



Cyber Security for SCADA Systems

**Vulnerability Assessment and Cyber security of ICS/SCADA systems  
for the Energy & Transportation Infrastructure**

*Majid.Ghadimi*  
December 2021  
Tehran/Sharif UN.

# Main Topics

**1**  
Quick Review  
on SCADA

**2**  
Cyber Security  
For SCADA

**3**  
RTU  
Configuration,  
Security and  
Vulnerabilities



3 Steps



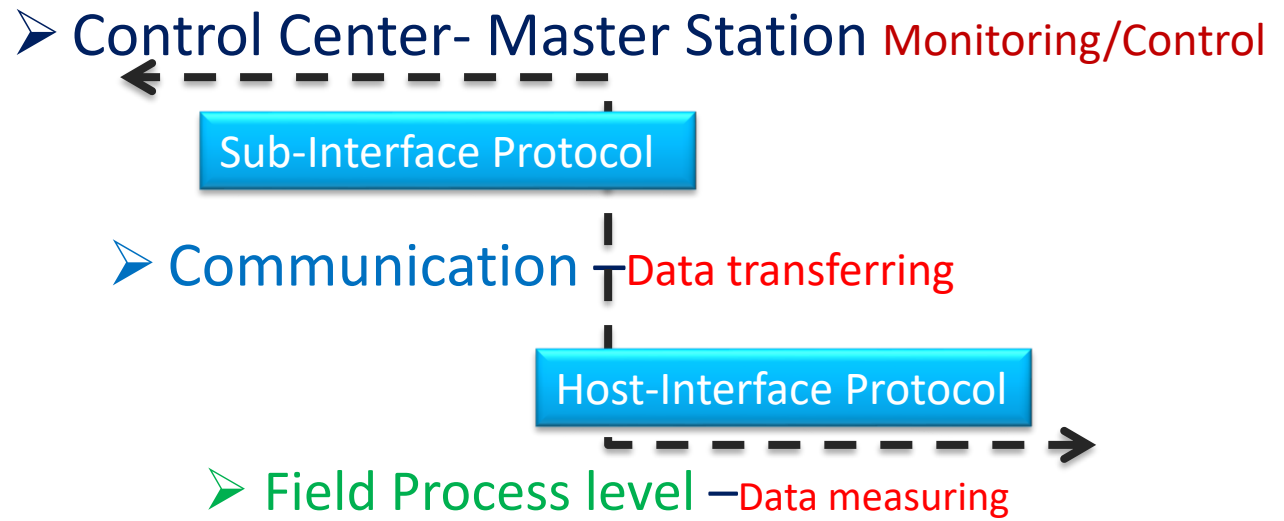


SCADA IS AN ACRONYM FOR  
***SUPERVISORY CONTROL AND DATA ACQUISITION.***

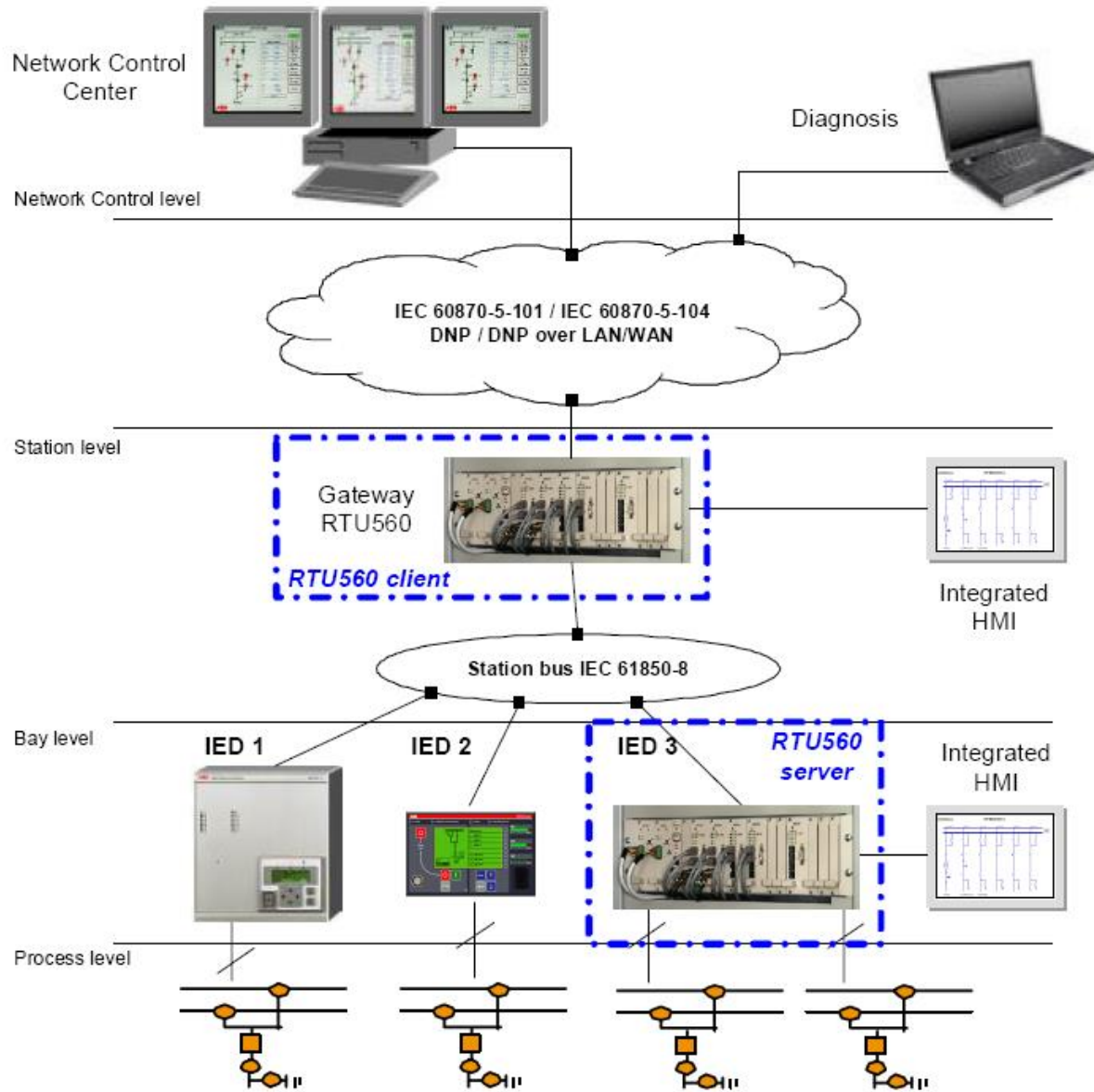
- A Kind of Industrial control system (ICS).
- Computer controlled to on line Monitor and Control industrial processes.
- Large scale processes including multiple stations, spread over large geographical areas
- Critical infrastructure, facility-based processes such as  
*Electrical Energy, oil and gas refining And **Rail-Way Transportation***

**SCADA Center, Communication Media, RTU and PROTOCOL**

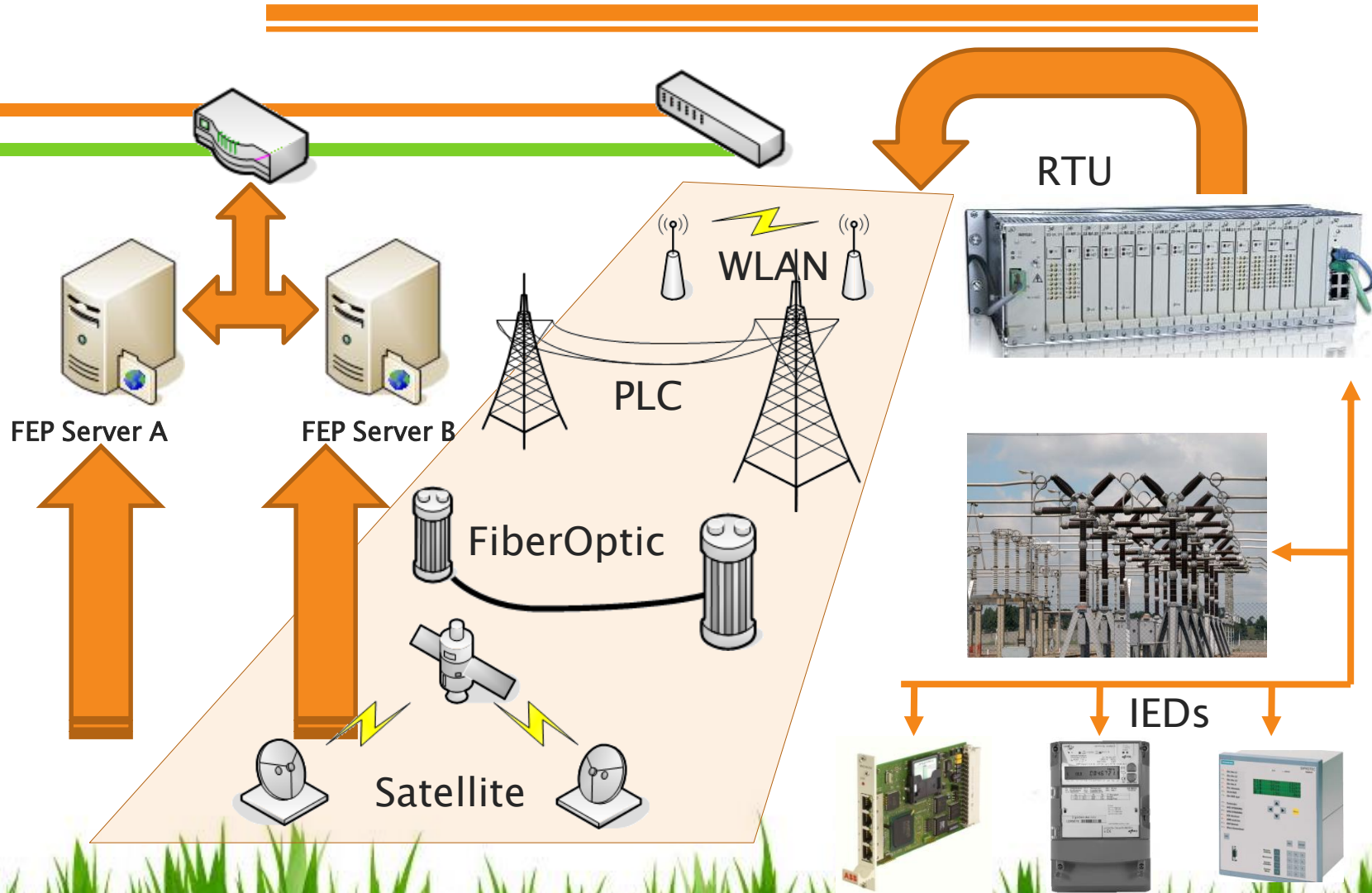
## HIERARCHICAL SYSTEM ARCHITECTURE:



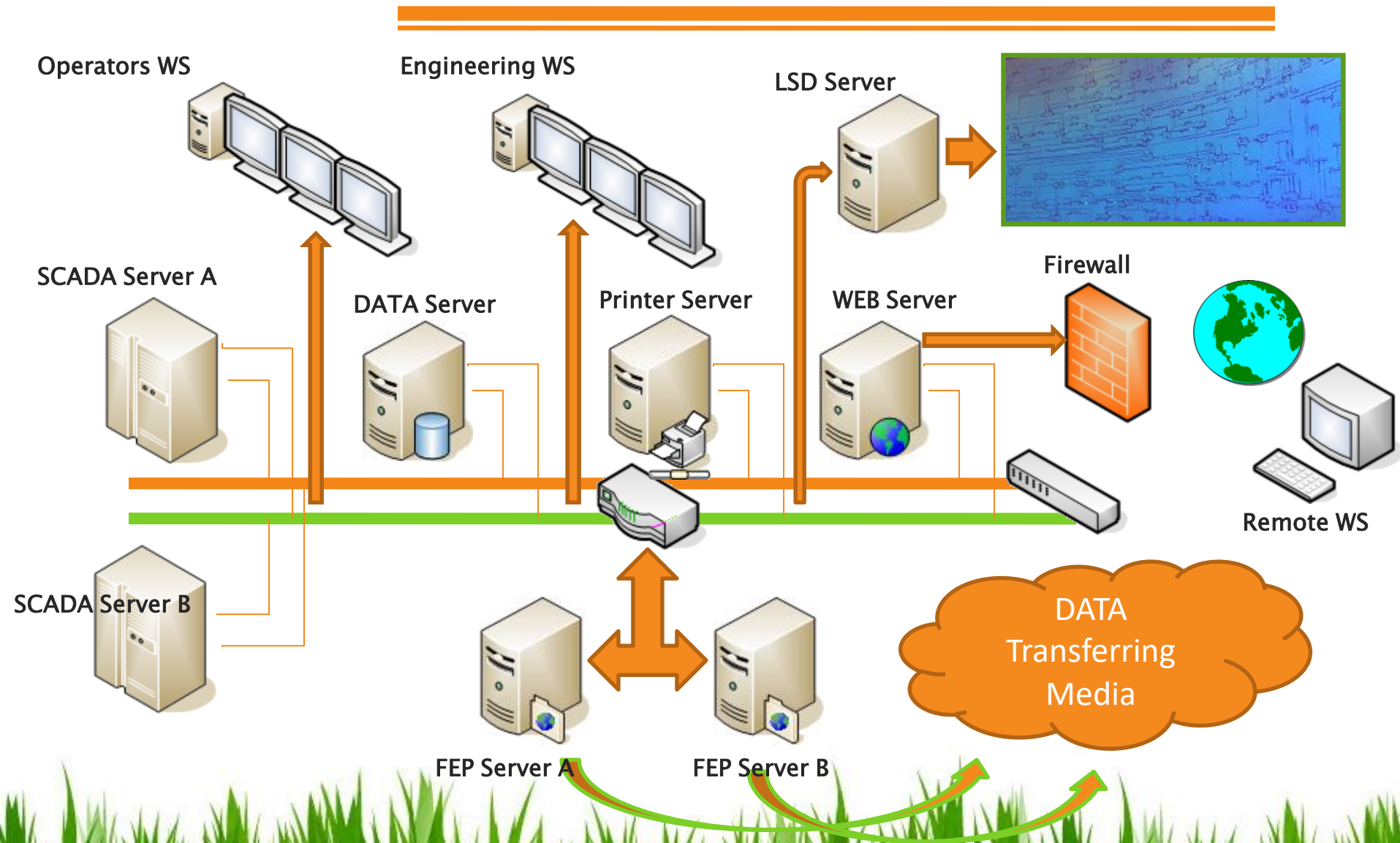
SCADA Center, Communication Media, RTU and PROTOCOL



# Overall SCADA Structure



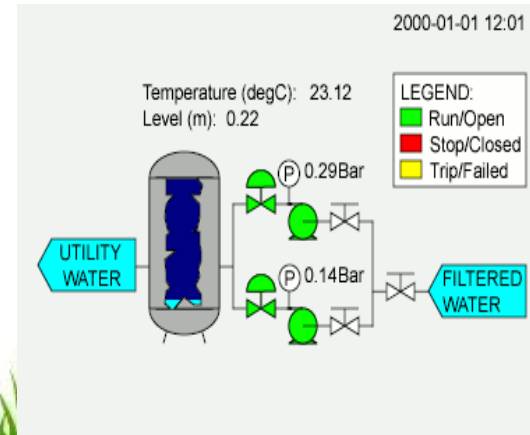
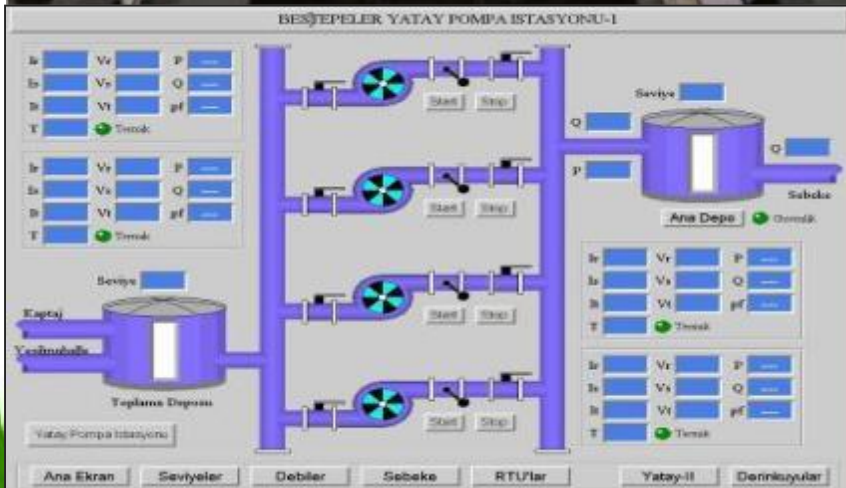
# Overall SCADA Structure



# SCADA Center



- **Front End Processor Servers (FEP)**
- **Master Database server**
- **Engineering work station**
- **Operator Work Station**
- **Human Machine Interface (HMI)**
- **SCADA SERVERS**
- **Specialized Application SERVERS**
- **Local Area Network ( Control LAN)**
- **WEB Server**
- **Printers, Video wall,...**





# Communications Network

A communications system used to transfer data between field data interface devices and control units and the computers in the SCADA central host.

The system can be:

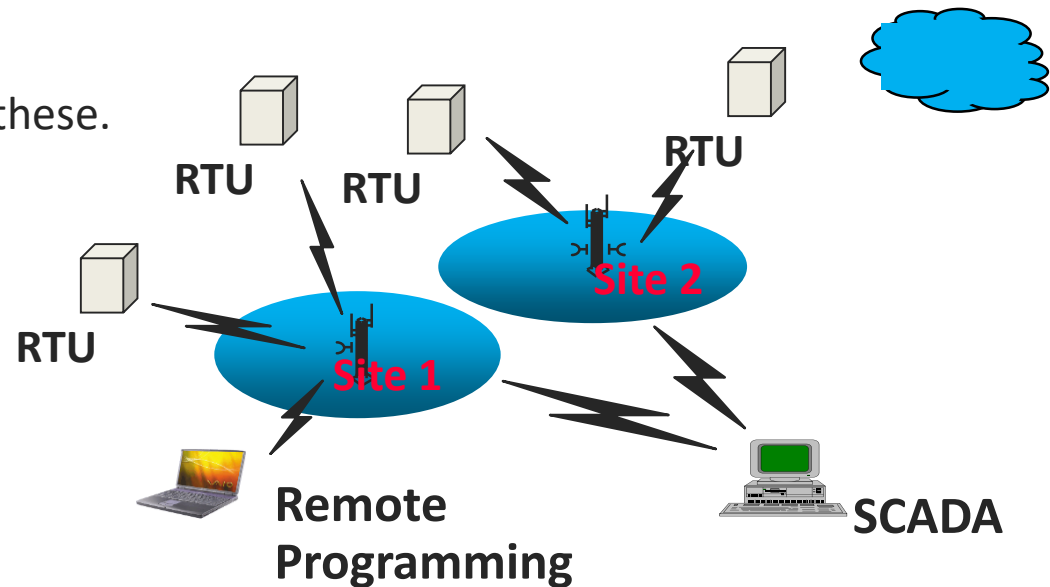
telephone, leased line

cable

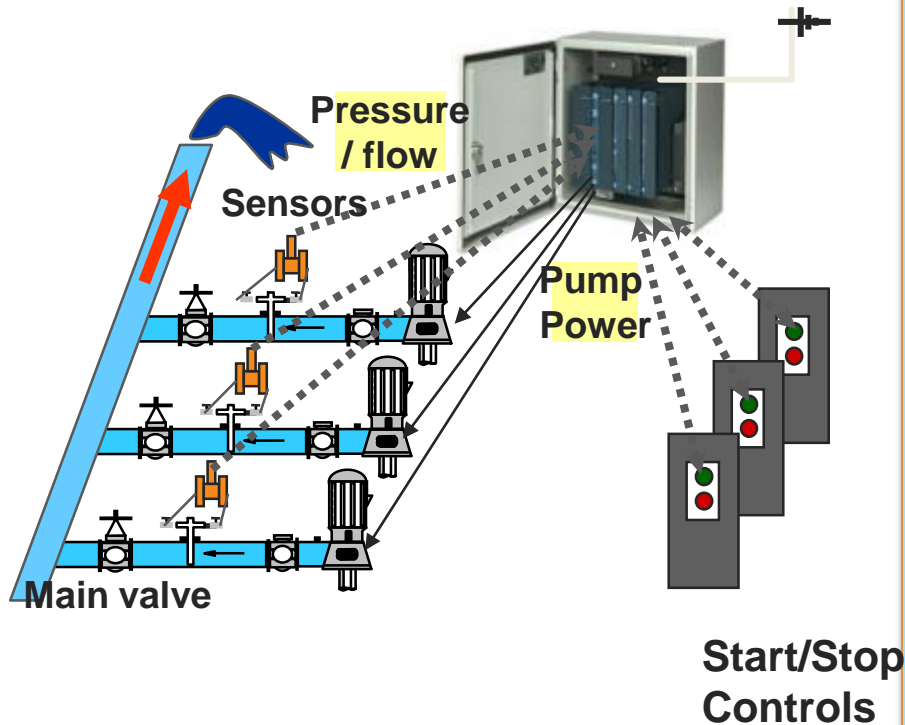
satellite, microwave radio

fiber optic transmission

etc., or any combination of these.



# RTU “ Remote Terminal Units”



## Monitoring Direction ←

- I. RTUs connect to sensors
- II. Converting signals to digital data
- III. Sending data to the CS.

## Control Direction →

- I. Receiving Commands From CS.
- II. Converting Digital COM to Signal
- III. Energizing Relays- Operating Actuators

- Power-Supply-PS
- I/O Cards-
- Communication Boards

# SCADA Protocol

- ✍ A protocol is a set of rules that governs how message containing data and control information are assembled at a source for their transmission across the network and then disassembled when they reach their destination.
- ✍ The protocol allows communication from one device to be understood by other devices.
- ✍ The Open Systems Interconnect (OSI) reference model is a layered set of protocols to facilitate open communications between computer networks. It was developed by the International Standardization Organization (ISO)

**IEC 60870-5-101**

**IEC 60850-5-103**

**DNP3**

**MODBUS**

**TCP/IP and SLIP**

.....

# SCADA Protocol

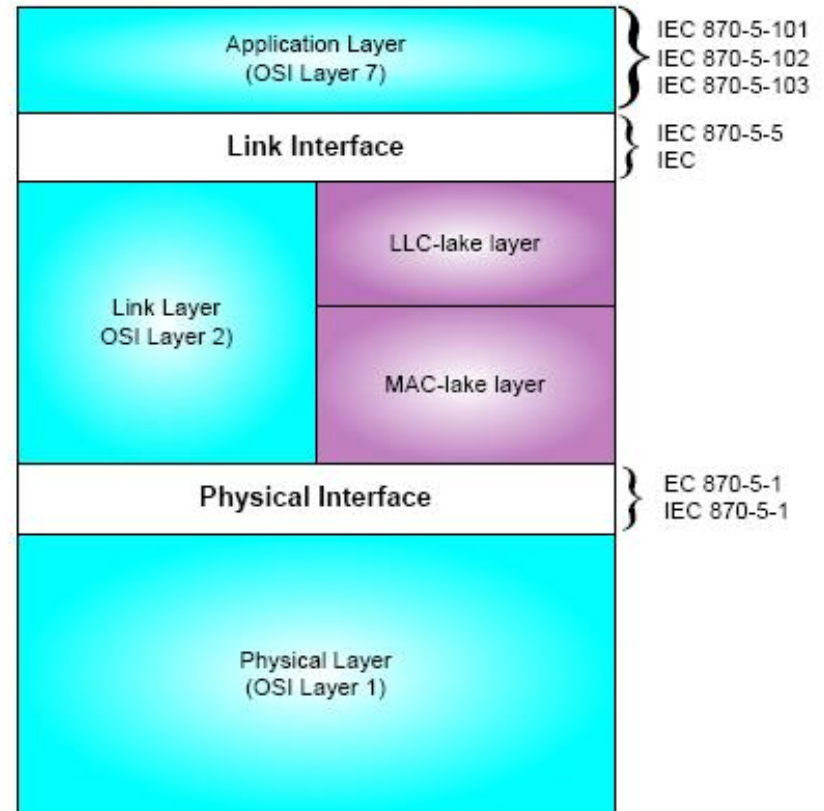
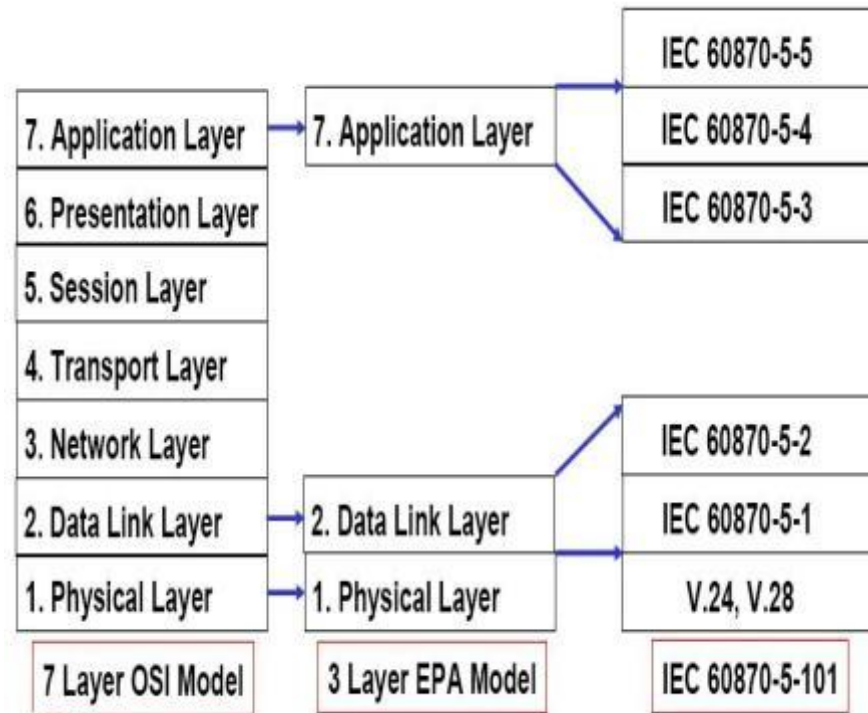
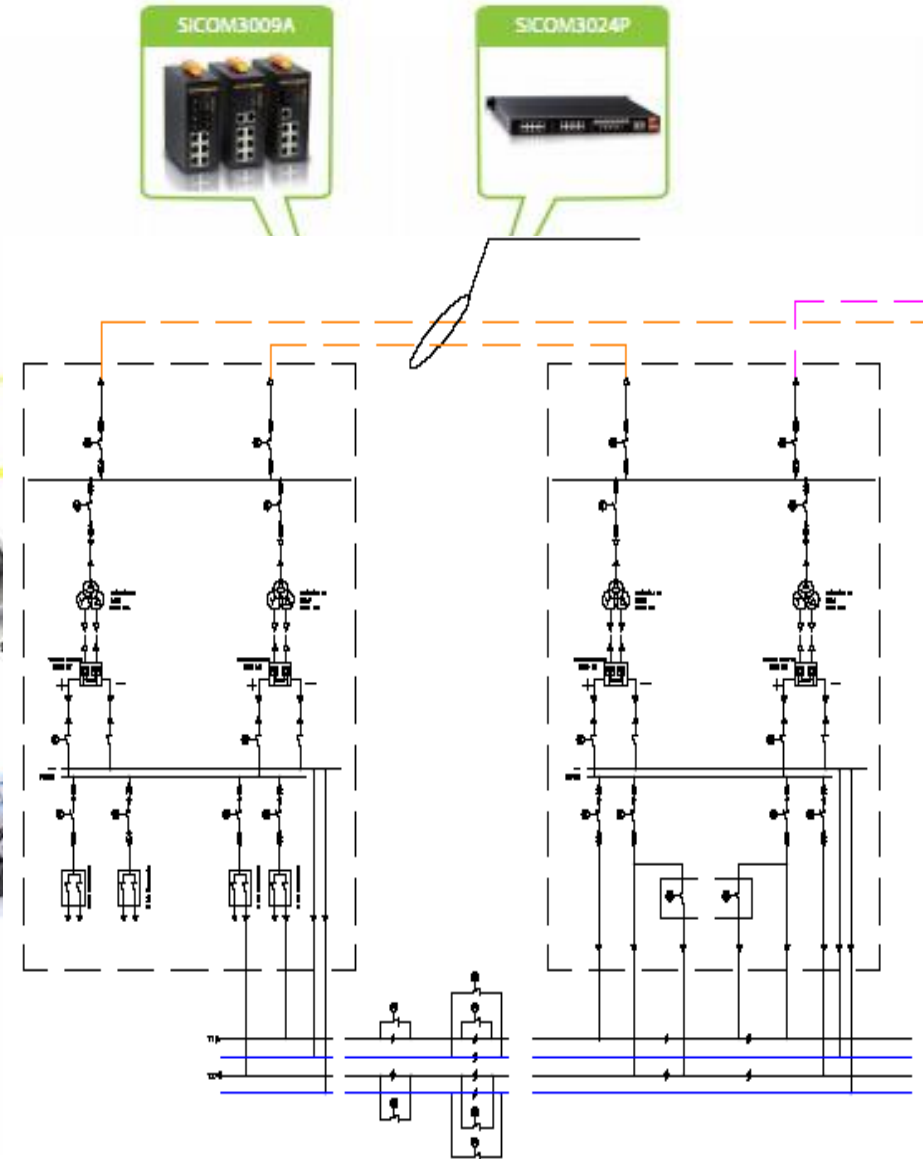
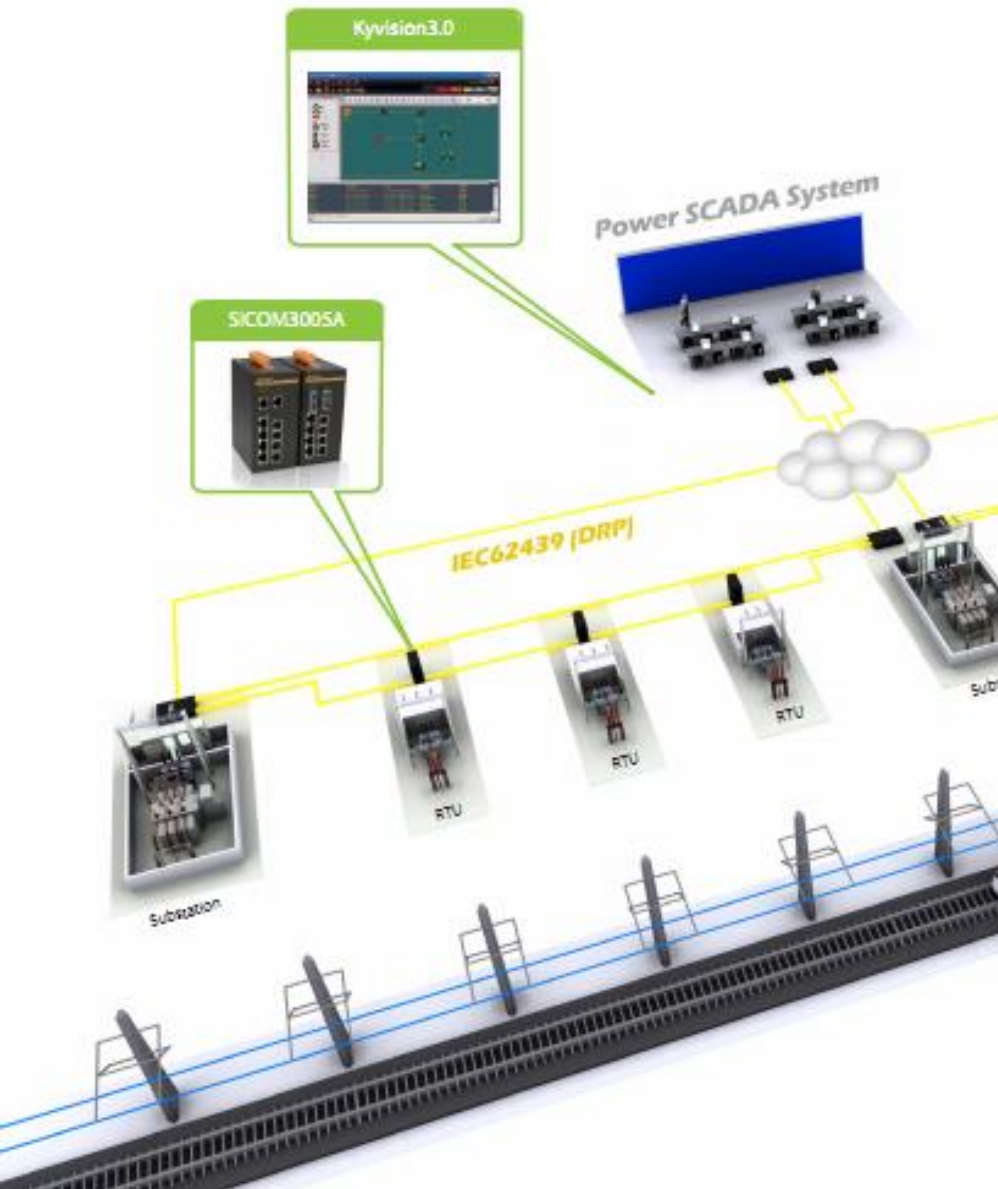


Figure 4.1: Enhanced Performance Architecture

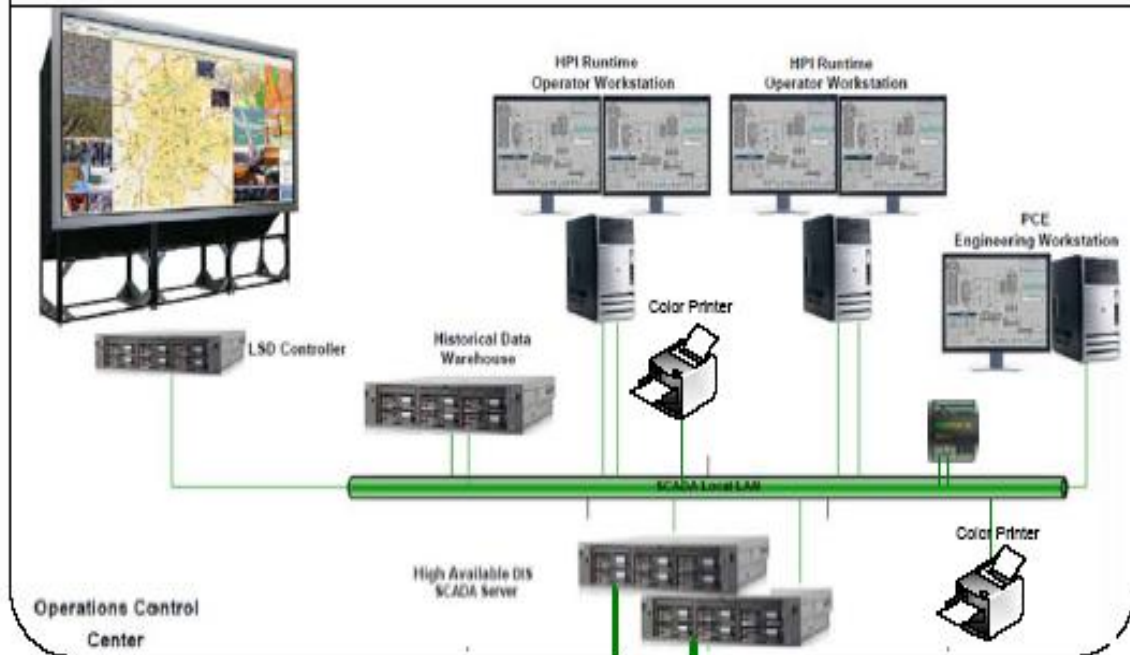
# Power SCADA Networking for Railway Traction System

- ❖ *Traction power supply systems : basic infrastructure for train operation.*
- ❖ *Transformers, switch-gears, low-voltage power distribution and control/protection devices are installed along the tracks,*
- ❖ *Power SCADA system ensures the service availability through its real time control and supervision.*

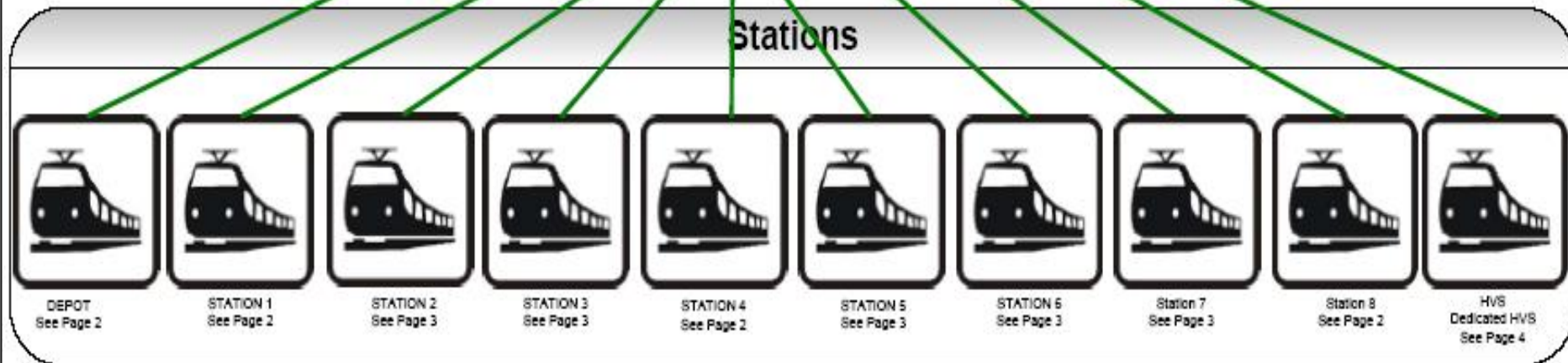




# OCC



Legend	
Industrial Ethernet	—————
Hard Wire	—————
Modbus	—————



# SCADA Center

- ➔ *Engineering work station*
- ➔ *Operator Work Station*
- ➔ *Human Machine Interface (HMI)*

Cutting-edge technology in STM's control center in Montreal (Canada)

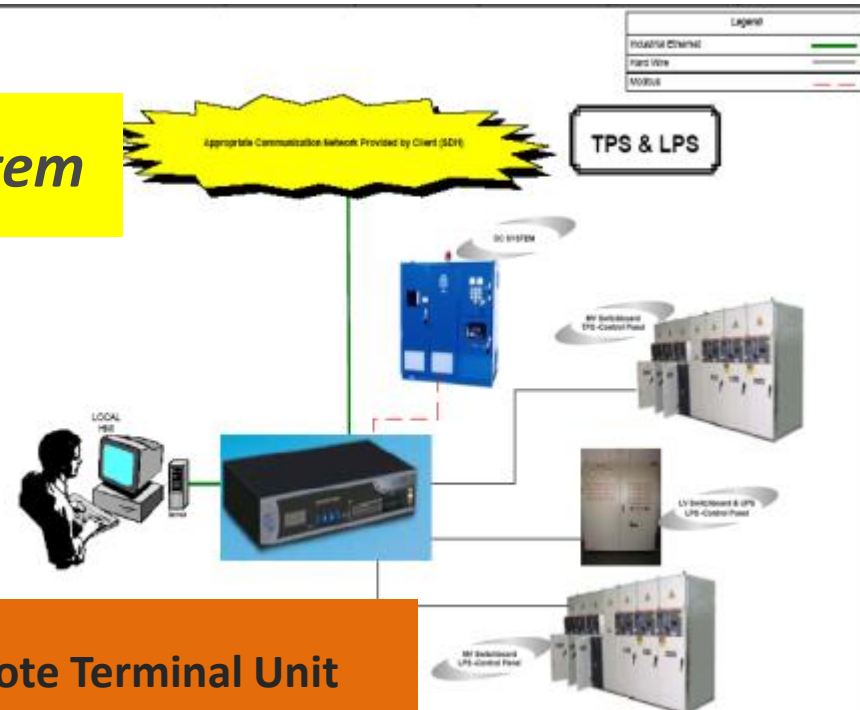
*communications system*

## Stations

*TPS :track Power Supply*

*LPS: Lighting & auxiliary Power Supply*

Remote Terminal Unit







# Cyber Security For SCADA

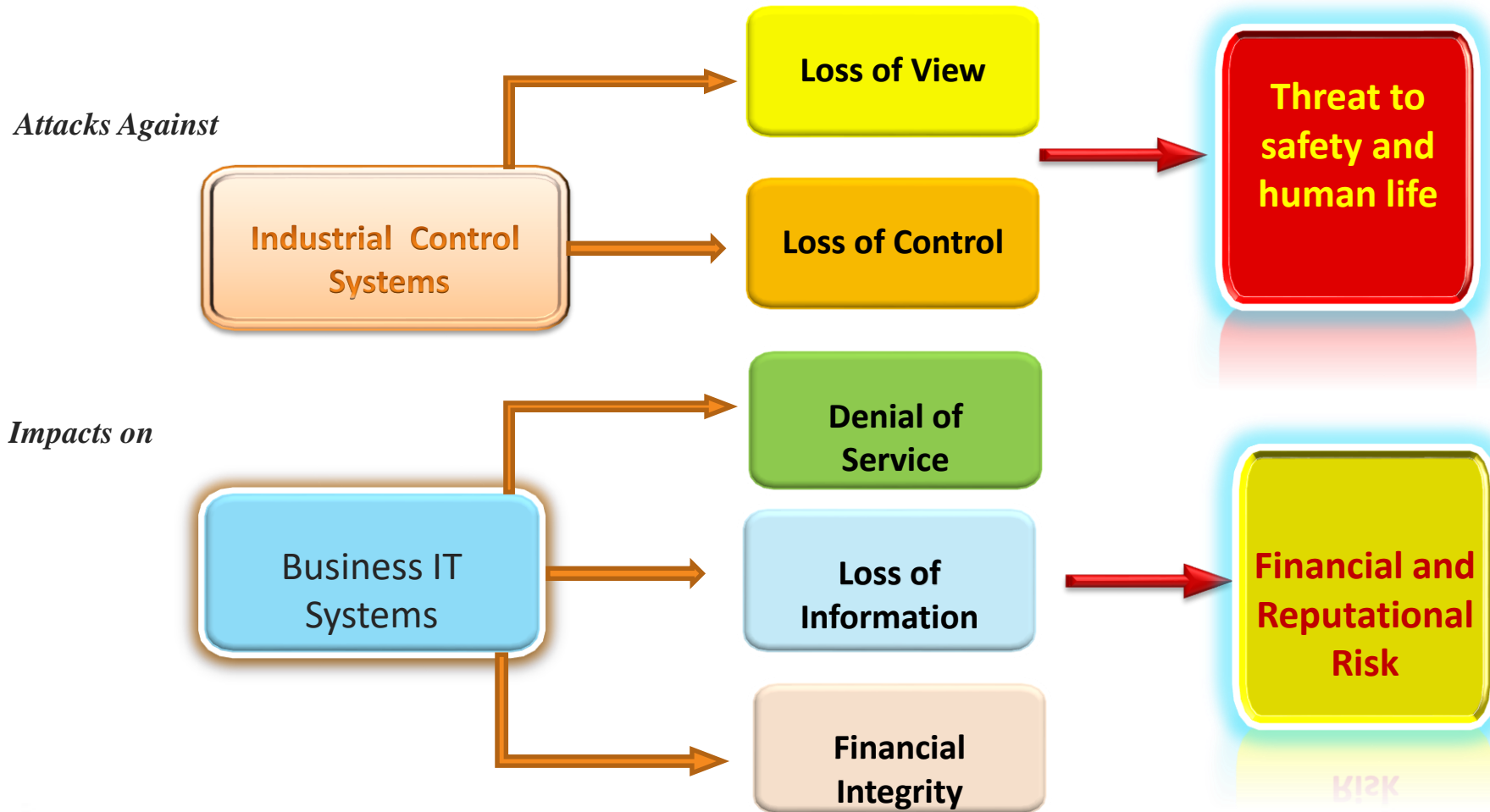
Introduction, Cyber Vulnerabilities, SCADA Security Strategy

# Introduction *SCADA Cyber Security*

- **Modern SCADA** systems- complex, distributed and connected to network.
- Based on **open standards and Protocols**.
- Evolution Towards using **(TCP/IP)**- Ethernet communications,
- Increased risk of **Cyber Intrusion**
- Yet, **A generation older CS** running some Critical industrial processes.
- **Before**, Cyber security not a **main Concern**
- Even **New Control systems** connected to the internet with **inadequate protection**
- SCADA Systems are **Vulnerable to cyber attack**



# SCADA systems and the Enterprise Network



## Typical Threat sources listed by CPNI Centre for Protection of National Infrastructure

- **Contractors**
- **Corporate intelligence**
- **Criminals / Organized Crime**
- **Disgruntled Staff**
- **Foreign Intelligence Services**
- **Hackers**
- **Internal Attackers /bystanders**
- **Protestors and Activists**
- **Staff undertaking unauthorized actions**
- **Terrorists**



- I. **Use a Denial of Service (DoS)** attack to crash the SCADA server leading to shut down condition (System Downtime and Loss of Operations)
- II. **Delete system files** on the SCADA server (System Downtime and Loss of Operations)
- III. **Plant a Trojan** and take complete control of system (Gain complete control of system and be able to issue any commands available to Operators)
- IV. **Log keystrokes** from Operators and obtain usernames and passwords (Preparation for future take down)
- V. **Change data points** or deceive Operators into thinking control process is out of control and must be shut down (Downtime and Loss of Corporate Data)
- VI. Use SCADA Server as a launching point to defame and compromise other system components within corporate network. (**IP Spoofing**)
- VII. **Modify any logged data** in remote database system (Loss of Corporate Data)

Some Common attacks on the SCADA host system

## SCADA Attack Matrix

Description of Attack	Type of Attack	Attack Motive	Impact to Victim	Impact Rating (1 = largest immediate impact 5 = least immediate impact)	Items Needed for Attack	Estimated Time to Implement Once System is Compromised
Denial of Service	System Shutdown	Wish to take down server and cause immediate shutdown situation	SCADA Server locks up and must be rebooted. When SCADA Server comes back on-line, it locks up again. Operations can no longer monitor or control process conditions, and the system will ultimately need to be shut down	2	Ability to flood the server with TCP/IP calls, the IP Address of SCADA Server, and the path to the server	5 min.
Delete System Files (Low-level format on all local drives)	System Shutdown	Wish to take down server and cause immediate shutdown situation	Critical Server and SCADA files are lost and operations can no longer monitor process or control plant or facility	4	IP Address of SCADA Server, path to server, and permission to delete files permission can be escalated used other tools)	15 min.
Take Control of SCADA System	Gain Control	Gain control of SCADA System to impact damage on industrial systems, possibly causing environmental impact, and damage corporate identity through public exposure	Highest impact, since attacker can then manually override safety systems, shut down the system, or takes control of the plant operational conditions.	1	IP Address of SCADA Server, path to server, and either Trojan or back door installed. (Can also use PCAnywhere, Terminal Services, SMS, or other system admin services.)	1 hr.
Log Keystrokes, Usernames, Passwords, System Setpoints, and any Operational Information	Information Mining	Gain Information for future attacks or satisfy curiosity	Lower immediate impact, but information gained can be used for future attacks.	4	IP Address of SCADA Server, path to server, and software or mechanism for logging the keystroke activities.	15 min.



## SCADA Attack Matrix

Description of Attack	Type of Attack	Attack Motive	Impact to Victim	Impact Rating (1 = largest immediate impact 5 = least immediate impact)	Items Needed for Attack	Estimated Time to Implement Once System is Compromised
Change Data Points or Change Setpoint(s) in SCADA System	Information Tampering	Desire to modify corporate data or process setpoints for malicious purposes	Higher impact since modified setpoint or control points can have adverse effects on controlled process, and potentially cause a shutdown condition	2	IP Address of SCADA Server, access to these servers, and some knowledge of SCADA software system inner workings	45 min.
Log any Operational or Corporate data for personal gain or sell to competition or hold as ransom	Information Mining	Try to steal corporate data and either sell to other companies or hold for ransom amount	Low environmental or immediate damage, but can damage corporate image if attacker builds attention to the fact that this system was compromised	4	IP Addresses of SCADA and database servers. (Would not even need IP addresses if protocol sniffer/logger used to sniff TCP/IP traffic.)	30 min.
Modify Data points on SCADA graphics to deceive Operators that system is out of control and must ESD (Emergency Shut Down)	System Shutdown	Cause danger to the facility or company by staging a false alarm shutdown of the plant or facility	Operations can no longer trust the SCADA System, and the attacker has deceived the Operator into thinking that there was an emergency condition in the plant	2	IP Addresses of SCADA servers, and access to them through the company network	45 min.



## SCADA Attack Matrix

Description of Attack	Type of Attack	Attack Motive	Impact to Victim	Impact Rating (1 = largest immediate impact 5 = least immediate impact)	Items Needed for Attack	Estimated Time to Implement Once System is Compromised
Capture, Modify, or Delete Data Logged in Operational Database SQL Server, PI Historian, Oracle, Sybase, etc.)	Information Tampering	Desire to modify corporate data or process setpoints for malicious purposes	Higher impact since modified setpoint or control points can have adverse effects on controlled process, and potentially cause a shutdown condition	3	IP Address of SCADA Server, path to database server, and knowledge of SCADA software structure	45 min.
Locate Maintenance Database and modify or delete information regarding calibration and reliability tests for industrial equipment	Information Tampering	Desire to steal, modify, or delete corporate data.	Less immediate danger, but corporate information data warehouse would be comprised	4	IP Addresses of database servers	30 min.





# The need for cyber-security in rail transit control systems

A transit agency is a very complex organization that has equipment that moves along railroad tracks. The systems that have been used to control and communicate are located along the routes in **wayside bungalows**, **stations**, **road crossings**, **signal towers**, **tunnels**, **maintenance yards**, power stations, refueling depots, equipment storage yards/parking lots, storage depots, local control rooms and operations control rooms. There are also key parts of the control system buried under or alongside the rail lines and signals that are transmitted in the rails or via specialized aerial paths.

There are several differences between a rail transportation system and a single manufacturing site:

- distance
- communication
- power
- **people**



# The need for cyber-security in rail transit control systems

- Modern [railway systems](#) rely on a wide range of digital equipment. For example, cab signaling, traction control systems, automatic train control (ATC) systems for controlling the train and directing operators, protection systems, and passenger information and entertainment systems.
- Waysides and train stations rely on digital systems for computer-based interlocking (CBI), centralized traffic control, level crossing protection, and switching yard automation. Digital systems are also used in traction substations, and in ticket/passenger information system.
- that railway systems are not difficult to hack, but the task does require specific knowledge in railway automation
- Analyzed various components of a railway system in an effort to raise awareness of the existing security weaknesses and force governments, vendors and operators to review their approach to railway cyber security.

# The need for cyber-security in rail transit control systems

**TABLE 3**

Malware Infection Methods


<b>Supply chain</b>	Undesirable software/functions may already be embedded or pre-loaded in off-the-shelf equipment. Vendors may deliver infected or un-validated software.
<b>Human factors</b>	Irresponsible use of portable media (USB) for unauthorized data/program transfer.
<b>Inadequate physical security</b>	Who is touching or can touch "secure" equipment?
<b>Inadequate configuration management</b>	Unknown connections may be made through a change to the system.
<b>Unexpected/indirect connections</b>	There are paths from one system to another that may not be anticipated or understood.



# The need for cyber-security in rail transit control systems

## APTA-Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones

**TABLE 2**  
Zone Names

Importance	Zone	Example System
<b>Most Safety Critical</b>  <b>Most Public</b>	Safety- Critical Security Zone (SCSZ)	Field signaling and interlocking
	Fire, Life-Safety Security Zone (FLSZ)	Fire detection/suppression
	Operationally Critical Security Zone	Traction power SCADA
	Enterprise Zone	Fare systems, turnstiles, accounting systems, schedule systems
	External Zone	Communications with the Internet, business partners, vendors and others

# Railway System Vulnerabilities

- **SIBAS**, a train protection system that is widely used in many European countries. SIBAS uses Siemens SIMATIC components, such as the WinAC RTX controller, which is designed for PC-based automation solutions.
- Experts have pointed out that **WinAC RTX** has several security **weaknesses**, including the ability to control the device without authentication, and the use of known protocols such as XML over HTTP, which makes it possible to create tools for controlling the device.
- Another railway component analyzed by researchers is **computer-based interlocking (CBI)**, a signaling system designed to prevent the setting up of conflicting routes.
- Experts believe there are three types of threats when it comes to **CBIs: safety, economics and reliability**. If an attacker can gain access to such a system, they can cause physical damage by changing a switch while a train is passing over it or by setting up conflicting routes. Causing a CBI component to crash, blocking controls or providing false information can have a negative impact on the operator's revenue. Finally, causing the communications network to crash can affect the system's reliability

# Railway System Vulnerabilities

- ➔ Attacks against CBI can be conducted by a malicious actor who has **physical access** to the system or by using **social engineering** to trick someone with access to the system to execute malicious code (e.g. insert a malicious USB drive).
- ➔ An attacker can also target the **communications systems** that connect various components of the CBI with each other and with the outside world.
- ➔ In some countries, such as **India and Germany**, there are companies that specialize in telecommunications for railways. **In Germany, DB Netze** provides **special GSM-R SIM** cards that are used to connect trains to control centers.
- ➔ These SIM cards have good encryption, but a malicious actor could attempt to **jam** the connection between the train and the control center using a **GSM jammer**. Researchers have pointed out that in areas where certain levels of the European Train Control System (**ETCS**) are used, trains automatically stop if the connection between the train's **modem and the control center is lost**. This means that an attacker who can jam the connection can cause a train to stop.
- ➔ **another problem with GSM-R** is that some handsets have a feature that can be used to manage the devices via **SMS**. An authentication feature that relies on a PIN is used to prevent abuse, but the **default code is 1234** and researchers believe engineers rarely change it. Over the air (OTA) management features present in some GSM-R equipment also introduce security risks, especially since some support OTA firmware updates.
- ➔ The **modems** used for GSM-R could also be vulnerable to the types of **mobile modem attacks** disclosed by Positive Technologies researchers — some of whom are members of the SCADA StrangeLove team — in early December. As demonstrated by experts at the time, an attacker who can compromise a modem, for example by using a malicious firmware update pushed via OTA, could also hack the host the modem is connected to.

# Railway System Vulnerabilities

In the case of railway systems, an attacker who can **compromise the modem**, could then **hijack the automatic train control system**, which can allow them to control the train.

**Modern trains also have entertainment systems, passenger information systems, intercoms, IP cameras and wireless access points**, and these systems can also pose a risk because they all operate via **one communications channel**.

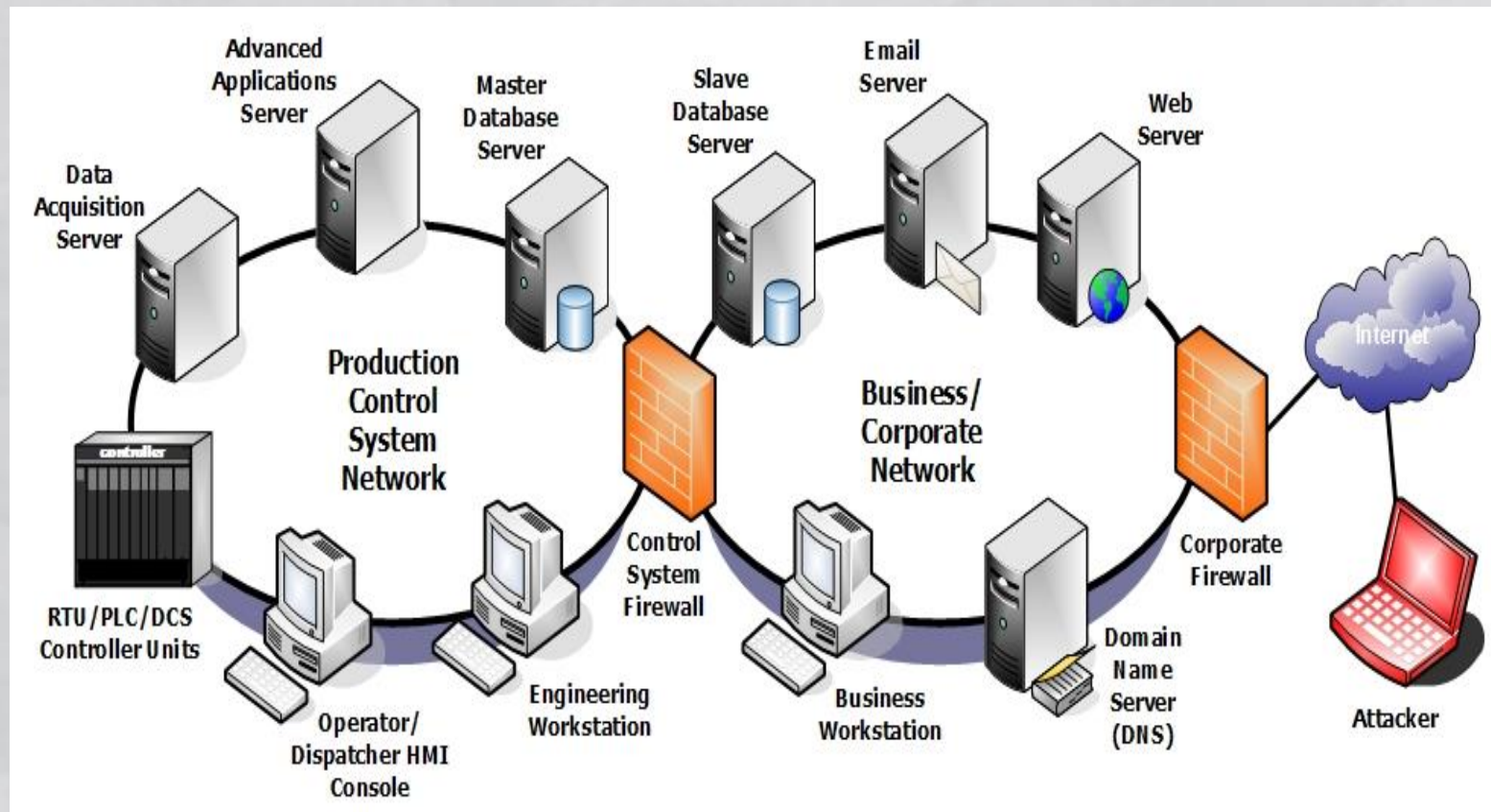
Researchers analyzed various devices from vendors like Bintec, Digi, Moxa, NetModule and Sierra Wireless that are used in railway systems. One concern with these devices is that their firmware in many cases includes hardcoded private keys for SSL certificates and **remote administration features**. This exposes supposedly secure communications **to man-in-the-middle attacks** and allows attackers to remotely login to a device. Attackers can also use the exposed keys to fingerprint devices and attempt to find equipment that is accessible over the Internet using services like Shodan and Censys.

Devices used in railway systems can be exposed to attacks due to the use of default credentials, and researchers have also found RCE vulnerabilities.

According to experts, some of the devices that have a USB port have the Autorun feature enabled. This feature is designed to enable engineers to easily perform software and configuration updates, but it also introduces security risks.

Researchers pointed out in their presentation at 32C3 that while railway systems appear to be isolated from the Internet, an attacker can use the security holes present in various components to reach critical systems remotely.

# Understanding Control System Cyber Vulnerabilities



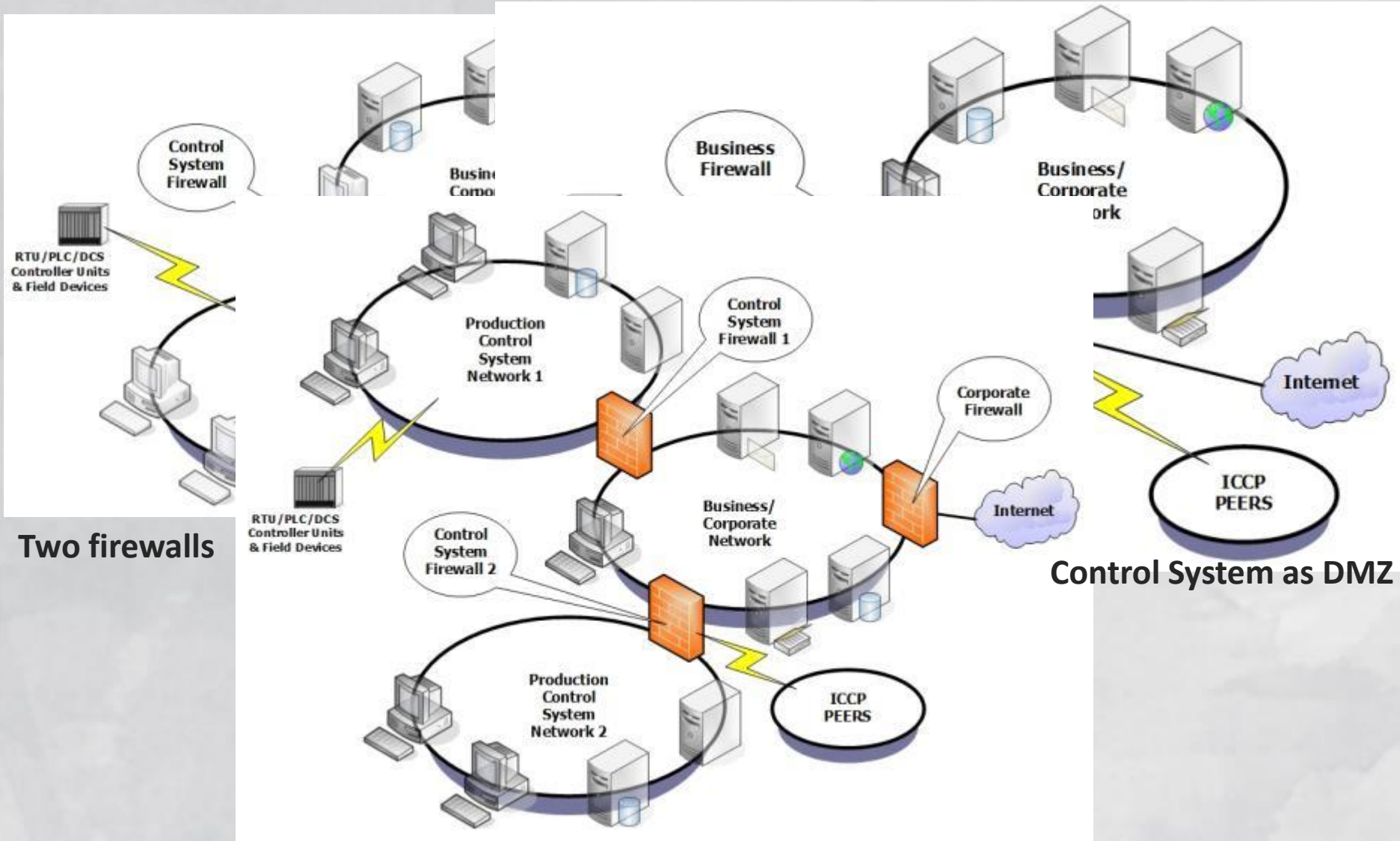
Typical two-firewall network architecture

## An attacker facing three challenges

- I. Gain access to the control system LAN
- II. Gain understanding of the process
- III. Gain control of the process.



# Access to the Control System LAN



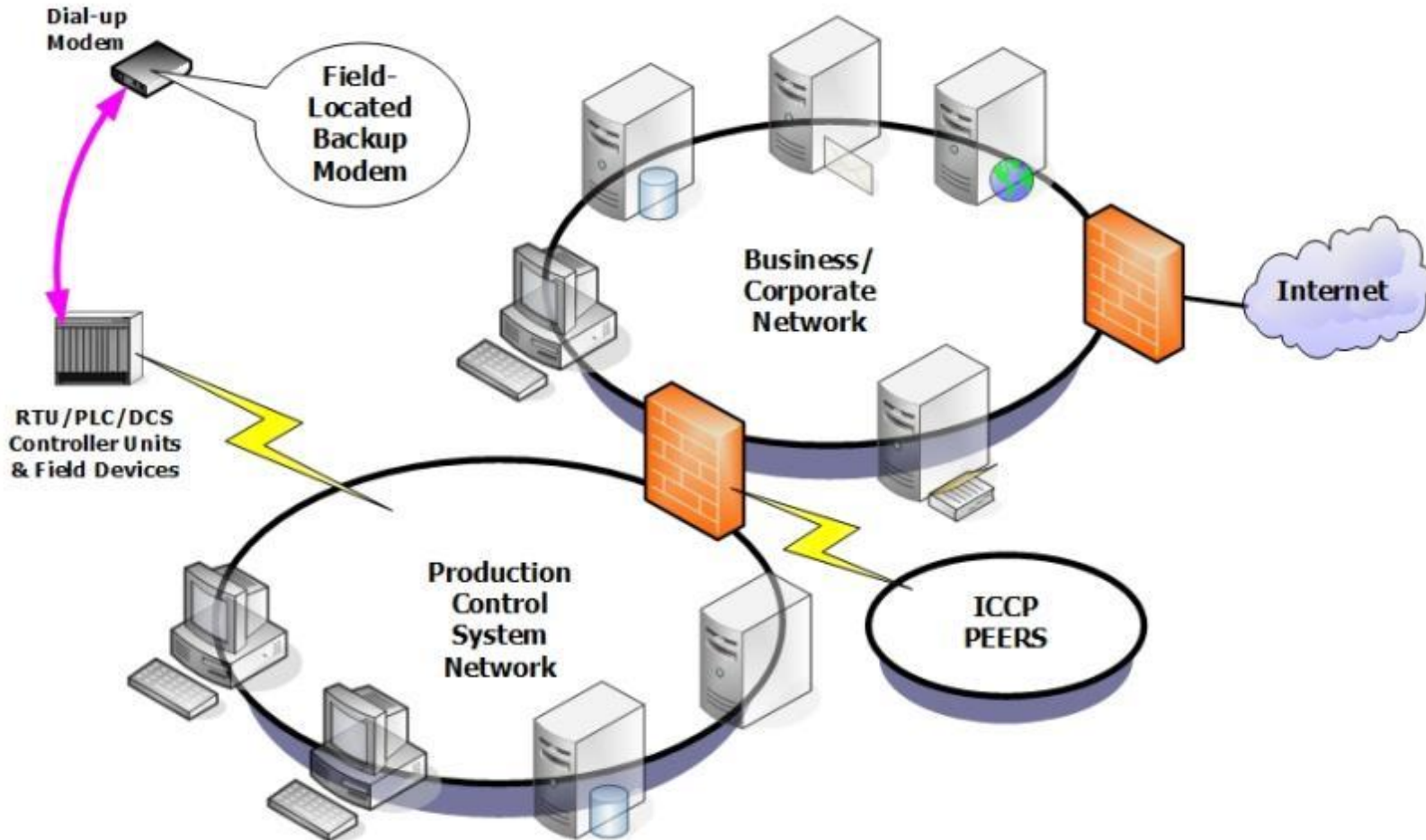
Two firewalls

Control System as DMZ

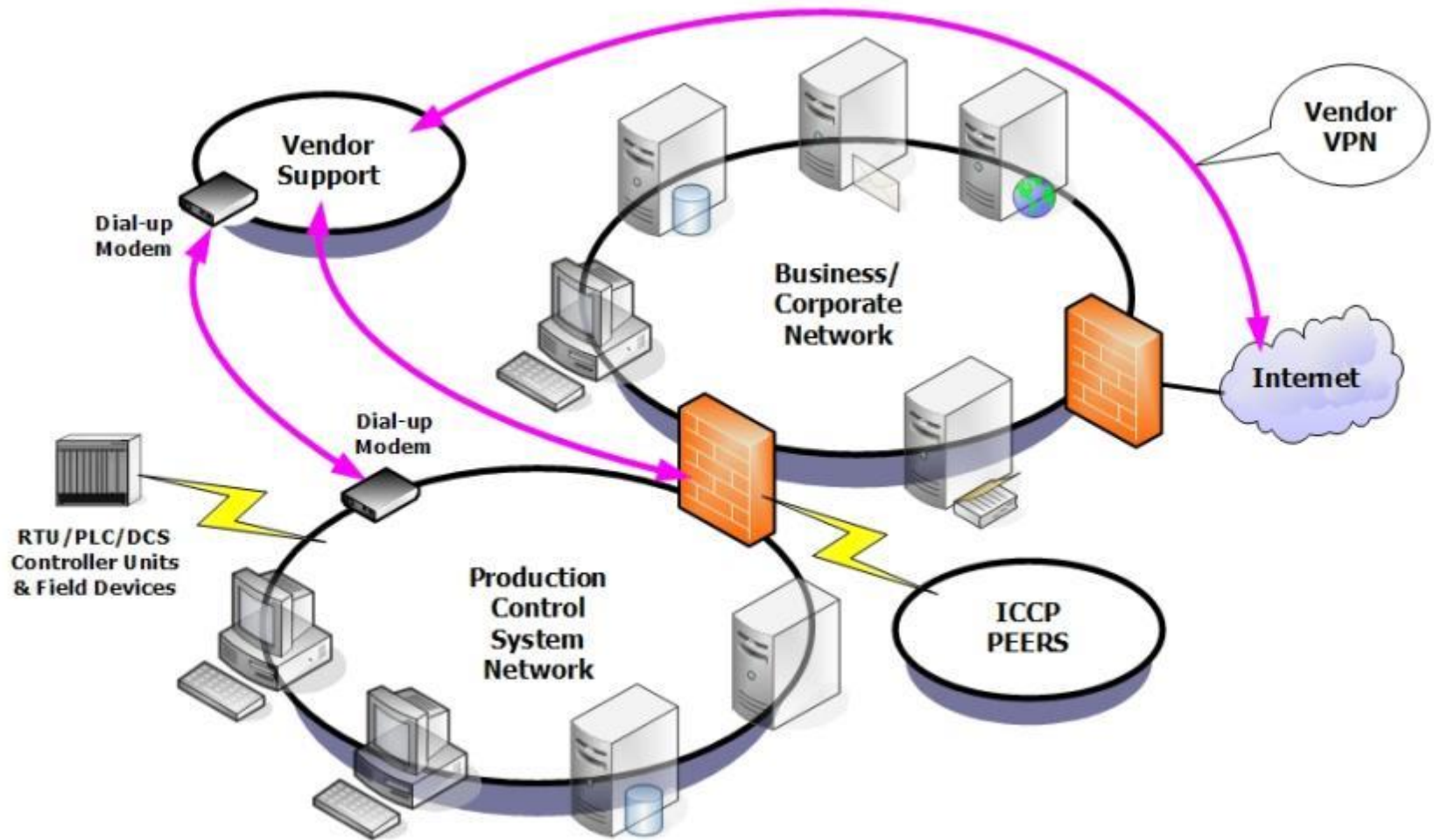
Business LAN as backbone

Common Network Architectures

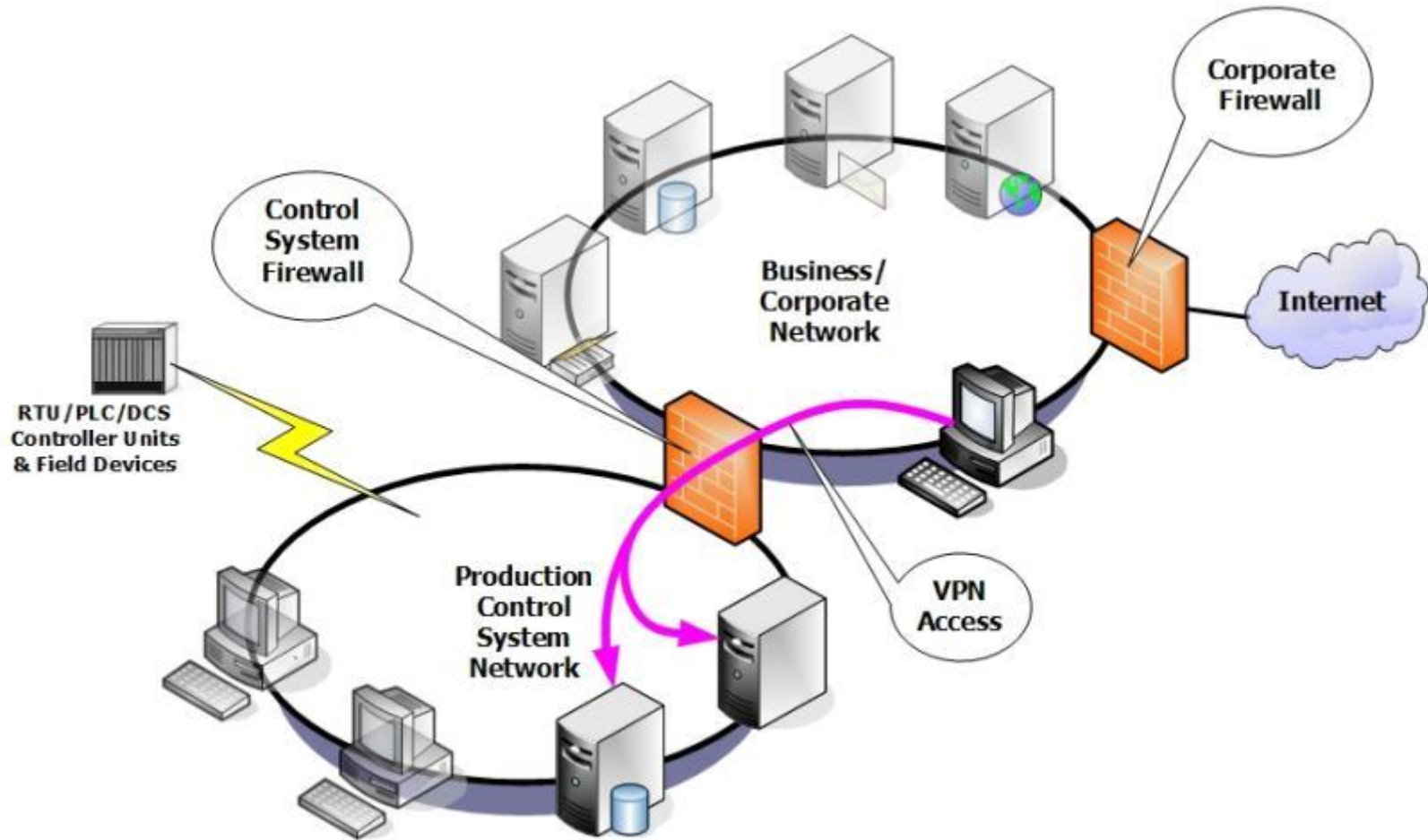
# Dial-up Access to the RTUs



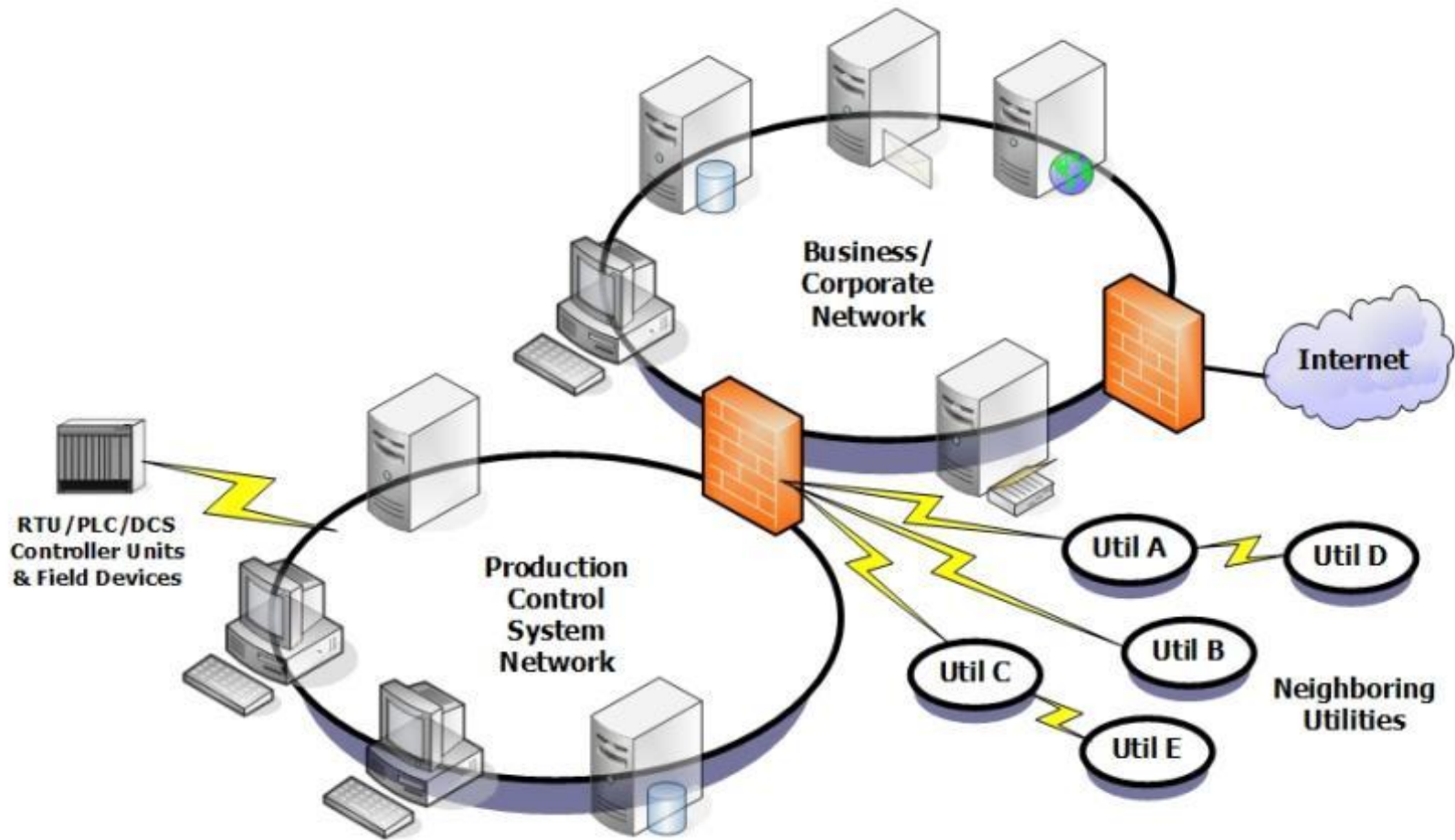
# Vendor Support



# Corporate VPNs



# Peer Utility Links

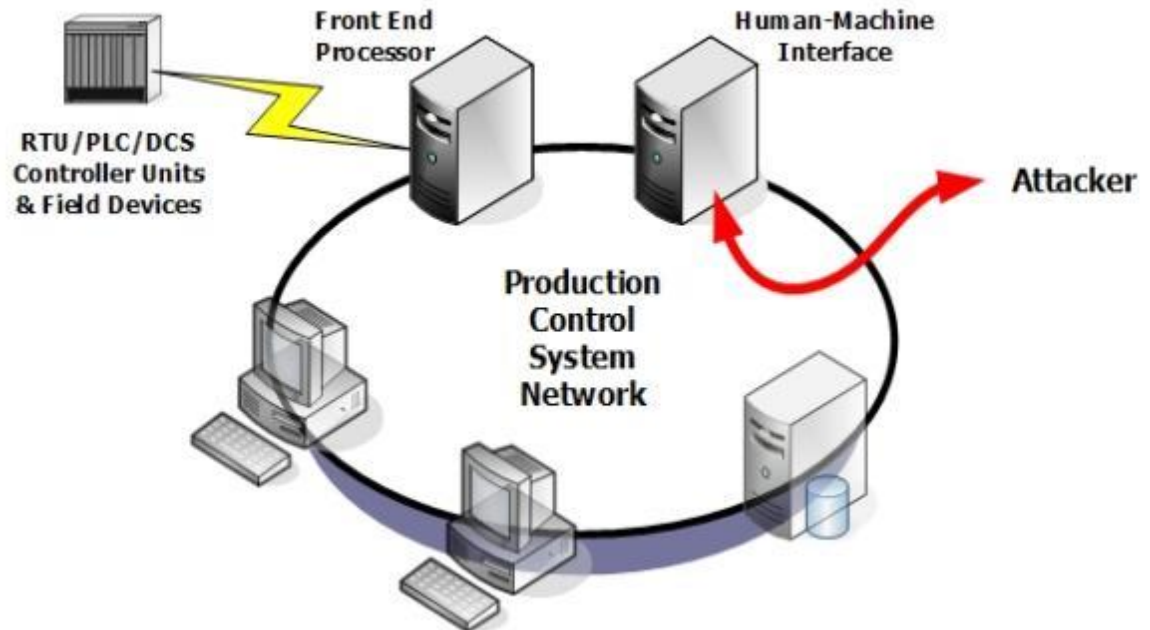


# Control of the Process

- Discovery of the Process**
- Sending Commands Directly to the Data Acquisition Equipment**
- Exporting the HMI Screen**
- Changing the Database**
- Man-in-the-Middle Attacks**

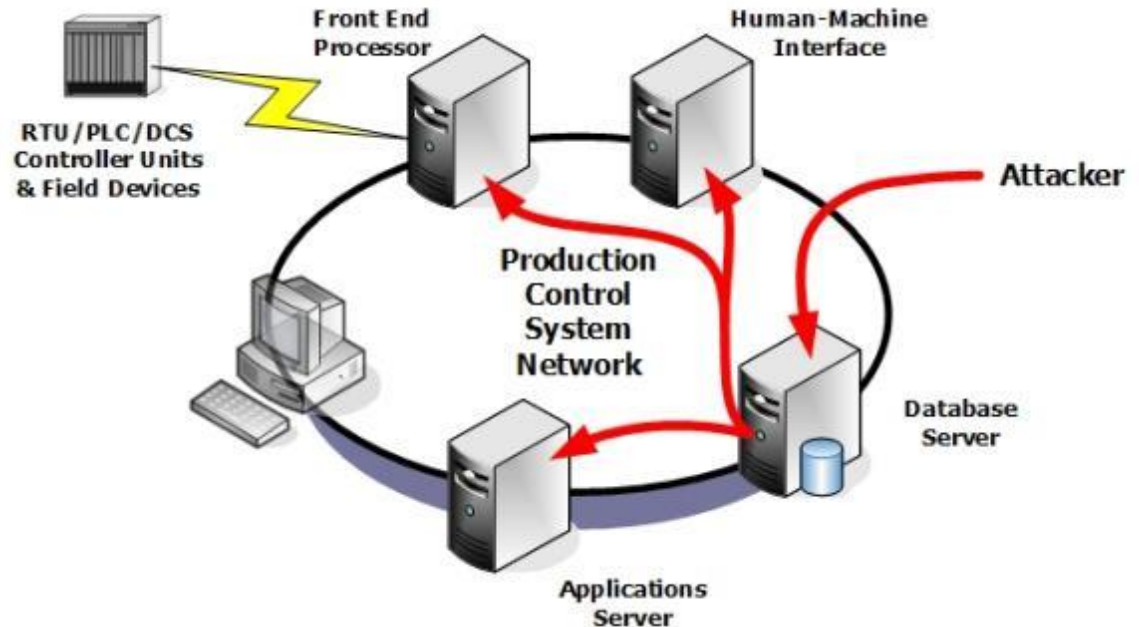
# Control of the Process

- ❑ Discovery of the Process
- ❑ Sending Commands Directly to the Data Acquisition Equipment
- ❑ Exporting the HMI Screen
- ❑ Changing the Database
- ❑ Man-in-the-Middle Attacks



# Control of the Process

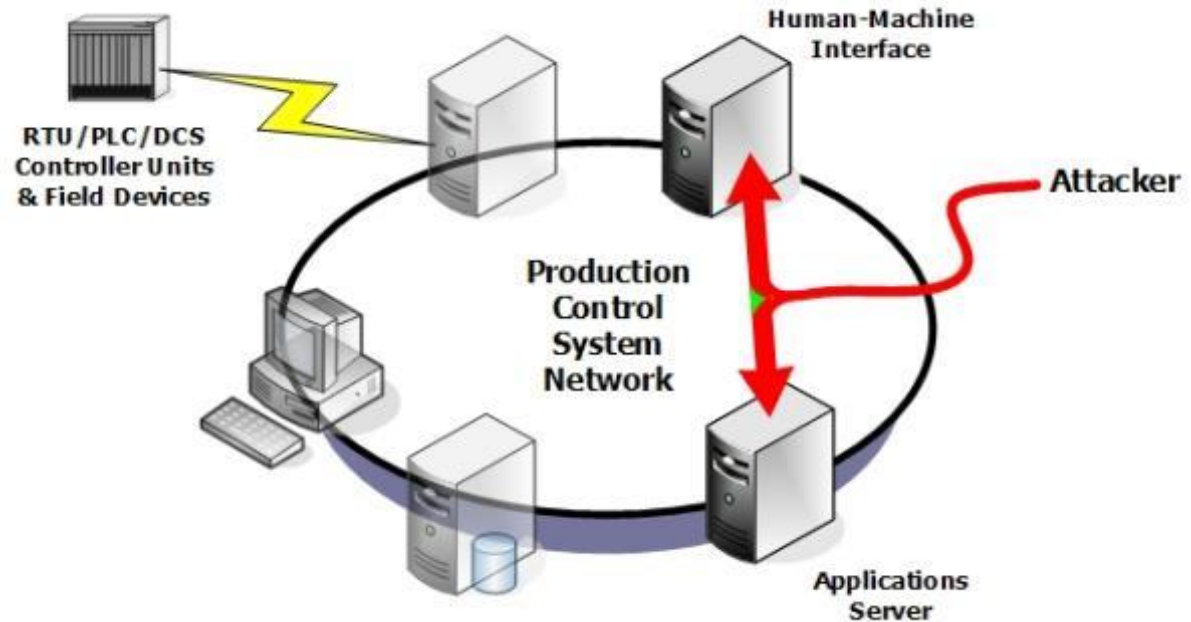
- ❑ Discovery of the Process
- ❑ Sending Commands Directly to the Data Acquisition Equipment
- ❑ Exporting the HMI Screen
- ❑ Changing the Database
- ❑ Man-in-the-Middle Attacks

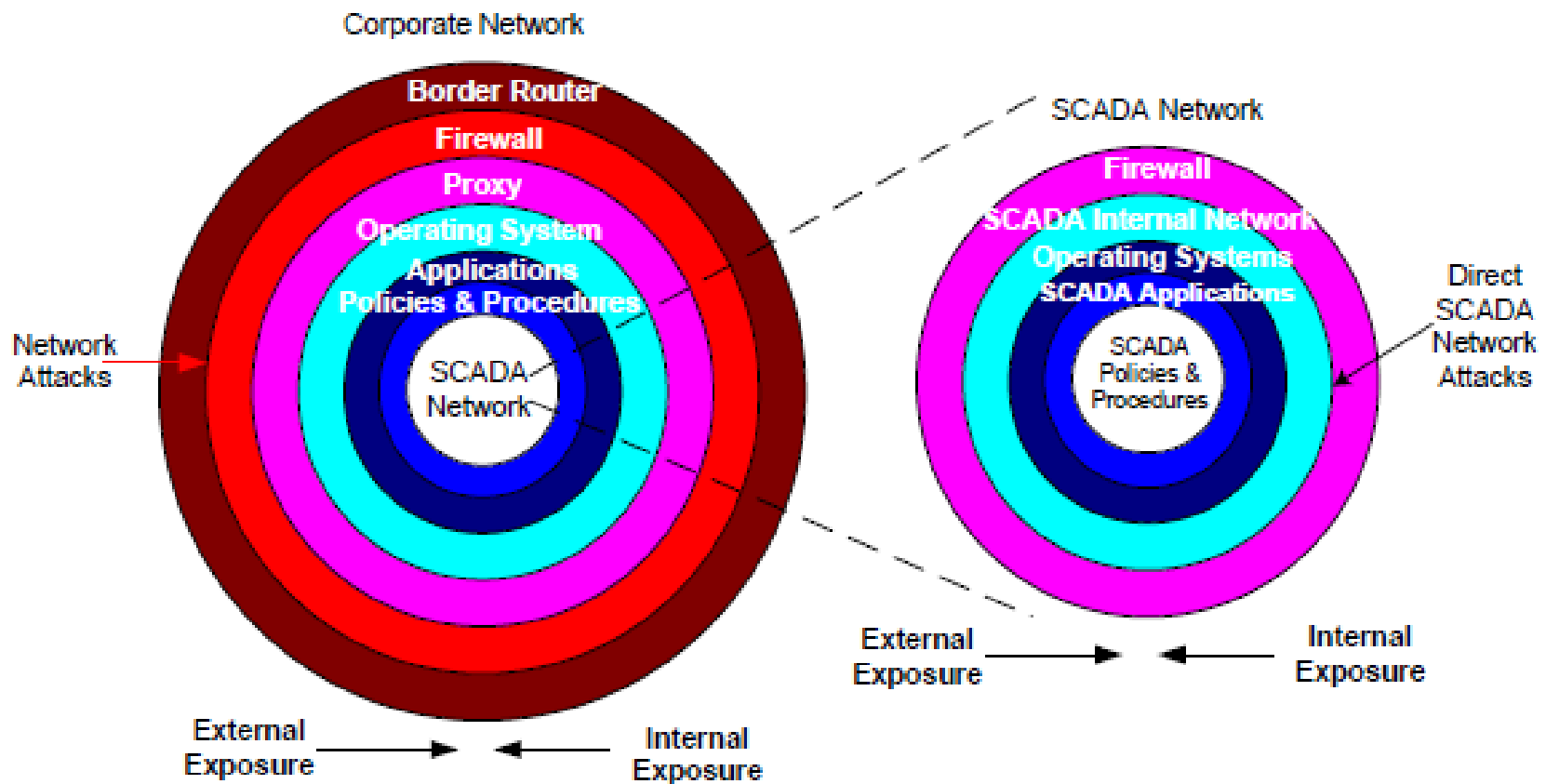




# Control of the Process

- Discovery of the Process
- Sending Commands Directly to the Data Acquisition Equipment
- Exporting the HMI Screen
- Changing the Database
- Man-in-the-Middle Attacks





Ring of defenses

## Developing a SCADA Security Strategy

Developing an appropriate SCADA security strategy involves analysis of multiple layers of both the corporate network and SCADA architectures including firewalls, proxy servers, operating systems, application system layers, communications, and policy and procedures

# Developing a SCADA Security Strategy

## Border Router and Firewalls:

- ❑ Firewalls, properly configured and coordinated, can protect passwords, IP addresses, files and more. However, without a hardened operating system, hackers can directly penetrate private internal networks or create a Denial of Service condition

## Proxy Servers

- ❑ A Proxy server is an internet server that acts as a firewall, mediating traffic between a protected network and the internet. They are critical to re-create TCP/IP packets before passing them on to, or from, application layer resources such as Hyper Text Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP). However, the employment of proxy servers will not eliminate the threat of application layer attacks.



# Developing a SCADA Security Strategy

## Operating Systems

- ❑ Operating systems can be compromised, even with proper patching, to allow network entry as soon as the network is activated.. As a result, operating systems are a prime target for hackers. Further, in- place operating system upgrades are less efficient and secure than design-level migration to new and improved operating systems.

## Applications

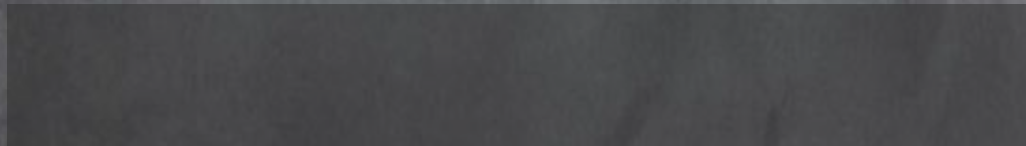
- ❑ Application layer attacks; i.e., buffer overruns, worms, Trojan Horse programs and malicious Active-X5 code, can incapacitate anti-virus software and bypass the firewall as if it wasn't even there.

## Policies and Procedures

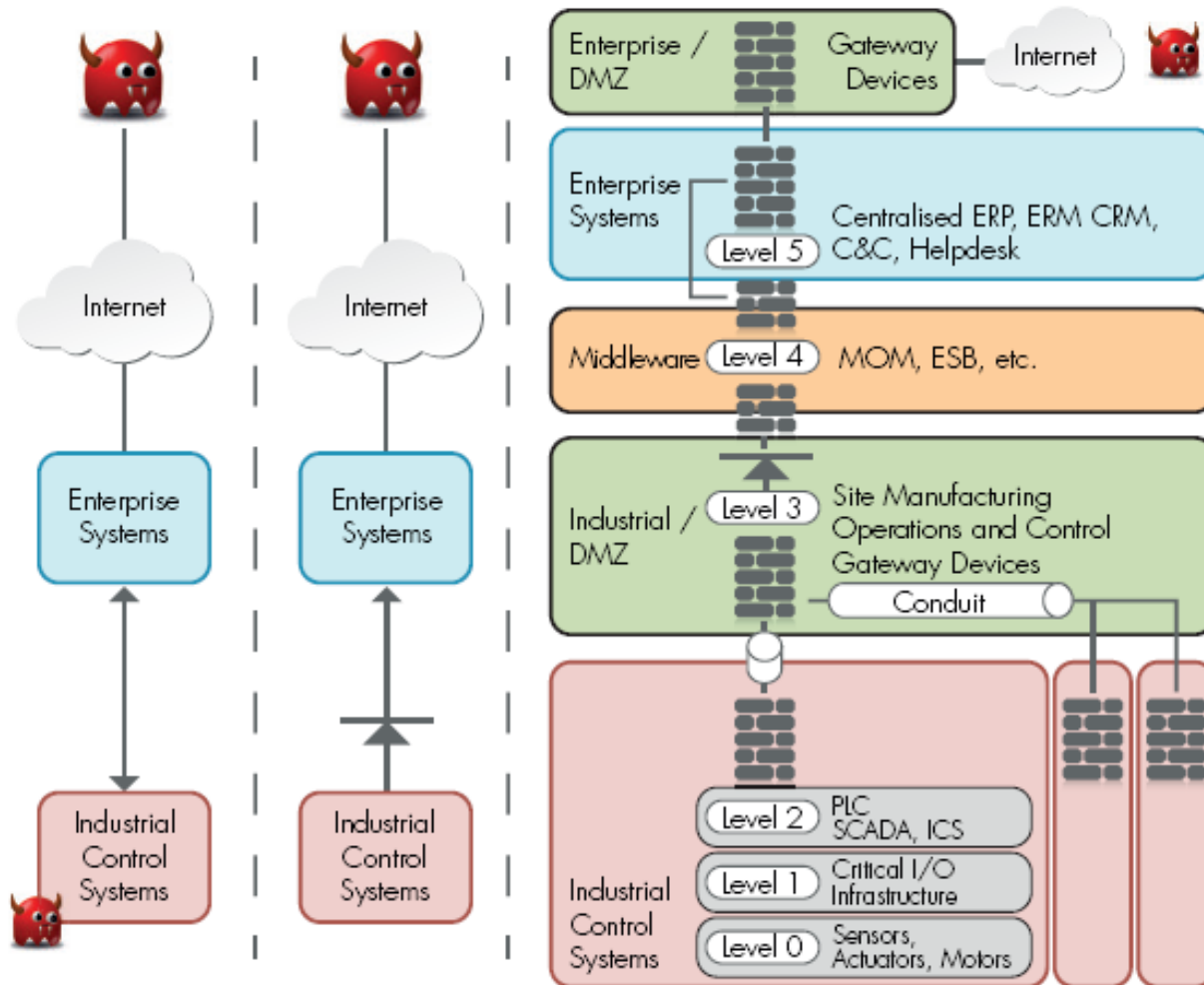
- ❑ Policies and procedures constitute the foundation of security policy infrastructures. They include requiring users to select secure passwords that are not based on a dictionary word and contain at least one symbol, capital letter, and number, and should be over eight characters long. Users should not be allowed to use their spouse, child, or pet's name as their password.

# Developing a SCADA Security Strategy

- ✓ **SCADA Firewalls**
- ✓ **SCADA Internal Network Design**
- ✓ **SCADA Server Operating Systems**
- ✓ **SCADA Applications**
- ✓ **SCADA Policies and Procedures**



# Zoning, Segregation, and Protection of Industrial Networks



**Defense-In-Depth : as a recommended approach for securing rail communications and control systems,**  
**defines :security zone classifications, and**  
**defines a minimum set of security controls for the most critical zones,**  
**SAFETY CRITICAL SECURITY ZONE (SCSZ)**  
**and**  
**FIRE, LIFE-SAFETY SECURITY ZONE (FLSZ)**

Intrusion Detector  
**Zoning & Segregation**



# **RTU Configuration** Security Constraints and Vulnerabilities Evaluation

Applicable Standards 



# Regulatory Compliance

**With the emergence of cyber threats and the need to secure data, standards have arisen for other industries**

IEEE 1686

UK CPNI Security Guides Centre for Protection of National Infrastructure

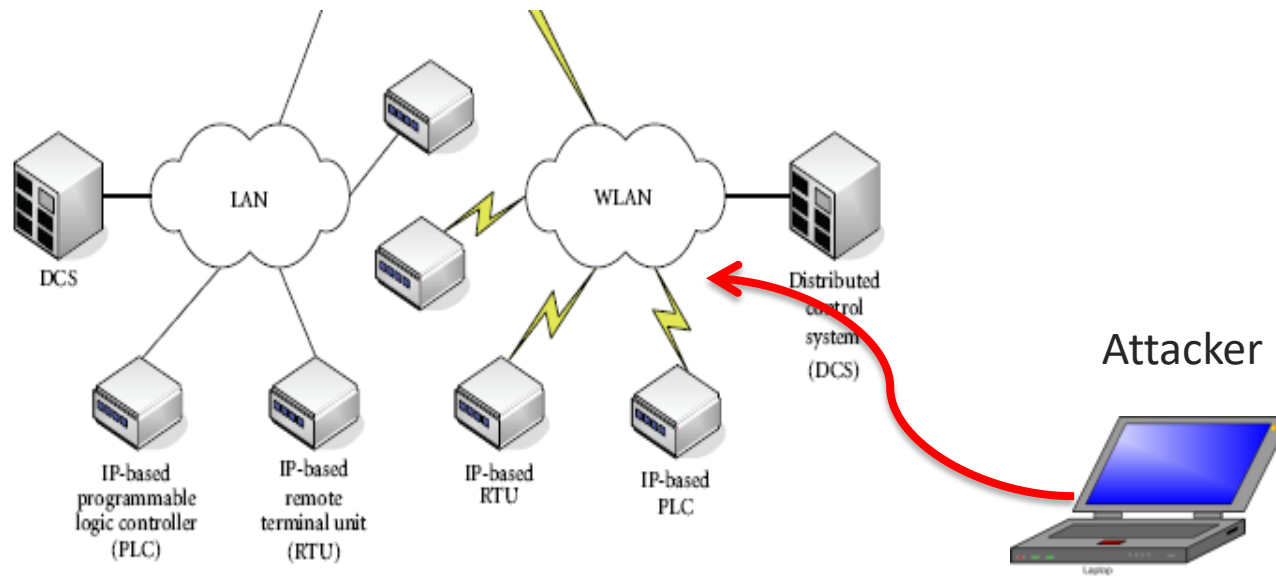
USA NIST 800-82

ISA 99

IEC62443

# Vulnerabilities

- » **Gaining Access to the Network at any site**
- » **Changing RTU/PC Configuration**
- » **Sending unauthorized Commands to the field**
- » **Sending wrong Data (status/analogue measuring) to Center**
- » **Manipulating System Setting**
- » **Interception of Data stream or disrupting RTU's connection to CS**



# Security measures of RTU/PC

## ➤ Physical interfaces

### *To reduce exposure for cyber-attacks*

- *Strict limitations and authority control*
- Security Permission Form.( Authorized Personnel )
- RTU/PC Cubicle should be locked
- The Signal Event of RTU/PC Door opening is to defined and sent to C.S
- preventing the unauthorized use of removable media (such as USB memory sticks) in station computers.

## ➤ Communication ports and services

<u>Port</u>	<u>Protocol</u>	<u>comment</u>
21	TCP	File transfer protocol
2102	TCP	IED configuration protocol

(1) Regular and thorough inspection of security and vulnerability,

# Security measures of RTU/PC

## Managing user roles and user accounts

Certification, Authorization with role based access control

The user roles with different user rights should be predefined in the IED.

## Password policies

To achieve IEEE 1686 conformity, a password with a minimum length of 8 characters must be used, and the square Enforce Password Policies shall be ticked “ lowercase letters ( a - z )/ uppercase letters ( A - Z ) numeric letters ( 0 - 9 )/special characters ( !@#+"\*%&/=? )/ Password expiry time

## Security Event

*A security event contains an event ID, a time stamp, a sequence number, the user name, the severity of the action and the name of the source. These events can be sent to external security log servers using Syslog.*

Syslog is a standard for computer message logging

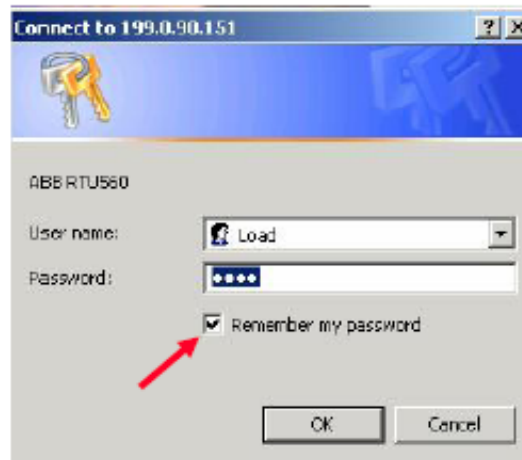
All Security events, All user actions Logging/ Configuration

Download/Upload



# Managing user roles and user accounts

## The Webserver, General



The access to the Webserver is protected by user-name and passwords.

For more easy use, the password can be stored on the client PC.

Show  
Load  
Control  
Admin

Show  
Load  
Control  
Admin

User is allowed to show information  
User is allowed to load configuration/firmware  
User is allowed to perform commands  
User is allowed to create/modify other user

Start change

Accept changes

Decline changes

## Predefined user roles according to IEC 62351-8

User roles	Role explanation	User rights
VIEWER	Viewer	Can read parameters and browse the menus from LHMI
OPERATOR	Operator	Can read parameters and browse the menus as well as perform control actions
ENGINEER	Engineer	Can create and load configurations and change settings for the IED and also run commands and manage disturbances
INSTALLER	Installer	Can load configurations and change settings for the IED
SECADM	Security administrator	Can change role assignments and security settings
SECAUD	Security auditor	Can view audit logs
RBACMNT	RBAC management	Can change role assignment

# Syslog

- ✓ [#017: At least one analog value faulty]
- ✓ [#018: At least one digital value faulty]
- ✓ [#019: At least one pulse counter value faulty]
- ✓ [#020: At least one object or regulation faulty]
- ✓ [#021: At least one analog output faulty]
- ✓ [#022: At least one digital output faulty]
- ✓ [#023: RTU is faulty]
- ✓ [#024: Device active]

SNMP network element supervision

SNMP Network element number

Configuration

External security log servers

Send security events to external log servers

Configuration

Configuration

External Security Log Servers

	Client Type	IP Address	IP Port
1. External Log Server	Syslog UDP	10 . 10 . 000 . 1	514
<input type="checkbox"/> 2. External Log Server	Syslog UDP	0 . 0 . 0 . 0	514
<input type="checkbox"/> 3. External Log Server	Syslog UDP	0 . 0 . 0 . 0	514

OK

Host Interface

Host number:

Buffer size for Priority 1 Datapoints:

entries

Buffer size for Priority 2 Datapoints:

entries

Buffer size for Integrated Totals (ITI):

entries

Priority of the ITI queue:

Buffer size for spontaneous transmit:

entries