

# CYBER SECURITY CONSIDERATIONS IN POWER SYSTEM OPERATIONS

Peter Roche, ESB International

On behalf of JWG D2/B3/C2-01 "Security for Information Systems and Intranets in Electric Power Systems".

## Summary

This paper is the second in a series prepared through the efforts of the CIGRÉ Joint Working Group (JWG) D2/B3/C2-01 "Security for Information Systems and Intranets in Electric Power Systems." The paper describes the distinguishing features of IT systems in the power industry, with emphasis on the operations area. The concept of an IT Security domain, as a means of analysing the interactions of IT systems is presented. The main domains in the power system operations area are discussed, the range of possible users is considered and the points of weakness are identified. The paper summarises a few known cyber security incidents to illustrate how real and extensive the risks are. Finally – as an interim measure - a list of immediate actions items to establish a high level IT security policy are presented.

## 1 Introduction

Today's power industry makes extensive use of the capabilities of Information Technology. The benefits of such use have been enormous, in the efficiencies that have been achieved, in the extent of automation that has been introduced and in the depth and breadth of information that is available both inside and outside the organisation. A very high degree of dependency on the proper functioning of IT systems has developed. The converse is equally true – that the organisations are quite vulnerable to mal-operation of IT systems.

An earlier paper entitled "Managing Information Security in an Electric Utility", published in *Electra* in October 2004, provided general background on:

- why information security is important for the electric power industry,
- where the threats and vulnerabilities arise,
- how the evolution of the architecture of IT systems has made modern systems more vulnerable and
- general information on the work of various groups which have examined IT Security issues.

The main purposes of this paper are to:

- describe the forces which have influenced the development of multiple, interconnected IT networks within the power industry,
- examine the special features of operational systems which make them vulnerable to IT threats,
- describe some reported cyber security incidents and experiences from case studies,
- suggest some immediate measures that can be taken to protect the integrity of key IT systems.

## 2 Principal Distinguishing Features of Modern Power Systems

Only a generation ago the Vertically Integrated Utility (VIU) was the most usual form of organisation in the power supply industry. The adoption of a business model designed to encourage competition and to force the separation of generation, transmission, distribution and supply businesses has dramatically altered the structure of the power supply industry. In parallel with these structural changes the potential of computer systems to support change has led to the installation of a multitude of IT systems, many of which depend on inter-operability to achieve their objectives.

The current power sector is characterised by a large and expanding number of participants, each of whom has a requirement to communicate with almost any other participant in the sector. The main

participants in the sector and the principal reason for communicating with others is shown below in Table 1:

<b>Participant</b>	<b>Business Activity</b>	<b>Main Business Partner</b>
Transco or TSO or ISO	Energy Transmission	DISCO, GENCO
SCADA / EMS Vendor	Remote Support for SCADA / EMS	DISCO, TRANSCO
Market Operator	Operate energy market	All market participants
GENCO	Power Generation	DISCOs, TRANSCO, Major consumer
IPPs	Power Generation	Major consumer, DISCOs
DISCO	Energy Distribution	TRANSCO, GENCO
RTU Vendor	Remote support of RTU	DISCO, TRANSCO
Relay Vendor	Remote support of protection relays	DISCO, TRANSCO
Consumers of all types	Cost minimisation, value	DISCO, TRANSCO, Market operator

Table 1: Main Participants in Power Industry

Tremendous productivity improvements have been achieved in most sectors, very often based on extensive deployment of computers. Computers underpin all aspects of the industry, from customer accounting and billing systems, to GIS and trouble call logging systems. Especially significant are the large number of operational systems which depend on computers – e.g. SCADA, automatic metering systems, digital substation control systems, digital relaying systems etc. In many respects it could be said that the technological fabric of today's power industry is supported by information technology.

The different participants in the power industry each develop their own IT systems, often with different hardware and software, with various network architectures and with different network management tools, systems and philosophies. Each participant has the expectation that he can communicate with other participants, normally using industry standard methods. In some situations communication may take place through industry specific protocols (e.g. UCA / ICCC), but more usually the internet, often with private subnets, is the vehicle of choice for communications.

Managers of IT systems have limited control of the IT security aspects of communications across the internet, using techniques and equipment such as encryption, access control, firewalls, etc. However an IT manager can never assume that those other organisations with whom his organisation communicates have taken adequate precautions to remove any risk of IT security threats or attacks.

### 3 Main Information System Domains in Power System

#### 3.1 Concept of Information System Domain

A traditional way of describing and analysing a computer network is from a hardware perspective, i.e. in terms of servers, bridges, routers, etc. But since the various systems, such as the power system control and the administrative systems, are getting more and more interconnected/integrated, another approach is needed to address and support analysis of the integrated system as a whole.

The safe, secure, responsive and confidential nature of the communications between networks and participants is at the core of the issue of IT Security.

The concept of Information System Domain is a powerful tool in the description and analysis of the interactions between the participants.

### 3.2 Interaction between Domains

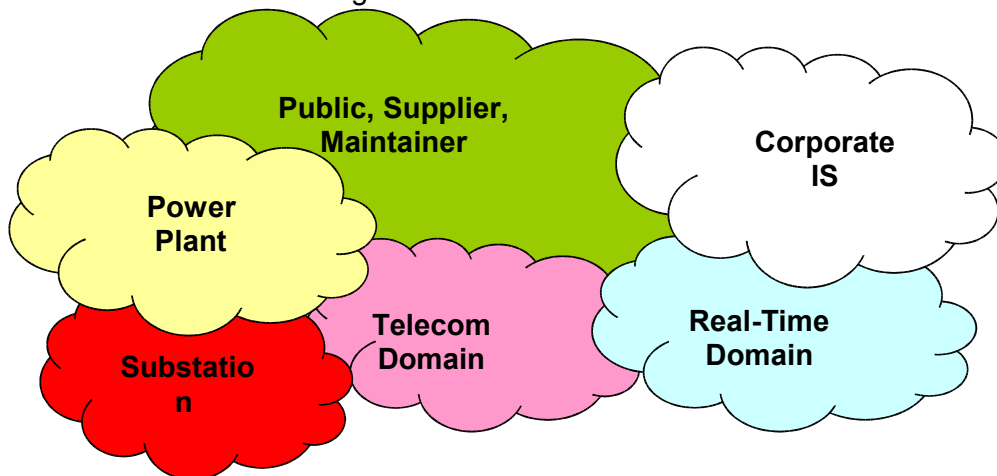
In an unbundled and competitive market a large number of domains exist - often as many as the number of participants shown in Table 1. In addition each main domain will have a number of sub-domains. A sub-domain is a specific area, wherein particular activities/business operations are being undertaken and where a common set of IT applications are executed. There are some points of note:

- A sub-domain may be quite small in extent e.g. an IT system which monitors and records information on substation assets may be confined to a small number of locations,
- Some sub-domains may be geographically very extensive e.g. a SCADA system which extends through the entire territory of the business,
- A business unit such as a TSO may have many sub-domains – SCADA system, metering and billing system, asset monitoring system, digital substation control systems, business planning system, finance and accounting system, etc.
- There is no certainty that an explicit set of security policies is in force either across the entire domain or even in every sub-domain. Some businesses are more aware of the need for security policies than others.

It is frequently the case that different sections of a business develop IT systems in isolation and at different points in time. Certainly they will usually be interconnected, but their origins will be evident from the different hardware and software, various network architectures and from the different network management tools, systems and philosophies that are employed. Crucially different IT security practices may exist in each domain.

Where the extent of unbundling is limited, or where limited competition exists then the number of sub-domains may reduce – in this case a single business entity may, in effect, own a number of the domains outlined above.

Returning to the central theme of security of information systems in the power system operations field, it is evident that an incident or event that takes place in one domain could, if not properly managed and contained, spill-over to impact the domains to which it is connected. Such a spill-over is most likely in situations where different cyber security practices apply in different domain – as will inevitably be the case. Obviously as the number of interacting domains increases the source of threats and risks to the integrity of the IT networks of other participants increases – as is implied from the multiple boundaries shown in the schematic diagram below.



Overlapping IT Domains

Figure 1 Concept of

### 3.3 Multiple Users within Power System Operations Domains

One of the most significant differences between the challenges facing the management of real-time schemes, in contrast with non-real-time schemes, is that there may be very many groups of users who interact with real-time IT systems. For instance operators, system maintenance personnel, vendor

support personnel or others may all have genuine reasons to access the same sub-domain. In Figure 2, at the end of the paper, a more detailed list of the owners of the domains, the primary users, the secondary users of the IT systems within the domains and the reasons why there are multiple users is summarised.

Most users of the IT systems will be employees of the owner of the sub-domain; however many users may report to other sections in the owning entity and other may belong to external organisations. This diversity of responsibility and reporting lines presents serious challenges for the secure management of the real-time IT systems.

#### **4 Points of Access / Weakness in Real-Time Systems**

Figure 3 shows a schematic representation of the IT systems which are used in real-time operations. The diagram represents the manner in which many real-time systems interact and exhibit vulnerabilities. The diagram depicts the following:

- how a central SCADA system collects data from RTUs in substations, indicating the connection points where a support engineer may gain access to the central system or to an RTU.
- how support may be provided for digital Substation Control Systems, where local access, or even remote access, may be obtained to enable local reconfiguration of devices or even remote support from a vendor's office.
- the points where a telecommunications engineer may access a node for maintenance or support purposes.

A brief examination of the diagram reveals that there are multiple points of access to the various IT systems. The systems are continuously transferring data and interacting with each other. There is a definite risk that an event in one system, say the activation of a virus within the Operating System of a digital Substation Control System, could cause it to transmit spurious data into the shared telecommunications network, with the risk of effecting other IT systems. Note also that all points of connection of PCs, or equipments with embedded PCs, or even printers are potential access points to the integrity of the network.

The telecommunications system usually used by a SCADA system may share a physical infrastructure with other business users, e.g. fibre optic or microwave radio links shared with general IT applications. Traditionally, however, the SCADA system utilises non-shared and independent bandwidth e.g. its own fibres or channels. This separation may eliminate many spill-over effects from disturbances originating from other users / applications on the shared medium. Nonetheless within the SCADA system itself, the presence of many fixed PCs, of other maintenance terminals / lap-tops temporarily connected for maintenance purposes and possible direct connection to substation SCS systems, provides many points of weaknesses, through which IT security threats can enter the SCADA system.

##### **4.1 Frequent Alterations in Network Configuration**

A unique feature, almost unknown in the non-real time situation, is that the basic hardware configuration of real-time IT systems is subject to frequent change. Not alone may the number of RTUs in a SCADA system grow; the number of Bay Control Units connected to digital Substation Control Systems is always increasing; the number of asset monitoring devices in substations increases and so on. The newly connected devices may be similar to those already on the network, often they may have been produced by a different manufacturer and only match existing systems in that they use a standard protocol. Thus the configuration of sub-domains frequently changes, without any guarantee that the new device entirely complies with existing IT security policy – where an explicit policy is actually in place.

However the most threatening practice in real-time IT systems is the connection of maintenance terminals – often lap-tops – to nodes in the network, i.e. where a maintenance technician connects his lap-top / maintenance terminal to an RTU, protection relay, digital Control System etc. for a variety of

purposes. This same lap-top represents one of the greatest source of risk to the integrity of IT security, as there is rarely a means of checking that the lap-top has not been infected with a virus, worm, Trojan horse etc.

#### **4.2 Alterations / Modifications to Basic Device Parameters**

Another unique feature, almost unknown in the non-real time situation, is that users may frequently access points in a sub-domain to make fundamental alterations to the parameters of embedded devices. For example a protection engineer may access a relay to reconfigure it, or to modify its characteristics. Or a support engineer may access a digital Substation Control System to reconfigure the software or hardware to add a new bay or signals to the existing system. In all cases the resultant alteration in the device software may introduce unexpected and unwanted effects.

### **5 Some Reported Cyber Security Incidents**

A significant number of cyber security incidents have taken place; only some have been described or admitted to. To show how multi-faceted the problem is, a sample of incidents is given below.

#### **Large Generating Plant Output Reduced to Zero**

The control system of a large generating plant operating at a number of 100 MW was infected by a virus and its output was reduced to virtually zero in a few seconds. Infection came from connected corporate IT network. The solution was to rigorously separate the real-time and corporate networks.

#### **Distribution SCADA System Partly Disabled**

A virus infected lap-top was used by a maintenance technician to modify a telecoms router. The virus effected all telecom nodes, including some used by a SCADA system. The SCADA system was made partly inoperable for a number of days. A part solution required better management of virus protection on lap-tops.

#### **Unauthorised Access to EMS Applications**

A utility gave remote access rights to an EMS supplier. It was observed that application patches had been applied without agreement. No problems arose, but the situation revealed that continuous, non verified access had remained open to an external internet port, with serious risk potential.

### **6 Suggested Actions to be Taken While Comprehensive Measures are Developed**

In a later Electra paper the Joint Working Group intend to propose a comprehensive policy as to how to establish and maintain a high level of cyber security protection. As an interim measure some key actions to be taken are suggested below.

1. **Define the Responsibilities and Authorities of those Charged with Cyber Security**  
Establish a cyber security organisational structure that defines roles and responsibilities and clearly identifies how cyber security issues are escalated and who is notified in an emergency. Those who design, operate, maintain real-time systems should be fully aware of the range of cyber security risks and their specific responsibilities to minimise the incidence and effects of cyber events.
2. **Document the Network Architecture and Identify All Real-Time Systems**  
Ensure that critical real-time systems are properly documented and that their telecommunications and IT links are accurately recorded. Ensure that documentation is kept up-to-date. During system design and extension, the designer must be fully aware of the risks and threats posed by Cyber security events. Maintain copies of all software off-site and record all changes to software and hardware.
3. **Perform Security Audits of all Real-time Networks and interconnected Systems**

Technical audits of all real-time systems and networks are critical to ongoing security integrity. Establish the organisational importance of each system. Analyse the vulnerability of each system and place a risk assessment on the issue. Identify the software versions and extent of patches applied so as to be aware of the levels of protection / vulnerabilities that exist. Establish an action-plan to address the more significant weaknesses.

4. Identify all connections to Real-time Systems

Identify and assess the risks posed by intra-company and external types of connections, including LANs, Intranets, Internet, leased or dial-up links, dedicated links, radio access systems etc.

5. Disconnect unnecessary Connections and Applications from Real-Time Systems

To ensure the highest degree of security of real-time system, isolate the real-time sub-domains from any other network connections as far as possible.

Disable or remove unnecessary applications or services, so only essential processing takes place on the system. Internet connections or infrequently run applications should be deleted.

6. Strengthen the Access Controls for any Remaining Connections

Where essential connections to external sub-domains are required, implement access control systems at every point of connection, e.g. with firewalls, intrusion detection systems, password protected and dial-back type modems and other appropriate security measures. Where infrequent connections are required, consider installation of access devices which can be temporarily enabled.

7. Install Appropriate Security Facilities provided by Manufacturers.

Analyse each real-time system to determine whether security features are present. offered by the manufacturers should be assessed. Install all appropriate security features and settings, with high threshold levels of security.

Note that reliance on proprietary protocols will not necessarily protect systems, unless suitable security measures are incorporated into the devices.

8. Establish Strict Control over non-Routine Access Mechanisms

Identify clearly those providers of services who must be given access to real-time systems. Where, for instance, external vendor connections must be provided for support purposes, strong authentication must be implemented to ensure secure communications. Wireless access is least desirable as its presence may be very hard to detect. Access should only be permitted through a temporarily enabled access route, which should be automatically disconnected after a set period of time.

9. Maintain a Comprehensive, Continuous Risk Management Process.

Due to rapidly changing technology and the emergence of new threats on a daily basis, a continuing and comprehensive risk assessment process is needed so that routine changes can be made to the protection strategy to ensure it remains effective. Fundamental to risk management is the identification of residual risk with a system protection strategy in place and acceptance of that risk by management.

10. Implement Intrusion Detection Systems

To be able to effectively respond to cyber attacks, it is necessary to be aware of cyber events on the real-time systems. Where possible an intrusion detection system should be installed. Regular monitoring and active follow-up is an essential feature of an effective cyber security protection scheme.

11. Assess the Integrity of Physical Security to Real-time Systems.

At every location where a node to a real-time system is installed (e.g. substations, telecommunications masts / towers, pole-top units etc.) conduct a physical security survey and list access points that could provide entry to a real-time sub-domains.

**12. Establish a Clear Organisational Cyber Security Philosophy**

Organisations and companies need structured security programs with documented requirements to establish standards and to enable personnel to be held accountable. A formal cyber security policy is essential for establishing a consistent, standards based approach to cyber security. Policies and procedures also inform employees of their specific cyber security responsibilities and the consequences of failing to meet those responsibilities.

The need for staff to comply with confidentiality practices and to avoid disclosure of sensitive information is a key requirement.

**13. Establish a System Backup Procedure and Disaster Recovery Plans.**

Establish a disaster recovery plan that allows for rapid recovery from any emergency (including a cyber attack). System backups are an essential part of any plan and allow rapid reconstruction of the network. Routinely exercise disaster recovery plans to ensure that they work and that personnel are familiar with them. Make appropriate changes to disaster recovery plans based on lessons learned from the exercises.

**7 Conclusions**

Modern power system operations are heavily dependent on IT systems, many of which operate in real-time. The introduction of competition and unbundling has brought many new organisations into the power sector. Much of the interaction between the participants in the power sector is carried out through IT systems. There are a wide variety of mechanisms through which cyber threats - viruses, worms, etc.- to the integrity of IT systems can propagate. It is important that every organisational entity in the power sector becomes aware of the cyber security threats. The paper presented a brief overview of the threats posed to real-time systems. A number of immediate steps that can be taken to ameliorate the risks have been outlined. The JWG will discuss further aspects of IT security in further papers in this series.

**Glossary**

DISCO	Distribution Company	EMS	Energy Management System
GENCO	Generation Company	GIS	Geographical Information System
ICCP	Inter Control Centre Protocol	IPP	Independent Power Producer
ISO	Independent System Operator	IT	Information Technology
NMS	Network Management System	PEX	Power exchange
RTU	Remote Terminal Unit	SCADA	Supervisory Control & Data Acquisition
TELCO	Public Telecom Company	TRANSCO	Transmission Company
TSO	Transmission System Operator	UCA	Utility Control Architecture
UTELCO	Utility owned TELCO		



<b>Domain Owner</b>	<b>Primary User Group</b>	<b>Secondary User Group</b>	<b>Purpose of Access</b>
Transmission system company – Transco	Operations & Maintenance staff	<ul style="list-style-type: none"> <li>• Hardware asset vendors and their support staff</li> <li>• ISO</li> <li>• Utelco</li> <li>• Telco</li> </ul>	<ul style="list-style-type: none"> <li>• Protection equipment support and settings, etc.</li> <li>• Disturbance data retrieval</li> <li>• Vendor Support for Digital Control Schemes</li> <li>• SCADA via RTUs,</li> <li>• On call engineers with remote access rights</li> <li>• Public web access to open data</li> <li>• Provision of voice &amp; data links</li> </ul>
Distribution company – Disco	Operations & Maintenance staff	<ul style="list-style-type: none"> <li>• Hardware asset vendors and their support staff</li> <li>• ISO</li> <li>• Utelco</li> <li>• Telco</li> </ul>	<ul style="list-style-type: none"> <li>• Protection equipment support &amp; settings, etc.</li> <li>• Disturbance data retrieval</li> <li>• Vendor Support for Digital Control Schemes</li> <li>• SCADA via RTUs,</li> <li>• On call engineers with remote access rights</li> <li>• Public web access to open data</li> <li>• Provision of voice &amp; data links</li> </ul>
Independent System Operator – ISO or ISA	System Dispatch staff	<ul style="list-style-type: none"> <li>• Asset Vendors and their support staff</li> <li>• Market participants</li> <li>• Telco</li> </ul>	<ul style="list-style-type: none"> <li>• SCADA system vendor support</li> <li>• On call engineers with remote access rights</li> <li>• Market system operators</li> <li>• Transco and Disco operators</li> <li>• Public web access to open data</li> </ul>
Market Operator	Market Operations staff	<ul style="list-style-type: none"> <li>• Asset Vendors and their support staff</li> <li>• Market participants</li> </ul>	<ul style="list-style-type: none"> <li>• Vendor system support</li> <li>• ISO interactions</li> <li>• Transco and Disco operators</li> <li>• On call engineers with remote access rights</li> <li>• Public web access to open data</li> </ul>
Utility Telecommunications Company – Utelco	Network Management staff	<ul style="list-style-type: none"> <li>• Asset Vendors and their support staff</li> <li>• Various clients using services</li> <li>• Telco</li> </ul>	<ul style="list-style-type: none"> <li>• NMS support,</li> <li>• In house staff supporting remote device configuration</li> <li>• On call engineers with remote access rights</li> <li>• Support from asset Vendors</li> </ul>
Independent Power Producers – IPPs	Operations & Maintenance staff	<ul style="list-style-type: none"> <li>• Asset Vendors and their support staff</li> <li>• Market operator</li> <li>• Transco operator</li> <li>• Telco</li> </ul>	<ul style="list-style-type: none"> <li>• Protection equipment support &amp; settings, etc.</li> <li>• Vendor Support for Digital Control Schemes</li> <li>• ISO interactions</li> <li>• Public web access to open data</li> <li>• SCADA via RTUs</li> <li>• Provision of voice &amp; data links</li> </ul>

Power Exchange - PEX		<ul style="list-style-type: none"> <li>• Asset Vendors and their support staff</li> <li>• Market participants</li> <li>• Utelco</li> <li>• Telco</li> </ul>	<ul style="list-style-type: none"> <li>• Asset Vendors</li> <li>• ISO operator</li> <li>• Interactions with Market Operator</li> </ul>
Public Telecommunications Company – Telco		<ul style="list-style-type: none"> <li>• Asset Vendors</li> <li>• Multiple other users both within and outside power sector</li> </ul>	<ul style="list-style-type: none"> <li>• In house NMS support</li> <li>• Support from asset Vendors</li> <li>• On call engineers with remote access rights</li> </ul>

**Figure 3 Owners and Users of IT Domains**

# Access points to SCADA System

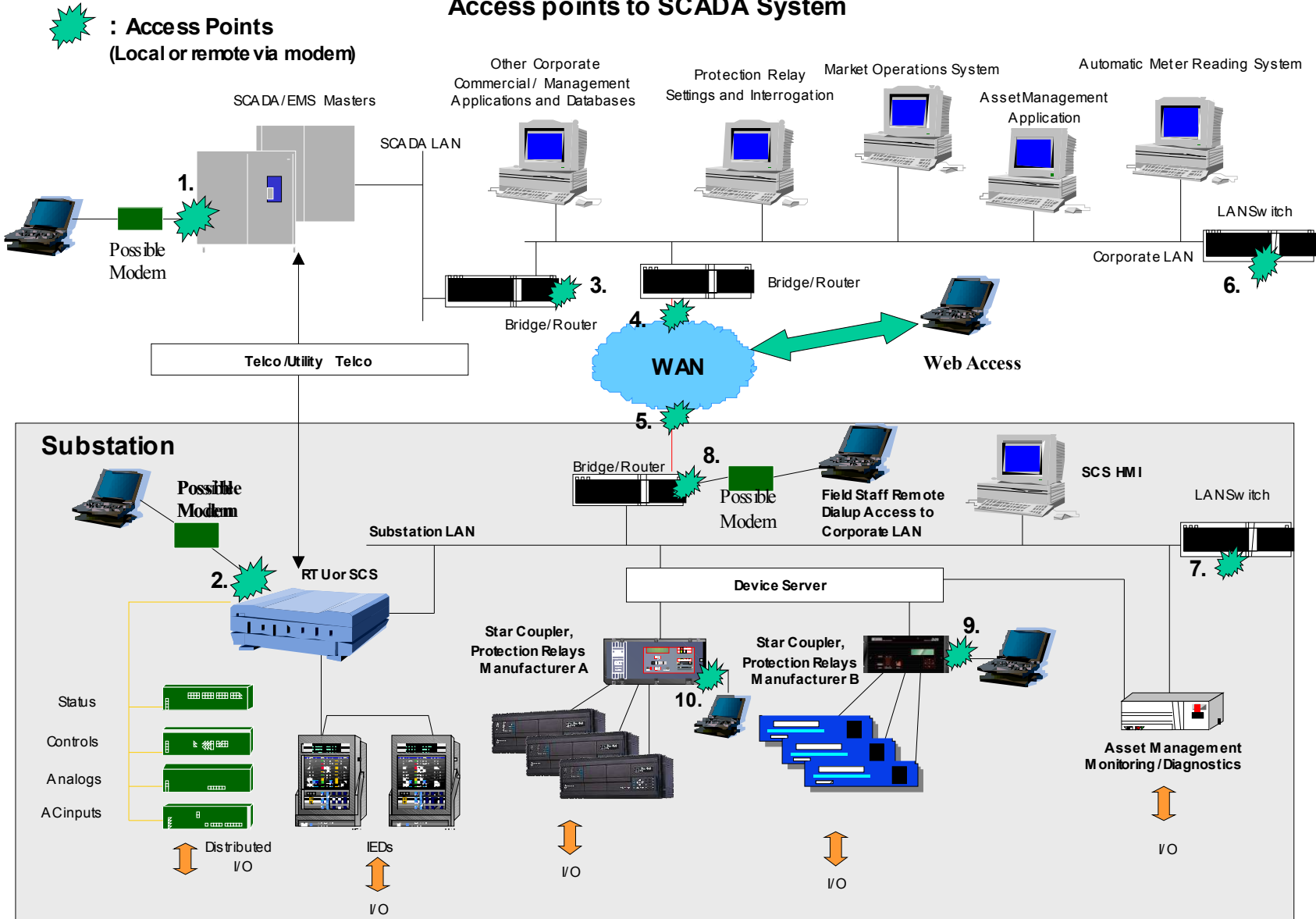


Figure 4: Schematic Diagram of Main Real-time Sub-Domains