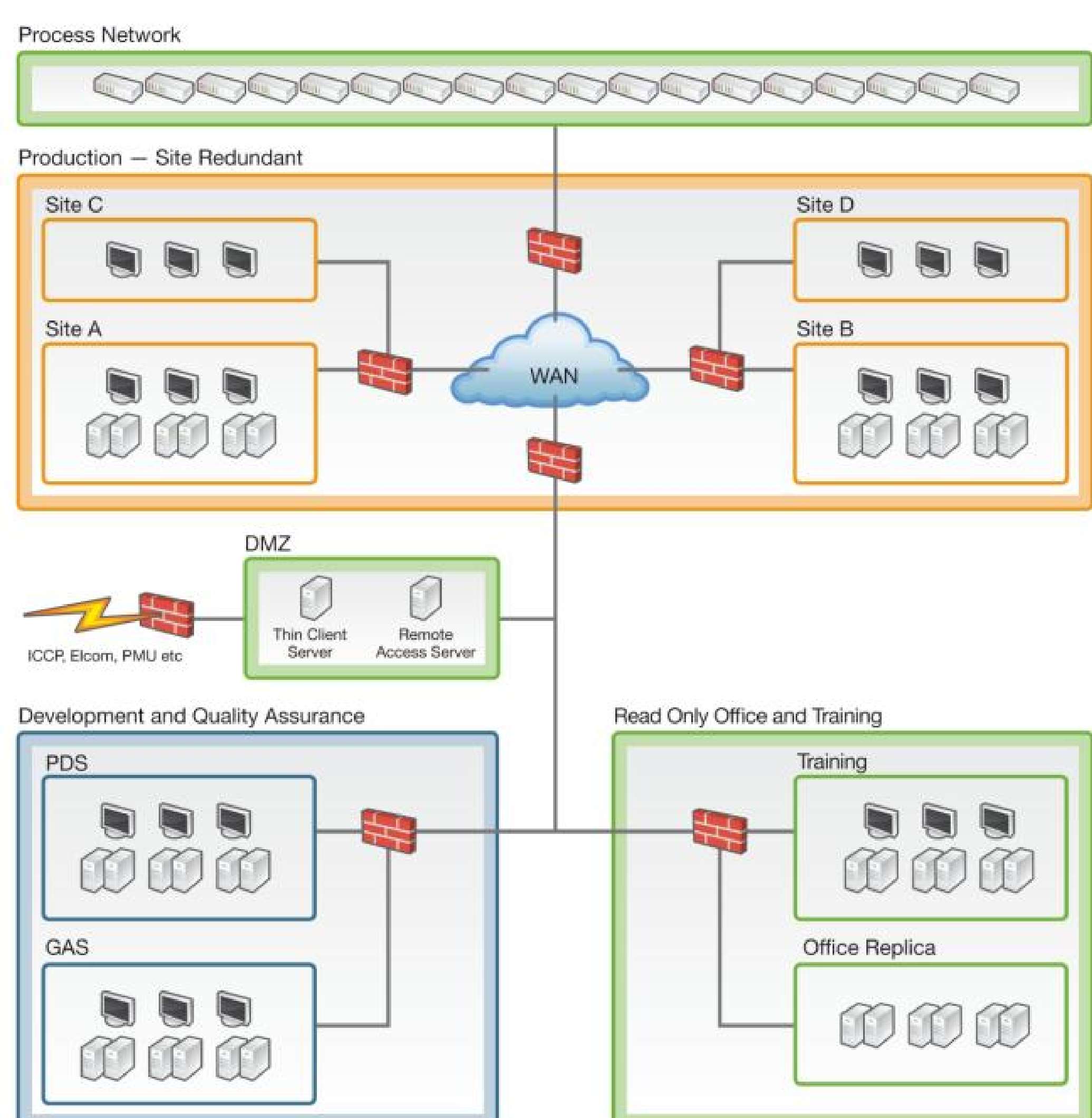


Figure 6 – Control System architecture with electronic perimeter protection

Intrusion Detection/Prevention systems are deployed to monitor, and perform log management of all devices in a network and use the Security Information and Event Management (SIEM) to detect and possibly respond to anomalies in the system. Quality of Service and Access Policies are defined in the firewall to ensure that only mission critical applications, services, ports, and devices are allowed access.

*Application and Process:* The security features on applications and process talks about Patch Management and Anti-Virus protection.

Patch Management: Processes and technology to insure that all available security updates that are verified not to interfere with system operation are installed in all hosts.

Anti-Virus Protection: Employs blacklist, heuristic, and behavioral detection and prevention of malware.



*Physical Infrastructure:* It has to be ensured that the critical assets are installed in a secured area and this area shall be explicitly displayed as “SECURED”. This includes identification of a Physical Security Perimeter with its access points and measures to control physical access to the perimeter.

The physical access can be controlled and protected by various means like card keys, special locks, security personnel, and other authentication devices etc. There can be intrusion detection alarms when there is a forced access into the “SECURED” area.

## **7. INTERNATIONAL STANDARDS AROUND CYBER SECURITY**

### **NERC-CIP**

The North American Electric Reliability Corporation (NERC) has established a Critical Infrastructure Protection program, popularly known in the industry as CIP, which is an effort to improve physical and cyber security for the bulk power system as it relates to reliability.

The following (Refer Table 1) are the different CIP standards that are in reference are

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

Table 1 CIP Standards

While majority of the CIP requirements are applicable to the utilities, CIP 007 which addresses password management, access rights, computer Operating System hardening, event logging, patch management, change control, and test procedures are related to the real time system deployment.

### **NIST Smart Grid**

NIST (National Institute of Standards and Technology) is working on the various smart grid activities and cyber security has got a lot of attention as part of its activities. There is a draft document from NIST – “Smart Grid Cyber Security Strategy and Requirements”, which contains the high level security requirements.

### **IEC 62351**

IEC 62351 is power system specific standard that aims to secure communication protocols like IEC61850 or IEC 60870-5-104. While, some parts of the standard has been released in 2009, there are still modifications being done. As this standard is under development/modification, it will take some time for the systems compliant with this standard to be available in the market.

As can be seen from the above brief descriptions, cyber security encompasses both the technical perspective – products, solutions and systems being implemented and the policy/process perspective within an organization.

## **8. THE FINAL WORDS**

*Protect, Detect and Respond:* The implementation should be able to minimize the attack surface, detect possible attacks and respond in an appropriate manner to minimize the impacts

*Defence in Depth:* No single security measure itself is foolproof as vulnerabilities and weaknesses could be identified at any time. In order to reduce these risks, implementing multiple protections in series avoids single point of failure.

*Technical, Procedural and Managerial measures:* Technology is insufficient on its own to provide robust protection. Cyber security policies and processes must be implemented in the organization to best be able to assess and mitigate the risks and respond to incidents.

There is no such thing as 100% security or a 100% secured system. Hence, implementing solutions around the cyber security has to be a continuous one. Therefore, it's not only important to protect a system from the current vulnerabilities, but is also equally important to have mechanisms (technical and process) in place to quickly detect and effectively react to any incidents and isolate security breaches.