Communication Challenges for Electric Power Transmission Systems

Spiros Chountasis

Independent Power Transmission Operator, Asklipiou 22, Krioneri, 14568 Athens, Greece
schountasis@admie.gr

Keywords: Critical Infrastructure Communications, Supervisory Control and Data Acquisition (SCADA), Security Trends, Telecommunication Protocols.

Abstract. Uninterrupted electric power supply and transmission is a part of critical infrastructure for any nation’s security, economy and healthcare systems. Essential requirements for operating and managing an industrial control system is the secure and instant data transfer between control centers and generation stations or substations. This paper review the general Energy Management System architecture implemented for the Hellenic Power Transmission System. The major contribution of this study is to provide a possible direction to the most appropriate SCADA system communication, indicating the most important security factors. A brief study of the communication protocols is also presented. This work focuses on the key role of telecommunication provision for critical distributed control infrastructures. Based on the relative analysis presented in this paper directions towards a secure critical infrastructures network communications are provided.

Subject Classification Numbers: 68M01, 68M10, 94A05.

1. Introduction

The electrical power network is described as a most critical infrastructure. The safety and the reliability of the systems and operations associate with is a major matter. Telecommunication for an electric power supply system has a long history in the transmission level. In today’s Hellenic Power Transmission System (IPTO), all the generation stations and substations (SSs) are monitored and most of them are controlled online by Energy Management Systems (EMS). Two Control Centers (CCs) that communicate to each other are receiving analogue and digital measurements obtained by field devices from SSs. These quantities are evaluated in the CC and operational messages are forward accordingly to the actuators that drive the field devices of the SS. Figure 1 illustrate that comprehensive operational control loop:

![Figure 1. An electric power system control loop](image-url)
The measurements from SSs and the operational messages from the CC are sent through dedicated communication lines using standard telecontrol communication protocols. The powerful role of these systems together with their tradition nature, making them an significant target for those who want to disrupt normal electric power transmission and distribution creating chaos. Supervisory Control and Data Acquisition (SCADA) system is responsible for monitoring and controlling our critical infrastructure. It is typically composed of proprietary software and hardware components designed specifically for electric power transmission, mostly in isolated environments. The increasing interconnectivity of SCADA network has exposed it to a wide range of network security problems [2, 9, 3]. Moreover, the inadequacy of secure methods and strategies in industrial communication presents a serious risk for the organization. The smooth and genuine operation of the system is one of the key concerns for the enterprises, because the consequences of breakdown of the framework may range from financial misfortune to natural harm to loss of human life.

There are many qualified organizations associated to the standardization and improvement of SCADA network security, but still there many open issues. The reluctance of companies to release incident information along with the possibility that some or many incidences go unnoticed makes it difficult to accurately assess the risk. This work depicts the general communication network architecture of the IPTO and presents some of the frequently used SCADA communication technologies. The overall goal of this research is to provide an overview of the urgent communication issues that are engaged in the operational power systems in order to strengthening the security of an EMS/SCADA network. The generic security threats in those networks are also discussed. Another aim of the paper is to provide the advantages of the existing EMS security strategies providing a study of the challenges facing SCADA networks.

SCADA systems can be standing unprotected when Internet technologies are accommodated. In network architectures where traditional SCADA systems are connected to modern business IT systems, conventional IT security solutions must be reconsidered. Multiple test scenarios must be successfully completed prior to their deployment on SCADA networks. The connection of permeable and less secure corporate networks to once isolated SCADA networks, using commercial-off-the-shelf (COTS) hardware and software, has unintentionally exposed SCADA systems to a host of vulnerabilities and threats for which it was ill prepared. There are several reports associated to networks security when SCADA systems are engaged [7, 8, 14, 13]. Motivated by these works, the current paper studies some major aspects of the communication security in EMS/SCADA networks. The investigation is based on communication architectures approved by IPTO. The security policy will benefit from the categorization provided on IPTO systems and the given communication technologies. The smooth and genuine operation of EMS/SCADA framework is one of the main concerns for the organization and the purpose of this work. Power applications require a secure communication infrastructure confronting the geographic disperse resources.

The outline of this paper is as follows. Section 2 describes the communication technologies that are currently used in IPTO. Section 3 provides the architectures in SCADA communication and Section 4 classifies the EMS communication requirements. The EMS/SCADA communication security strategies are discussed in Section 5. Finally, the conclusions are presented in Section 6.

2. Communication Technologies for Power Transmission Networks

The 400kV/150 kV power transmission lines on IPTO are equipped with optical fiber cables. These cables are integrated by Optical Ground Wire (OPGW). Most of the SSs are also accessible via leased communication lines. In the case where the installation of optical fiber cables is not economical or leased communication line solutions are not physical possible, SSs are bridged through power line carrier communication systems.

The communication needs in a transmission level environment differs from that of a widely telecommunication environment. Therefore, it is essential that the appropriate communication technologies are deployed, depending on availability of optical fiber cables, frequency spectrum for leased wireless telecommunications, or length and quality and of the power line communication
cables. Sometimes a tailored mix of these technologies is mandatory. To minimize potential attack surfaces, we need to separate or segment different types of communication networks. Depending on the utilities needs the most notable types of communication technologies in the IPTO are the following:

- Optical Communications
- Power Line Carrier Communication
- Leased Communication Lines by telecommunication providers

These technologies will be briefly discussed in the following sections.

I) Optical Communications

Optical communication technologies are based on light wave systems that utilize optical fibers for data transmission. Fiber optics is the best transmission medium. Some of the reasons are: can be easily installed and maintained, are reliable for being not susceptible to electromagnetic interference, can be used for most data and easily upgraded. Moreover, it has practically unlimited transmission capacity. The IPTO communication functions ordinarily operate using the following two types of fiber optic cables.

a) OPGW that is a standard type of cable located at the top of the high voltage pylons, incorporating both electrical conductor and optical fibre. It is housed on a stainless steel tube installed along the power transmission line route.

b) Fiber-optic cables that are laid subterranean connecting individual SSs with the CCs. The installation is associated with excessive and costly construction works. In IPTO case, this service is part of the leased communication lines.

The IPTO deploys two optical communication technologies.

a) Plesiochronous digital Hierarchy (PDH)
PDH designed for proper transmission of a large amount of data over digital equipment. It employs a multiplexing method that is pseudo-synchronous. The basic data transmission rate that is supported is 2,048 Mb/s. In order to transport the data in the long distance data streams are multiplexing in group of four. It must be functioned for the high bit rate channel down through all multiplexing levels until the optimal rate is located. PDH systems fall short in terms of network management and synchronization, and therefore, they are steadily replaced with newest technologies such as Synchronous Digital Hierarchy (SDH).

b) Synchronous Digital Hierarchy (SDH)
As digital telecommunication increased in complexity, new standards for multiplexing technologies developed. The SDH is an international comprehensive set of standards designed for high speed transport channels. It combines data streams of low bit rate to form high rate data streams on a simple and flexible synchronous clock network. It was designed to have a greater channel capacity, improved network management including protection/recovery mechanisms for the services.

Today, SDH technologies combined with PDH access multiplexers are in operation and they provide a justified solution for the communication requirements of the IPTO. Considering the growth of power transmission network and the implementation of future power transmission systems, higher capacity optical communication system based on Dense Wavelength Division Multiplexing (DWDM) can be introduced. DWDM is a technology that by sharing a single optical fiber pair transmits optical signals with different wavelengths from different sources. An optical link in DWDM has several optical components such as optical fibers, optical amplifiers, optical add-drop multiplexers (OADM), laser sources and transceivers.
II) Power Line Carrier (PLC) Communications

Power line carrier (PLC), is a power system technology employed in the high voltage network that utilizes the existing infrastructure of power transmission line in order to transmit and receive the data. It has been developed as one of the most economical and reliable forms of communication solution which offers a broad coverage in power systems. PLC communication is still a viable part of IPTO main telecommunication infrastructure. It serves as a robust and an economical way to provide digital communication and transmit protection signalling to SSs with no other connection access.

A basic PLC communication system consists of the following components: transceivers, line matching units, coupling capacitors, line traps and of course the power transmission lines as communication media. Such communication systems can be categorised according to their frequency bandwidth usage into the following technologies:

a) Analogue PLC
The analogue PLC communication technologies use single side band modulation with reduced carrier that operates in 30 to 500 kHz frequency range. Normally a bandwidth of 8 kHz is used for simultaneously transmitting and receiving data and voice.

b) Digital PLC
The last main evolution in the field of PLC has been the introduction of digital PLC communication systems. It provides more efficient use of the frequency band, higher transmission capacity, data compression and implementation of digital signal processing modulation. Based on that:

- the output signal of digital PLC is in the same frequency range as that of an analogue PLC and
- the line traps, coupling capacitors and line matching units are totally compatible with digital PLC

The IPTO is conveniently adopting this technology to all new SSs successfully. The bandwidth and transmission rates provided by the PLC communication systems depend on the quality of the power transmission lines, in terms of efficient coupling and attenuation. The age of the power lines cable and the coupling equipment have a positive impact on the achievable results.

III) Leased Lines Communications

The situation in Leased Lines communication is quite different in that telecommunication providers offer a solution where the telecommunication routing and usually the medium of it are unknown to the clients and power transmission system operators. The selection of a communication solution depends on the IPTO operators. Mostly heterogeneous communication networks are provided that consists of fiber optics communication and wireless communication technologies. Lately Ethernet technologies also play a vital role in the leased lines communication backbone.

3. SCADA Communications

An electric power system consists of interconnected power grid elements where electricity flows from power generators to consumers over a link of transmission lines and distribution feeders as shown in Figure 2.
An integral part of electric power system is the SCADA system that is responsible for the primary functionality of monitoring, recording, reporting and controlling automation operations taking place in a transmission SS. SCADA can be described as a centralised event driven system. Numerous Remote Telemetry Units (RTUs) topographically distributed in the country are connected to a central unit - master terminal, the CC. RTU is a devices that collect SS operational states from sensors (analogue or digital) and route control signals. Signal delay is not an option for SCADA system that often has finite connection speed and limited processing power. Generally, control systems tend to be different from traditional IT systems in several ways as shown in Table 1.
Table 1. Differences between SCADA and Traditional IT systems

<table>
<thead>
<tr>
<th>Category</th>
<th>IT Systems</th>
<th>SCADA Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance</td>
<td>• High throughput,</td>
<td>• Medium/low throughput,</td>
</tr>
<tr>
<td></td>
<td>• tolerate delay or jitter</td>
<td>• no tolerate delay or jitter</td>
</tr>
<tr>
<td>Quality of Service</td>
<td>• Not time sensitive operation,</td>
<td>• Uninterrupted operation,</td>
</tr>
<tr>
<td></td>
<td>• not necessary real time monitoring,</td>
<td>• highly sensitive to errors for long periods of time</td>
</tr>
<tr>
<td></td>
<td>• rebooting or shutdown is an option</td>
<td></td>
</tr>
<tr>
<td>Communication Protocols</td>
<td>• Operating systems protocols</td>
<td>• Different proprietary communication protocols</td>
</tr>
<tr>
<td></td>
<td>• Standardized IP - based protocols</td>
<td>• Not include security mechanism</td>
</tr>
<tr>
<td>Security Architecture</td>
<td>Protection on core internal systems</td>
<td>Protection on the edges (perimeter devices) and the core internal systems</td>
</tr>
<tr>
<td>Priority of Security</td>
<td>1. Confidentiality</td>
<td>1. Availability</td>
</tr>
<tr>
<td></td>
<td>2. Integrity</td>
<td>2. Integrity</td>
</tr>
<tr>
<td></td>
<td>3. Availability</td>
<td>3. Confidentiality</td>
</tr>
<tr>
<td>Component Lifetime</td>
<td>3 - 5 years</td>
<td>15 - 20 years</td>
</tr>
<tr>
<td>Physical Accessibility</td>
<td>Easily accessible</td>
<td>Isolated and remote, may be very difficult to access</td>
</tr>
</tbody>
</table>

Communications on a SCADA network is paramount. In order to correctly incorporate them it is vital to have a deep knowledge of the potential standards and technologies [19, 11, 12]. Accordingly, the IPTO inherits the following IEEE standards for its operating communication network:

- IEEE 802.1 - for LAN/MAN bridging and management and remote media access control bridging.
- IEEE 802.2 - for Logical Link Control connectivity.
- IEEE 802.6 - for information exchange between systems.
- IEEE 802.8 – Fiber optic connection.
- IEEE 802.9 - for integrated services.
- IEEE 802.10 - for LAN/MAN security implementations.
- IEEE 828 - Configuration Management in Systems and Software Engineering
- IEEE 1547 - for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces

Its communication architecture with the RTUs is shown in the block diagram presented in Figure 3.
The RTUs (total number of 450) are installed at unmanned or partially manned 150kV and 400 kV SSs that interconnected to the CC (SCADA master station) through separate communication channels for redundancy reasons. Three generic data communication telegrams can be identified among the master station and the SSs in electric power transmission utility:

i) At least one message is transmitted; receipt confirmation or retransmission upon loss is not required.

ii) One message is transmitted; a receipt acknowledges is required otherwise the message is retransmitted.

iii) Two messages ‘select’ and ‘confirm’ are transmitted, respectively. The latter verifies the correct response of the device upon the selection message. Consequent to the confirmation a message ‘control’ is sent followed by an acknowledgment revealing that the message is accurately received. The whole process is also known as ‘select-before-operate’.

At the moment, Alstom’s EPC3250 (HNZ) communication protocol is mostly used where for the newest SSs the IEC-60870-5-101 protocol is also required for implementation. In 1995 the IEC-60870-5-101 (IEC-101) protocol released, by the International Electromechanical Commission. A communication standard for electric power systems that involves monitoring and regulating operations. Its successor, the IEC-104 was proposed a few years later. Although the IEC-104 does not support all the available by IEC-101 functions it enables the Transmission Control Protocol/Internet Protocol (TCP/IP) transmission. This combines the application messages of IEC-101 with the, which itself introduces. Within TCP/IP communication frame, manifold security challenges are introduced. A serious vulnerability of the protocol is that the data at the application level is transmitted without authentication or an integrating encryption mechanism, making the protocol most accessible and the most exposed to the outside world [16, 20]. To preserve the SCADA system network protection, fundamental telecommunication issues such as concrete security-related protocols must be considered [4, 15]. Two categories of exposures can be distinguished related to protocols. Firstly, the protocol built-in vulnerabilities associated to the specifications and secondly, the improper implementation of the protocol. These vulnerabilities
lead to the ability of a cyber attacker to control RTUs or even operate an automatic SS resulting in disastrous consequences [10]. The IEC 61850 standard was initially designed to manage applications/communications within the substations. Recently, an undergone research work for supporting distributed intelligence has been presented [21]. Security issues for the employment of the IEC 61850 in the context of distribution automation environment also being considered.

Current communication networks equipped with TCP/IP based systems ensure major amount of operational data transfer through greater bandwidth and higher availability channels accessed. TCP/IP is not appropriate for device control and monitoring due to its non-deterministic latency. Its “slow-start” nature causes an unforeseen performance [1]. Protection is a major concern of these open architecture technologies, compared to isolated private networks communicate with proprietary protocols. The propagation of data via public or private communication channels in a standard format pose a significant security risk. Additionally, modern network security techniques such as authorization, authentication, and encryption demand extra bandwidth, processing power, and memory. Typical power control system components cannot retain these requirements as they are not intended for telecommunication networking. Developing reliable communication technologies, protocols and standards could provide SCADA system personnel with the required tools for adequate development and secure implementation. A case study of an encrypted real-time exchange data is followed.

### 3.1 Case Study – Exchange Real Time SCADA Data via ICCP/TASE.2 Protocol

The IPTO’s EMS is able to exchange real-time SCADA data with other Control Centers utilizing the standard communication protocol IEC 60870-6 TASE.2 / Inter Control Centre Protocol (ICCP). The majority of IPTO’s TASE.2 is used with TSOs of neighboring countries in order to comply with European Union requirements related to energy transfer. The data is used for the State Estimation and Security Analysis of IPTO’s observability area. Moreover, the ICCP system is exchange data with a European Awareness System. It's a real-time platform for monitoring the current state of Europe's interconnected power transmission infrastructure in order to respond promptly in the event of major outages. The ICCP servers communicate with encrypted ICCP in complying with the European cyber security directive.

In a non-secure ICCP communication link an ordinary network analyzer could capture the data which is in plain text. The data in an ICCP packet is transmitted in plain text and may be easily retrieved by such a device that intervenes on the network. The network analyzer is able to monitor the internet protocol (IP) packets that are sent across the network. The header, the destination address, and the data content of these IP packets all follow a standard structure. In a secure ICCP communication link the data is encrypted using the certificates installed on the ICCP server. Thus, the server ensures and validates the integrity of data. Figure 4 illustrates the configuration settings for operating a secure ICCP link.
A server for certificate validation is required in order for the IPTOs transition to a run-time secure ICCP communication link. The server obtains relative information from SCADA and ICCP systems enabling encryption certificate management and establishing secure ICCP communication links.

4. Classifications of EMS Communication

The technical evolution of data communication systems has opened up new possibilities to power control systems. Closed system architectures are changing into interconnected or even integrated computer systems that support new functionalities that are also user friendly and cost efficient. This give rise to harder security issues generating new power system security challenges. The best approach to a reliable monitoring and precise controlling process is to provide robust and secure communications for the SCADA system applications. In our days most of the vendors are utilizing COTS products as part of their EMS/SCADA systems instead of using ‘tailored’ solutions providing custom-made systems.

The considerations that lead to the EMS/SCADA system security risk escalation can be summarized as follows:

a) Adoption of commercial technologies well exposed with proven vulnerabilities. Proprietary hardware devices, software applications, and network protocols make it hard to grasp how critical operations accomplished by EMS/SCADA systems. Black-hat hackers will be investigating plenty of time to understand and interfere to the system.

b) CC systems connectivity to corporate networks for business applications as they may employ wide area networks and Internet services. EMS/SCADA systems must have limited access, for monitoring only.

c) Insecure remote connections, such as leased communication lines, wide area network links, and radio/microwave links occupied for data transmission between CCs and SSs.

d) Availability of detailed technical information about critical control systems and operations.

For protection of an EMS/SCADA system a separation of operational and administrative IT environments must be obtained [5]. Variations in response time and that of latency are critical for control operations. For control signals bandwidth is not important in general but reliability is. This is opposed to other non-operational implementations such as video surveillance where bandwidth is required. Combining the different requirements in a single easy to implement solution is a hard and
challenging task. Several solutions are available but these mainly focus on carrying all communications over IP. For SCADA, power stations and SSs, this sets a requirement of using devices converting traditional serial port (RS-232) based traffic to IP (Ethernet) based traffic thus utilizing COTS products. On the other hand installing new natively IP enabled equipment is not an economically viable solution since SCADA system have a relatively long life span. On the basis of these requests, EMS/SCADA communication requirements should be classified into the following four categories:

I) **Real-time operational data communication requirements**

Real-time operational communication includes all the real-time data communications that is essential to sustain operation of the electric power system. It is characterized by the fact that real-time data exchanged, for teleprotection purposes and power system control must take place with hard time requirements.

- For teleprotection purposes, messages should be transmitted within a very short time frame of just a few milliseconds, usually 10-20 msec. It originates from the necessity that the fault-current disconnection must be performed within approximately 100 msec.

- For power system control, measured values must not exceed 15 sec, when appear at the CC. Breaker status must be reported within 2 sec after the occurrence of the event.

II) **Real-time operational voice communication requirements**

In the case of a disturbed power operating incident the actual prospect of providing voice contact is considered, by the CC personnel as one of the most important service. PLC telephone system is part of real-time operational voice communication system.

III) **Administrative data/voice operational communication requirements**

In addition to real-time data operational communication, available information is required after significant power system disturbances happened. This type of communication is characterized by the fact that data analysis not need to occur in real-time but abnormal events has been recorded for future evaluation. Moreover, operational voice communication also encompasses the voice recorded procedure, a procedure necessary for the normal operation of the system and the future development process. Examples are the Historical Information System (HIS) a powerful, scalable archive system able to process very large data volumes and voice recorders.

IV) **Administrative communication requirements**

Administrative communication involves all the communications that are de-coupled from the EMS/SCADA operational communication requirements. It also includes telecommunication services from geographically dispersed locations. The de-coupling of the energy control network from the corporative network is one important step toward a more secure system state [6].

Generally, the EMS/SCADA system is inflexible, static and follows centralized architecture that limits system interoperability. On the other hand integrating an amalgamation of industrial and business systems is more prone to attacks in comparison to the traditional EMS due to the larger exposed space.

Overall, the network architecture must be composed by two types of foundation networks: the corporate network and the energy control network. For the former, the operations are more business oriented where for the latter all the operational tasks are carried out. To ensure the functionality of the independently networks the above restrictive categories must be pursued thoroughly.
5. EMS Communication Security Strategies

The current EMS communication architecture in the IPTO is considered as a central structural model as can be identified in Figure 5.

![EMS central structural model](image)

**Figure 5.** EMS central structural model

It follows a module-specific approach i.e., the system contains modules such as the SCADA, the Automatic Generation Control etc. Each module may include many subsystems for example the AGC module has the following subsystems: load frequency control, economic dispatch, generation scheduling, transaction scheduling, etc. These modules are inter-connected and confined inside small range network, Local Area Network (LAN) resulting in more processing power, redundant and reliable system. Wide Area Networks (WAN) is used for intercommunication between RTUs and CCs. SCADA operations are distributed across a back-up CC through WAN providing reliability and scalability and handling disaster recovery issues. Reliable communication across a WAN is often achieved by means of a SDH technology over fiber-optics rings. The redundancy provided by the SDH network make it a viable choice for efficient communication in critical electric power transmission applications. A LAN can be linked to a WAN through multiplexer devices as shown in Figure 6 where four sites at different geographically location are linked through a SDH communication ring.
The encrypted fiber-optic ring protects the most exposed portion of the communication channel that is not in a physical building, CC or SS. The multiplexer devices also support advanced security encryption methods making them suitable for the electric power industry.

Current generation of EMS/SCADA system architectures is closely related to our central structural model with the significant difference in the deployment of open standards and protocols for communication rather than proprietary protocols. Due to the usage of open standards peripheral devices which are located across multiple SSs can be connected to SCADA network using Internet Protocol (IP). SCADA connectivity with open protocols and networks over internet significantly improved. Networked SCADA open new ways to connect several types of input/output devices or COTS systems but also make EMS/SCADA system more vulnerable from several types of attacks and threads [17]. It is critical to understand that by employing the latest internet protocol suites there can be multiple access points to EMS networks and physical isolation is no longer guarantee network security.

The following strategies are considered to preserve the efficiency and the reliability of the system while developing a new communication installation or transformation:

**Strategy 1:** Minimum possible changes to the existing operational system are aimed. Due to complexity and the size of the EMS, substantial changes in the software/hardware need a large amount of testing work. Always create a test environment that is as close as possible to the real time running environment. That will give some degree of confidence before making any change.

**Strategy 2:** Recently developed components with possible faulty behavior should not trespass into the legacy system disturbing the normal operation of the system as a whole. The existing system’s reliability, efficiency and functionality should be preserved.

**Strategy 3:** As there is a constant rise in the number of SSs in the power transmission network the underlying communication network need to be scalable to accommodate such growth with minor configuration effort.

**Strategy 4:** It should be a cost-effective solution.

Computer security administration is the key in handling security risks and obtains sustainable security strategies. The requirement for trained system security personnel who will have
experience in SCADA and automation systems is one main factor for successful EMS/SCADA system security administration. The SCADA security administrator should have a strong technical knowledge in modern IT security but must also be a member of the EMS/SCADA engineering team [18]. Furthermore, the security must needs of the business network are not the same as the security needs of Control Centre / Operational network. For example, the business firewall typically allows network users to browse the internet using HTTPs, while the Control Centre / Operational network requires security policies that must explicitly forbid this. A good Control Centre / Operational system security strategy needs to offer layers of protection i.e., a “defense in depth” security strategy. Firewalls cannot be all things to all divisions in the organization. The nature of attacks on modern power systems has evolved from easily observable physical damages to more subtle damages. Cyber-intrusions and cyber-attacks can go on for a long time without causing an immediate impact on the system’s functioning.

Current IPTO is categorized into two subsystems the Operational EMS/SCADA systems and the Administrative IT system as shown in Figure 7.

![Figure 7. IPTO layered SDH communication ring](image)

The two subsystems provide varied functionalities that are segmented hierarchically according to the adopted operational time. This architecture offers a useful model of distinguishing between operational and administrative systems, and enabling the design of possible secure interfaces.

6. Conclusion

In the recent years there has been a growing interest in securing SCADA systems that perform vital functions in National Critical Infrastructures. It should be mentioned that the tendency in modern EMS/SCADA system communication framework is leading away from serial communication model to IP oriented network. Unfortunately, this trend is mostly used to improve performance at the cost of increasing vulnerabilities on the EMS and SCADA interconnections. Extra care must be taken when applying existing IT security technologies to SCADA systems since these technologies may have unacceptable adverse impacts on those systems. This work highlights the need for an in depth EMS/SCADA system defense strategy. This mainly includes the communication architecture of such a critical infrastructure. This study depicts the general communication network architecture of IPTO and presents some of the frequently used SCADA communication technologies. Dedicated communication links must be utilized for remote supervision of energy facilities. The current study focuses at how network security measures benefit from system and communication technology categorization. Over the years, it has been noticed that haphazard deployments of current IT technology, informal security policies and an unpredictably adapting environment frequently result in unnecessary system risk. Not all cyber security countermeasures exploited in IT system are applicable to EMS. We emphasize the importance of de-coupling data provided for the demands of electric power operation and control sector from those of the administrative and business sectors.
References


