CH 09
ICS/SCADA SYSTEM SECURITY FOR CPS

Course Code: CYS401

CHAPTER OVERVIEW

- Introduction to ICS/SCADA Systems Security
- Architecture of ICS/SCADA
- ICS/SCADA Vulnerabilities
- Attacks, Threats, Challenges in ICS/SCADA
- Security Objectives, Requirements, Security Policies, Governance and Compliance
- Case Studies: Smart Grid

INTRODUCTION TO ICS/SCADA SYSTEMS SECURITY

- **Cyber-physical systems** CPSs are a various collection of information communication technology (ICT) and embedded microprocessors which are communicated to the physical world via sensors and actuators.
- **Applications of CPS:** Smart Grid
- **ICS/SCADA:** The remote activities of the CPS applications(smart grid's) are monitored and controlled by specialized computing system called **industrial control systems** (ICSs) or **supervisory control and data acquisition** (SCADA) systems (ICS/ SCADA).
- **Importance of ICS/SCADA security**: It is very crucial to keep ICS/SCADA system safe and secure in order to prevent any cyber attack that causes a physical hazard to the CPS applications(smart grid), which might affect the human life, national safety, or economy.

INTRODUCTION TO ICS/SCADA SYSTEMS SECURITY

- **Few more commercials of CPS:**
  - The water supply, (Water Treatment and Distribution)
  - Oil and Gaz Industry,
  - Transportation and Smart Cities
  - Telecommunication
  - Electricity power generation and transmission. (Smart Grids and Power Systems)
  - Manufacturing and Automation
- **ICS/SCADA requirements**: The operations of CPSs need to be safe to avoid any hazard to the human and the surrounding environment, by ensuring and maintaining the security properties confidentiality, integrity, and availability (CIA). In addition, any cyber attacks targeting CPSs working for the critical infrastructure such as smart grid will have a great negative impact; it might go further of losing the human lives.
- **Security attacks**: eavesdropping, denial of service (DoS), and the wireless jamming etc.

INTRODUCTION TO ICS/SCADA SYSTEMS SECURITY

- **ICS** : These systems are used in national critical infrastructure (such as smart grid) to monitor, manage, and control various critical processes and physical functions, remotely and in a real-time manner.

ICS is a general term and includes many various types of control systems such as **SCADA** and **distributed control systems** (DCSs).

- **Functionality of ICS/SCADA:** ICS/SCADA systems are meant to acquire data from various remote instruments such as pumps, transmitters, valves, etc. and control them remotely from a host's central SCADA software

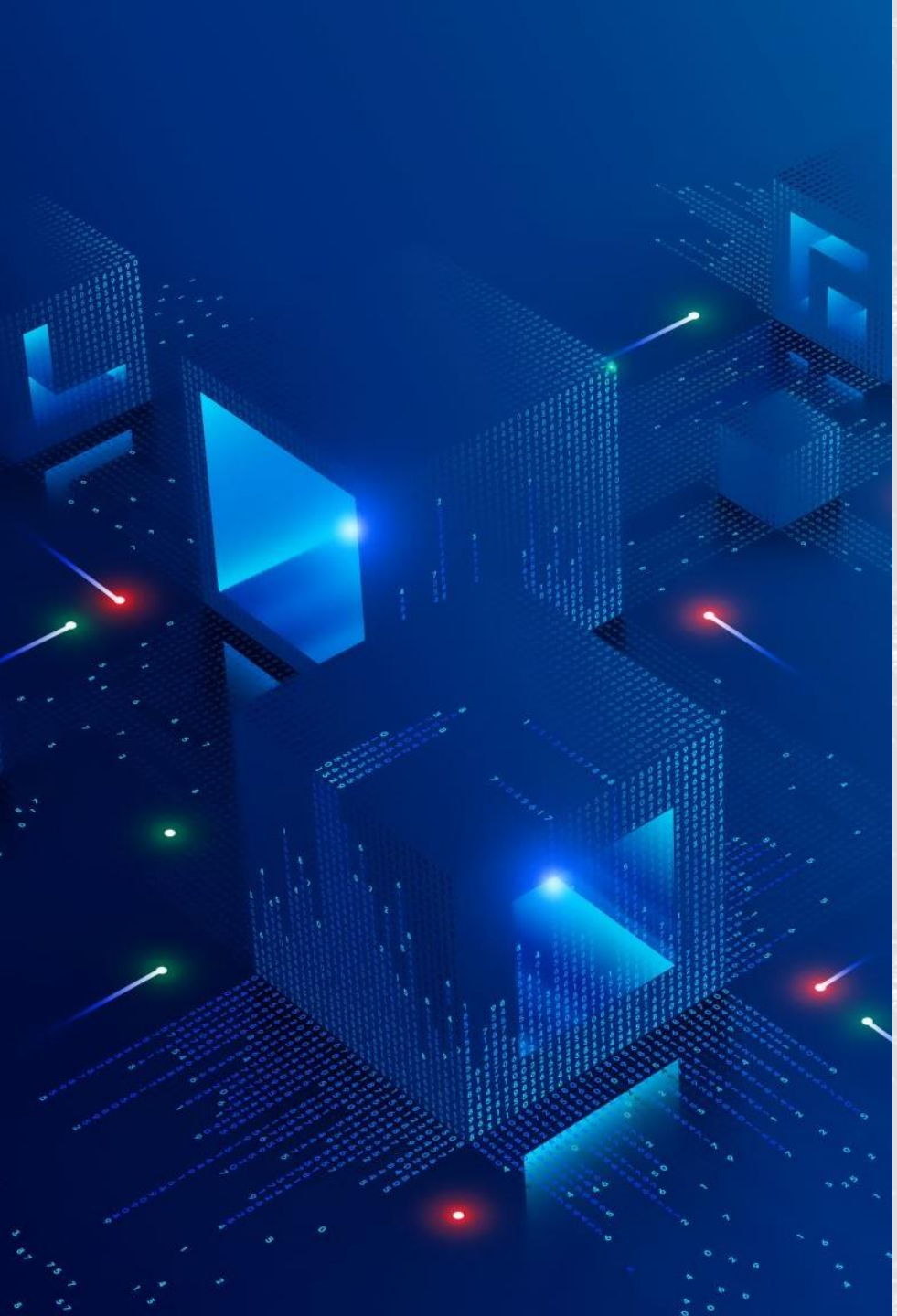
IT VS OT ENVIRONMENTS

- Information Technology (IT)
  - Focus on data processing
  - Confidentiality is the top priority
  - Frequent updates and patching
  - Short system lifecycle
- Operational Technology (OT)
  - Focus on physical processes
  - Availability and safety are priorities
  - Limited downtime allowed
  - Long system lifecycle

- **Components of ICS/SCADA**: it is composed of computers, networks, and embedded devices which work together to monitor, manage, and control vital processes in various industrial and critical infrastructure areas such as oil and power management.

This combination consists mainly of:

- **Field instrumentation (Sensors and Actuators)**
- **programmable logic controllers (PLCs) and/or remote terminal unit (RTUs),**
- **communications networks, and**
- **ICS/SCADA host software (Human-Machine Interface (HMI))**

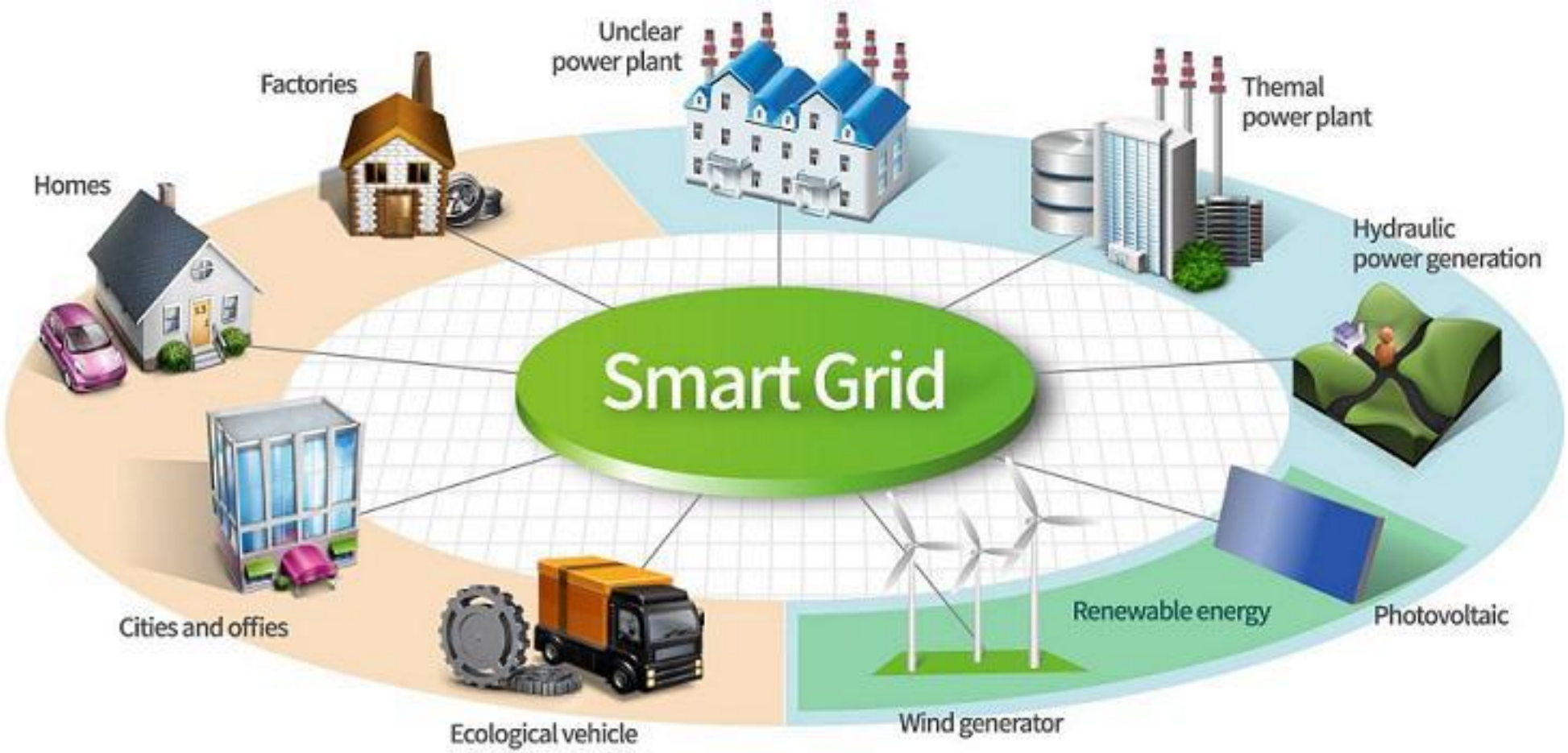


PURDUE ENTERPRISE REFERENCE ARCHITECTURE

- Level 0: Physical Process
- Level 1: Sensors and Actuators
- Level 2: PLCs and RTUs
- Level 3: SCADA and HMI
- Level 4: Enterprise IT Systems
- Level 5: Cloud and External Networks

INTRODUCTION TO ICS/SCADA SYSTEMS SECURITY

- **An example of ICS/SCADA** :
- Smart grid's field instruments are monitored and controlled remotely through ICS/SCADA control.
- The power's real-time data should be secured and available continuously to provide reliable and best power management . For that, smart grid should be well protected from such cyber attacks.
- Protecting such critical infrastructure is vital and challenging at the same time because a minimum downtime can cause many problems.
- Therefore, smart grid must carefully identify the security problems of ICS/SCADA systems, the possible attack vectors, evaluate and rank the different threats, and remediate the possible vulnerabilities.


Unclear
power plant
Factories
Themal
power plant
Homes
Hydraulic
power generation
Smart Grid
Cities and offies
Renewable energy
Photovoltaic
Ecological vehicle
Wind generator

ARCHITECTURE OF ICS/SCADA

A conceptual illustration of ICS/SCADA infrastructure has four main components, namely :

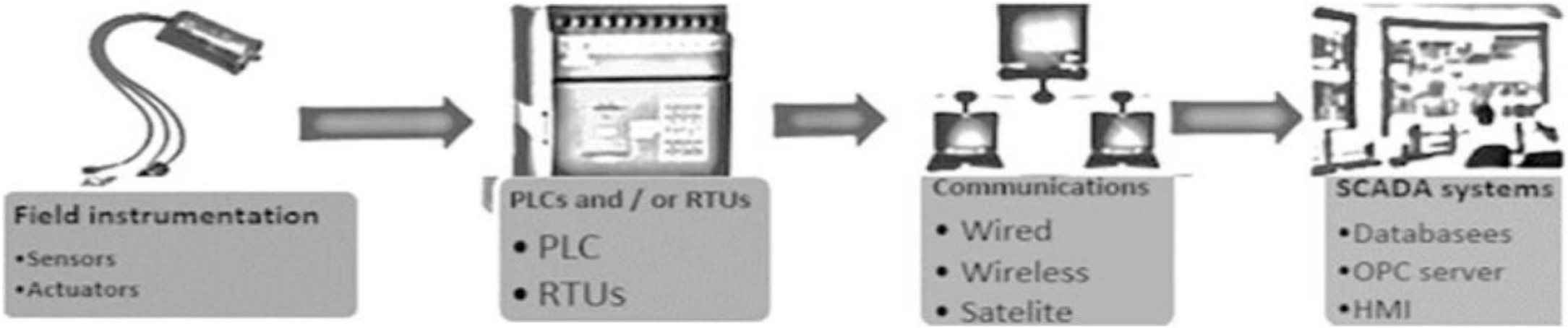


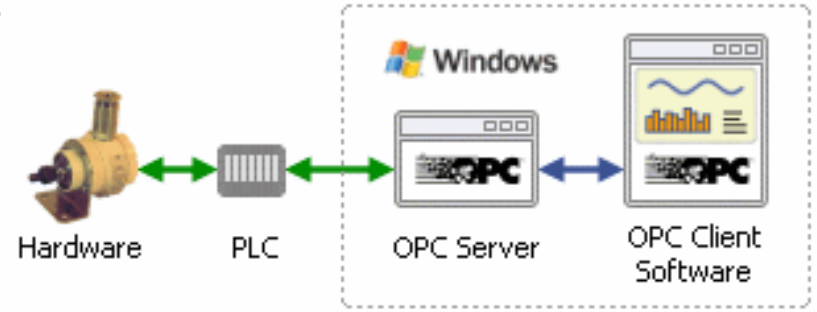
Fig. 5.1 Conceptual illustration of ICS/SCADA infrastructure developed

ARCHITECTURE OF ICS/SCADA

- **ICS/SCADA control center:** It consists of servers which include OPC and database, and the end user computers and HMI. OPC server is used as a software interface to allow Windows software to communicate with the industrial hardware instruments, like the concept of the object linking and embedding (OLE), but for process control.

OPC = OLE for Process Control

- **Communication networks :** They allow connectivity between SCADA control room, PLCs, RTUs, and the various field instruments. It can use numerous communication technologies and devices such as fiber, Ethernet, Wi-Fi, switch, routers, modems, satelli

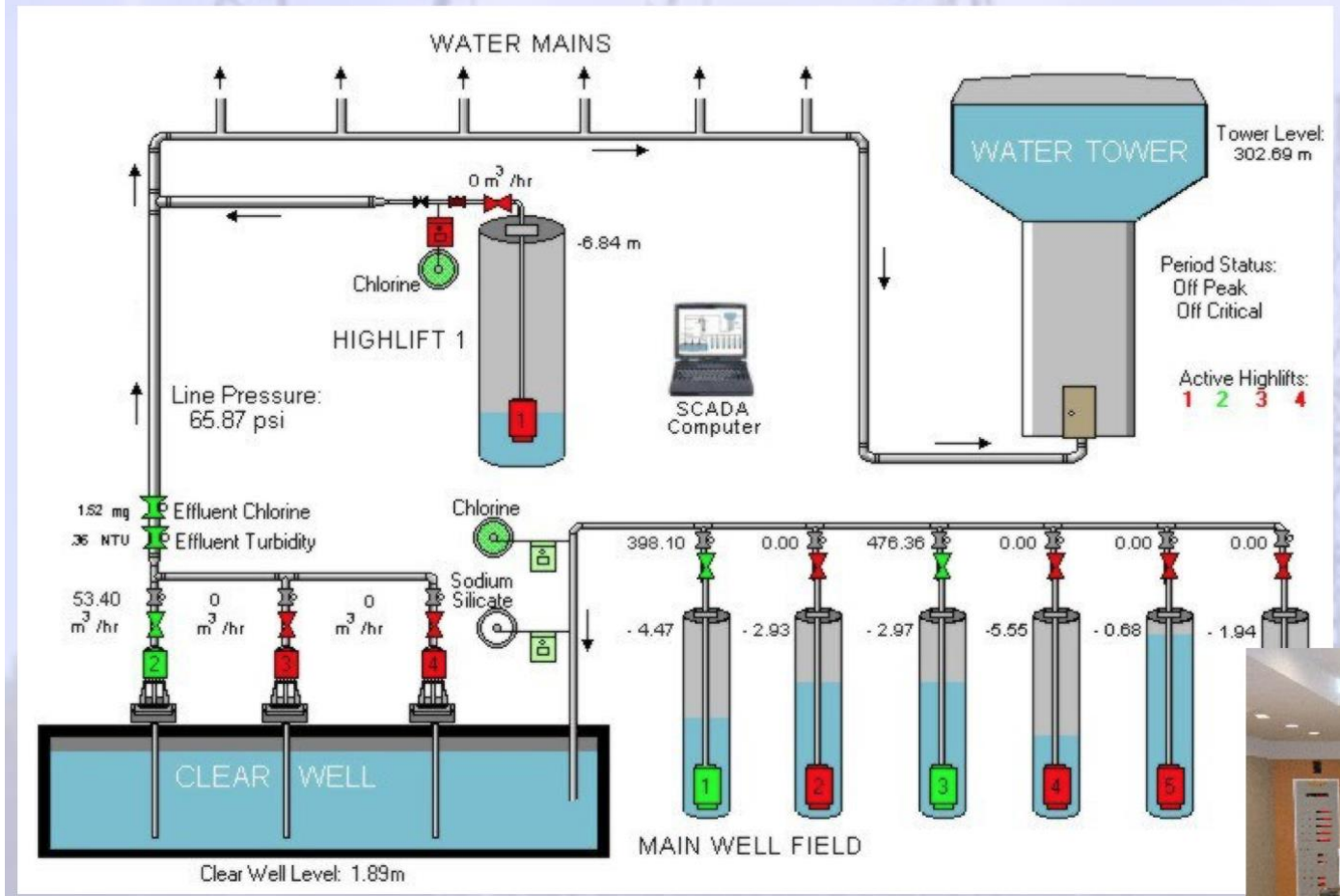


ARCHITECTURE OF ICS/SCADA

- **PLCs and/or RTUs:** PLCs are rugged specific industrial computers with predefined instructions stored in their memory to do certain tasks, and always observe the state of its connected input devices such as sensors, and act based upon custom programming codes to change the state of output devices such as actuators.
- PLCs have inputs/outputs to interact with field instruments such as sensors, actuators, valves, pumps, etc. and keep continuously observing the state of the various input devices and make logic-based decisions upon predefined custom instruction to control the state of output devices.
- Therefore, ICS/SCADA systems depend totally on PLCs to monitor and control the field instruments.
- **RTU** is a telemetry electronic device that connected to remote input devices such as sensors and receives input data from them and transfers it to the ICS/SCADA control room.
- **PLCs and RTUs** are becoming one of the **core technologies** used in smart grid environments.

ARCHITECTURE OF ICS/SCADA

- Master Terminal Unit (MTU): It is the heart of the SCADA system, which can be a dedicated computer, a Programmable Logic Controller (PLC), or a network server that communicates with remote field side RTUs. It initiates all communication, collects the data, stores the data in database, provides interfaces to operators and sends the information to other systems.
- It allows the users to perform controlling functions on field devices such as breakers, switches and other actuators depending on the gathered data. It continuously communicates with other devices in master station so as to facilitate data logging, alarm processing, trending and reporting, graphical interface and security system



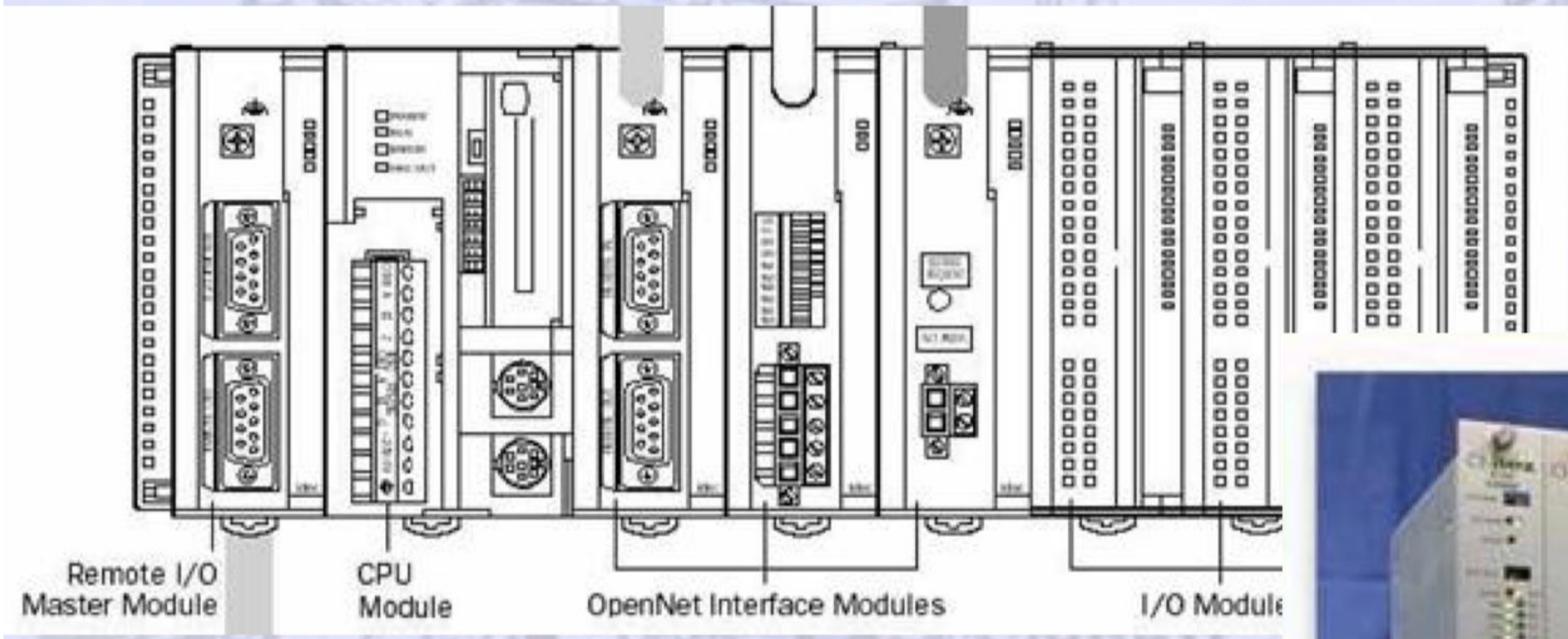
Water SCADA HMI

Korean control center

ARCHITECTURE OF ICS/SCADA

- Programmable Logic Controller (**PLCs) and/or** Remote Terminal Units (**RTUs)**: PLCs are rugged specific industrial computers with predefined instructions stored in their memory to do certain tasks, and always observe the state of its connected input devices such as sensors, and act based upon custom programming codes to change the state of output devices such as actuators.
- PLCs have inputs/outputs to interact with field instruments such as sensors, actuators, valves, pumps, etc. and keep continuously observing the state of the various input devices and make logic-based decisions upon predefined custom instruction to control the state of output devices.
- Therefore, ICS/SCADA systems depend totally on PLCs to monitor and control the field instruments.

Programmable Logic Controller (PLC)



Intelligent Electronic Device (IED)

Remote Terminal Units (RTUs):

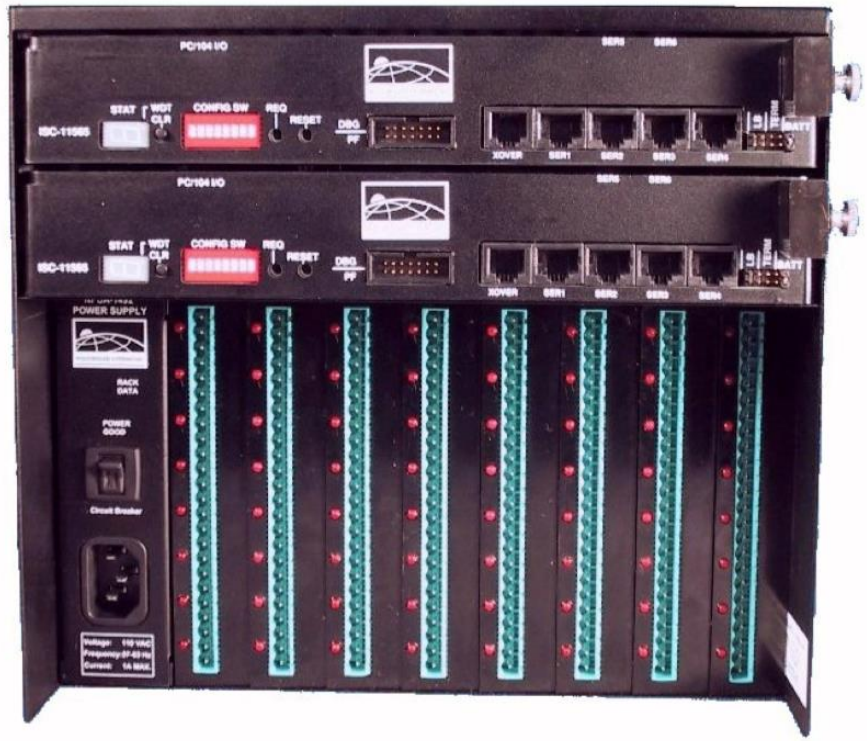
RTUs gathers the information from various field sites in which they are employed. Each RTU is connected with various sensors and actuators that manage local process or field equipment. It collects the information from various sensors and sends the information to the MTU. Also, it receives the control commands from MTU and correspondingly controls the various actuators.

Sample RTUs

Radio RTU

Cellular RTU

Serial RTU

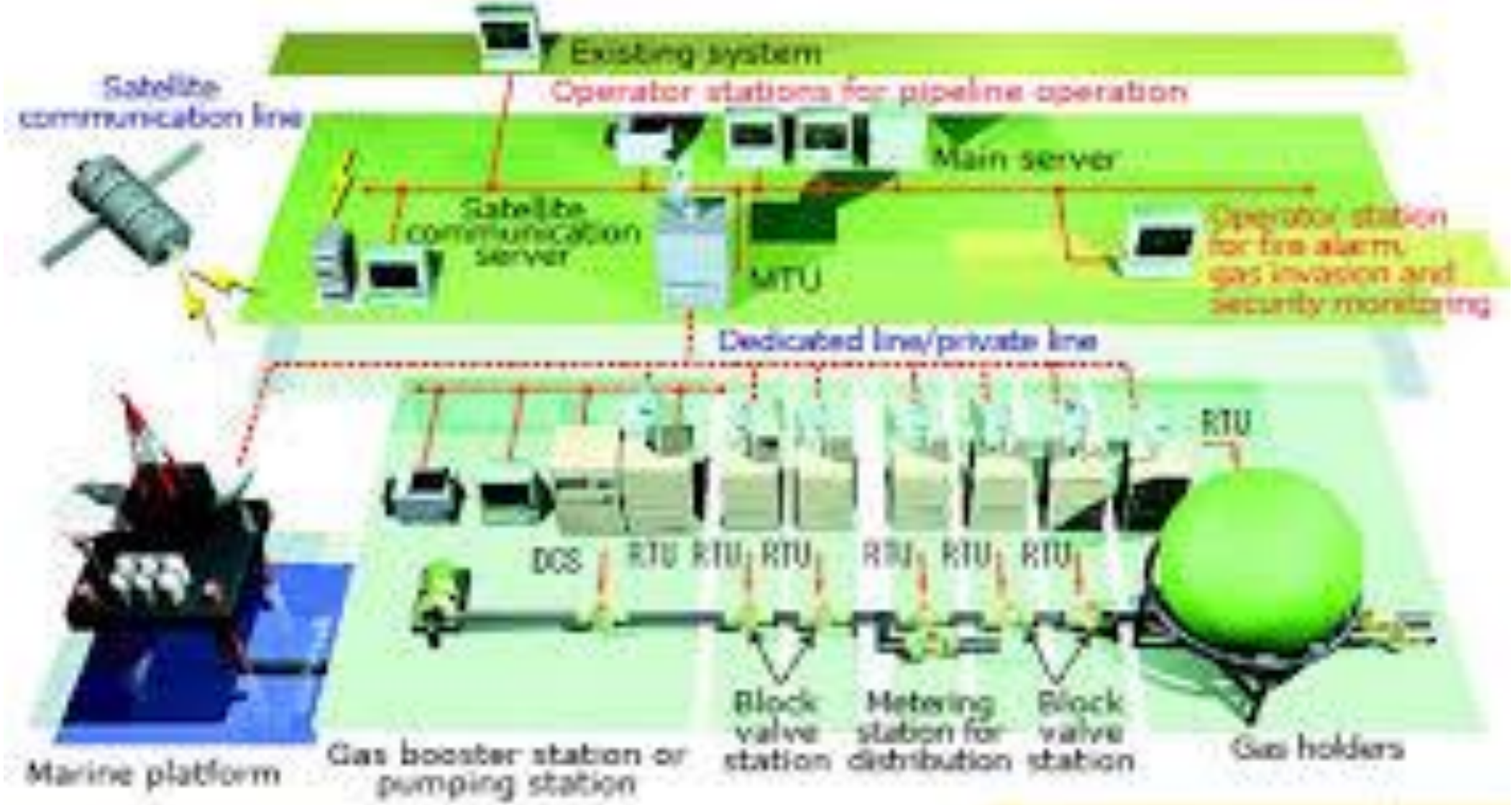


- Many RTUs store the data in their database and waits for a request from the MTU to send or transmit the data. In sophisticated systems, PLCs are used as RTUs which directly transfers the field data and controls the parameters without a request from the MTU. It uses a local area network to communication with various field intelligent devices.

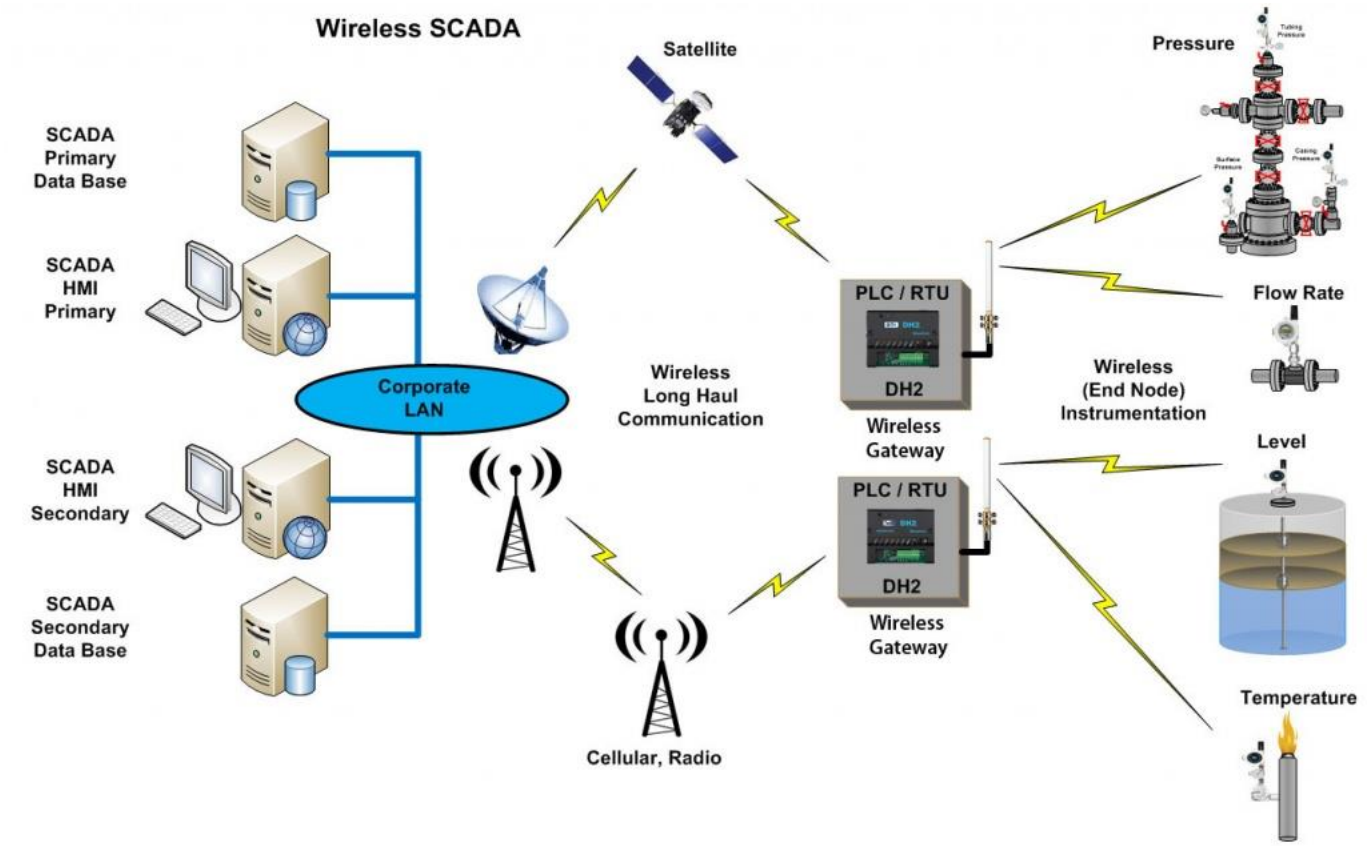

mobile phone
GSM MODEM
PLC
meter
Relay
monitor center
CWT5005
water pump
Temperatrue/Humidity
detector
Infrared
detector
Smoke
detector
Gas
detector

em
secu
rity

- Communication Equipment/Network: It provides the link between RTUs (in the field) to MTU (in the control center). The communication can be wired or wireless or through internet which provides bidirectional and uninterrupted communication between RTU and MTU.
- SCADA systems can be connected using various communication mediums including twisted pair cables, coaxial metal cables, fiber optic cables, satellites, high frequency radio, telephone lines, and microwave radio.
- The topology of the SCADA system network depends on the type of system or application it is intended for. **Mostly redundant topology is recommended for critical control applications.**


Existing system
Operator stations for pipeline operation
Satellite communication line
Main server
Satellite communication server
MTU
Operator station for fire alarm, gas invasion and security monitoring
Dedicated line/private line
RTU
DCS
RTU RTU RTU
RTU RTU RTU
Block valve station
Metering station for distribution
Block valve station
Gas holders
Marine platform
Gas booster station or pumping station
MTU: Master terminal unit
RTU: Remote terminal unit

ARCHITECTURE OF ICS/SCADA



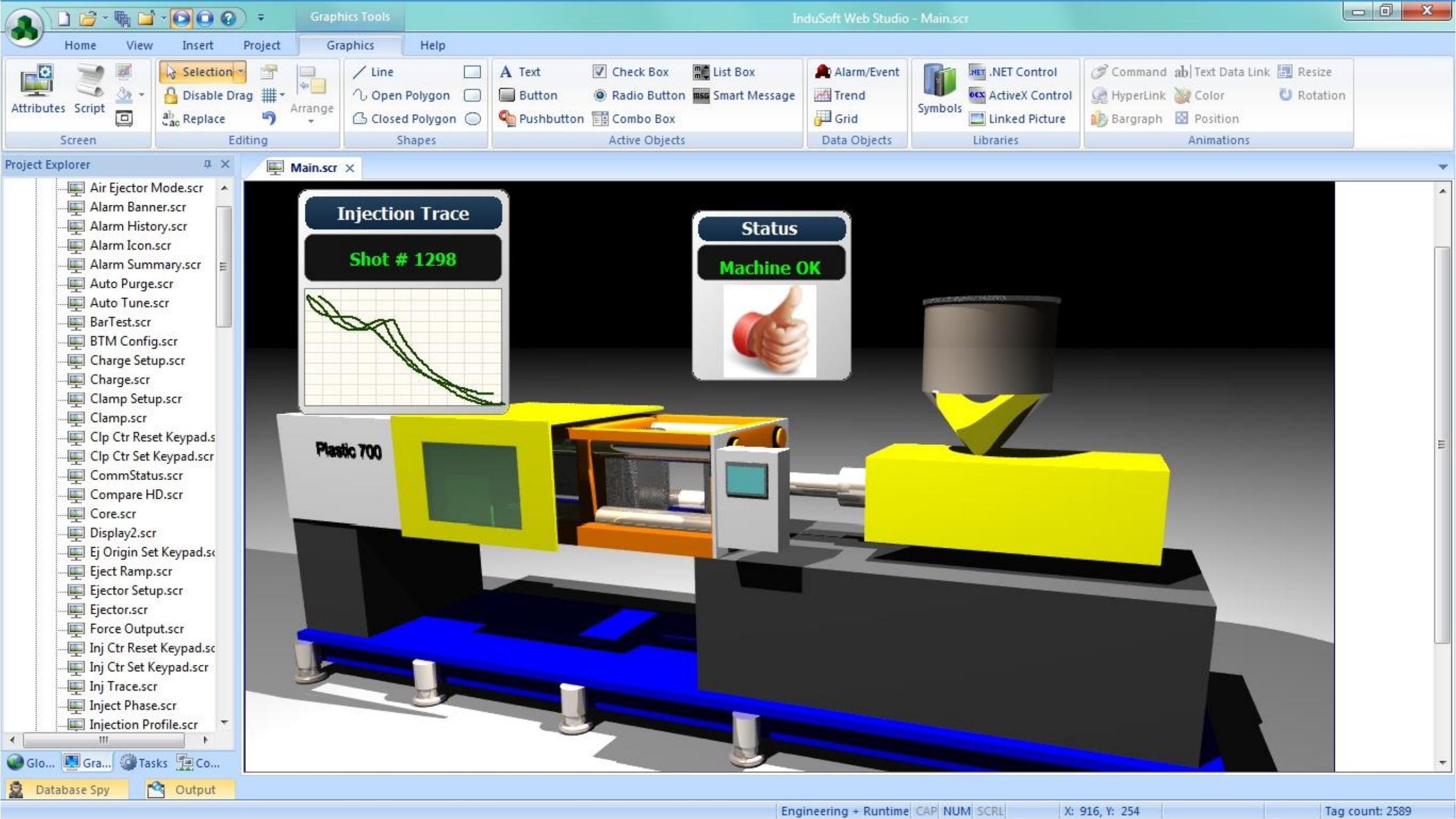
ARCHITECTURE OF ICS/SCADA

- **Field instruments** : consist of miscellaneous instruments and devices such as temperature sensor, pressure sensor, level sensor, flow meter, various valves, smart pumps, etc.

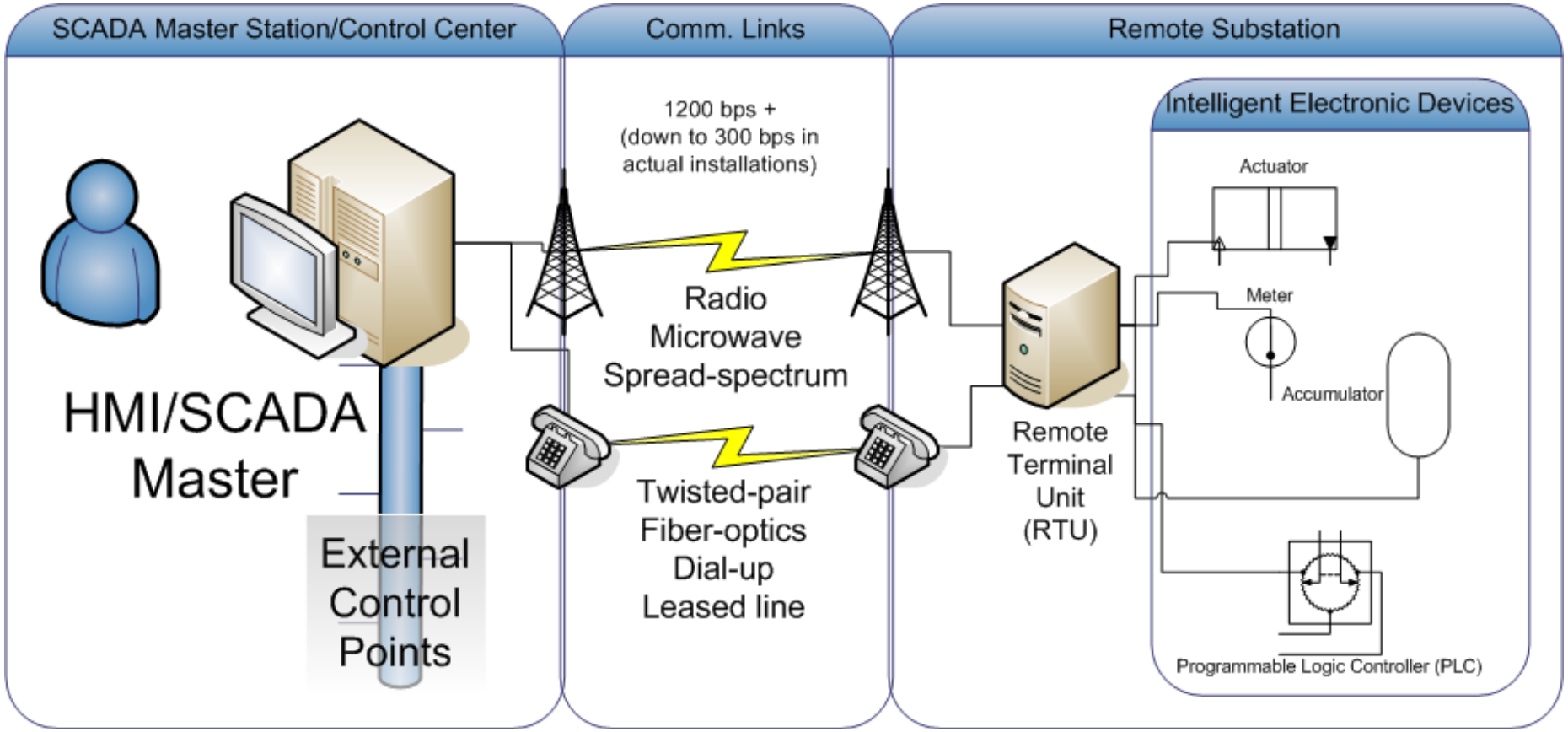
- **Sensors:** are small electronic devices that sense the surrounding physical quantities measurements such as voltage, temperature, pressure, speed, etc. These sensors send the collected physical data to the ICS/SCADA controlling servers for further analyzing and monitorir

- **Actuators:** are devices that are responsible for making action to the surrounding or to the attached environment's components, and the action might be mechanical or electronic. Also, these devices will act upon receiving controlled orders from the ICS/ SCADA control room. These instruments are critical analog input devices to the PLCs and modern RTUs to process the input data and make the logic-

- SCADA Software: It is an important aspect of every SCADA system which presents the information to the user and also allows the user to intervene in the process control. Many SCADA systems use commercial proprietary software upon which SCADA system is developed.
- This software comprises a computer operating system which controls the central host computer hardware, communication network management, graphical generation tool for HMI, database management and report generation tools.
- Other components or auxiliary equipment in central station includes HMI station, which gives graphical representation of field parameters, alarm generators to inform normal and abnormal conditions of process and recorders to produce a permanent record of analog and discrete variables


Graphics Tools
InduSoft Web Studio - Main.scr
Home
View
Insert
Project
Graphics
Help
Attributes
Script
Selection
Disable Drag
Replace
Arrange
Screen
Editing
Line
Open Polygon
Closed Polygon
Shapes
Text
Button
Pushbutton
Check Box
Radio Button
Combo Box
List Box
Smart Message
Active Objects
Alarm/Event
Trend
Grid
Data Objects
Symbols
.NET Control
ActiveX Control
Linked Picture
Libraries
Command
Text Data Link
Resize
HyperLink
Color
Rotation
Bargraph
Position
Animations
Project Explorer
Air Ejector Mode.scr
Alarm Banner.scr
Alarm History.scr
Alarm Icon.scr
Alarm Summary.scr
Auto Purge.scr
Auto Tune.scr
BarTest.scr
BTM Config.scr
Charge Setup.scr
Charge.scr
Clamp Setup.scr
Clamp.scr
Clp Ctr Reset Keypad.s
Clp Ctr Set Keypad.scr
CommStatus.scr
Compare HD.scr
Core.scr
Display2.scr
Ej Origin Set Keypad.sc
Eject Ramp.scr
Ejector Setup.scr
Ejector.scr
Force Output.scr
Inj Ctr Reset Keypad.sc
Inj Ctr Set Keypad.scr
Inj Trace.scr
Inject Phase.scr
Injection Profile.scr
Main.scr
Injection Trace
Shot # 1298
Status
Machine OK
Plastic 700
Glo...
Gra...
Tasks
Co...
Database Spy
Output
Engineering + Runtime
CAP
NUM
SCRL
X: 916, Y: 254
Tag count: 2589

ARCHITECTURE OF ICS/SCADA



ARCHITECTURE OF ICS/SCADA W.R.T SMART GRID

- ICS/SCADA architecture in smart grid is almost similar with some unique features.
- For instance, in the smart grid, the utility's substations send the most real-time electrical data status to SCADA control room via PLCs or/and RTUs.
- Also, the modern substations are occupied with intelligent electronic device (IED) such as electronic circuit breakers and power monitors which cooperate with PLCs/RTUs to transmit the collected data to the substation's computer which concurrently will be transferred to the main centralized SCADA system.

SCADA COMMUNICATION PROTOCOLS

- • There are multiple communication protocols used in SCADA or Industrial Control Systems (ICS). Unlike Ethernet or Internet Protocols (IP), the industrial control industry uses multiple protocols.
- ➢modbus (port 502)
- ➢dnp (port 19999)
- ➢dnp3 (port 20000)
- ➢fieldbus (port 1089-91)
- ➢ethernet/IP (port 2222)
- ➢etherCAT (port 34980)
- ➢profinet (port 34962-64)

Protocol	Security Level	Notes
Modbus	Low	No encryption or authentication
DNP3	Medium	Supports Secure Authentication
OPC UA	High	Encrypted and authenticated
IEC 61850	High	Used in smart grids

ICS/SCADA VULNERABILITIES

- Cyber-physical's embedded systems are the operation fundamental of the ICS/ SCADA systems which become more vulnerable to exploitation; therefore, they should be well-protected and secured.
- The vulnerability of the ICS/SCADA system is due to many factors such as:
  - the absence of real-time network scanning to detect suspicious activities,
  - identify the threats, and react accordingly,
  - the slowness for systematic and careful updating and patching, and
  - lack of knowledge about the specification and capabilities of the old and new devices.
  - Also, not having enough information about the network's traffic status is the core reason for the vulnerability because it stops the security specialists to know about any abnormal activities or potential threats to field instruments and ICS/ SCADA system.
  - Neglected, unskilled, and unsafe practices of authentication give chances to the attackers to gain access to these holes.

ATTACKING METHODS TOWARDS ICS/SCADA

- An attacker targeting the ICS/SCADA systems are not in one trial but through a bulkiness of efforts and methods to gather the most applicable and adequate information to create a great negative cause.
- The type and complexity of attacking methods that are used are determined by
  - how much the attacking purpose is vital,
  - what is the impact level must be achieved to satisfy these purposes, and
  - how much the ICS/SCADA system is secured. For instance, if an attacker has no harm objective, s/he might satisfy using DoS.
- However, s/he needs to go further to destruct the ICS/SCADA system by manipulating the operational process to achieve the ultimate damage and harms to the structure, equipment, data, and human. Then, a huge systematically attacking method will be used .

THREATS CATEGORIES FACING ICS/SCADA

The security of the ICS/SCADA operations is threatened by two main categories of intimidation including

1. Unintentional (inadvertent) **threats** are mainly originated from inside the premises, and the primary sources are the human, devices, or the surrounding nature.

- The **human factor** including the **employees, contractors, and/or business partners** can be a source of threats in the form of **neglect, carelessness, or lack of knowledge**, so s/he might produce a threat toward the ICS/SCADA system without awareness or intention to do that.
- the **machine's failure, devices safety weakness, and equipment crashing** are a great source of threats to the ICS/SCADA security .
- the natural disasters such as **avalanches and landslides, earthquakes, sinkholes, volcanic eruptions, floods, tsunami, and blizzards** can cause disruption to the ICS/SCADA security.

2. Purposeful threats : The ICS/SCADA system can be targeted by the meaning of purposeful attacks by annoyed employees, industrial espionage, sabotage, cyber hackers, viruses and worms, physical theft, and electronic terrorism.

LETS WATCH THIS…

https://www.youtube.com/watch?v=NBc_KXTtlK4

https://www.youtube.com/watch?v=LmMxiZztxpY

https://www.youtube.com/watch?v=6cwK9PZC23Y

THE CHALLENGES TO PROTECT ICS/SCADA

There are many security challenges facing the professionals to protect the ICS/ SCADA systems such as:

- The old and basic architecture designs in which the security matter is not considered.
- The message are still transmitted internally and between remote connections using clear text form without adopting any encryption technologies.
- There are many applications and servers' operating systems and applications that have no regular patching scheme, even some firmware not updated at all.
- Another challenge is to secure the remote communication of the ICS/SCADA components which are geographically scattered such as sensors, actuators, RTUs, and PLC.

- In addition, there are several management, operational, and technical challenges to secure the ICS/SCADA systems, such as:

  - vulnerability tracking problem,
  - standardization of devices and systems,
  - downtime for maintenance,
  - unsupported OS and applications,
  - exposed to operational technology (OT) network to public networks,
  - unable to pen-test in production real time,
  - limited time for remediation once incidents occur,
  - share accounts or no authentication within users, and
  - secure the connection between information technology (IT) and OT.

ICS/SCADA SECURITY OBJECTIVES

There are many objectives to protect the ICS/SCADA architectures such as

- keeping the ICS/SCADA systems **functioning as much as possible** during the most difficult conditions.

➢ This involves creating a redundancy for the most ICS/SCADA critical devices such as historian servers, switches, modems, and the field instrumentations.

➢ Also, during a failure, the device should not cause unnecessary traffic on the ICS/ SCADA networks or cause extra trouble elsewhere.

ICS/SCADA SECURITY OBJECTIVES

- ICS/SCADA system should be designed to allow for **systematic degradation** such as transferring from "**normal condition**" with full automation to "**emergency condition**" with operators interfere making less automation to "**full manual status**" with no automation at all.
- Another protection objective is to provide a systematic and practical way to detect the various security events and incidents.
- For instance, security specialists can safeguard the operations of ICS/SCADA if they can detect early the failure of devices, services exhausted resources such as memory, processing, and bandwidth that are being used

ICS/SCADA SECURITY OBJECTIVES

The three traditional security objectives for securing the ICS/ SCADA systems are:

- **Availability** is on top of security objectives priority list which is focusing on keeping ICS/SCADA systems services offered continuously 24/7 when monitoring and controlling critical infrastructure or life-safety systems.
- **Integrity** comes the second order in the list by the ability to offer the operators/controllers the confident needed to fully trust the integrity of the various physical information that is received and to take the most suitable actions based on reading feedback or status from the various instruments and devices.
- **Confidentiality** is not as important as the availability and integrity because the received physical information from sensors, PLCs and RTUs, are used and the transmitted is state-based and only valid for that specific time; then, it will be discarded after processing and storing them in the historian servers.

ICS/SCADA SECURITY REQUIREMENTS

- **Importance of Security Countermeasures:**

➢Security requirements (countermeasures) are an **action, device, procedures, or techniques that reduce a threat, vulnerability, or an attack.**

➢These requirements are aimed to eliminate or prevent the threat by decreasing the negative impacts automatically or by discovering and reporting it so that corrective solutions can be taken by the IT specialists or the operators.

ICS/SCADA SECURITY REQUIREMENTS

- Protecting the field instruments (e.g., **sensors, actuators, PLC, and RTU**) is the main security concern for securing the operations of the ICS/SCADA system.
- This protection starts from selecting the right device with **compliance** to the latest security standards.
- Security of field instrument should go throughout its life cycle: **procurement, installation, monitoring, and maintenance.**
- Field instruments should have met the core security requirements such as the **authentication, authorization, and CIA**
- Physical security countermeasures for field instruments should start from providing the applicable secure fences and gates which must be accessed through the combination of traditional hardware and electronic locks.
- A motion detector linked with closed circuit television (CCTV) is recommended to record and discover any intruder to the remote stations.

ICS/SCADA SECURITY REQUIREMENTS

- ICS/SCADA control room's servers and hosts must be well protected from the logical and physical attacks.
- Moreover, to provide the optimum availability the redundancy and high-capacity links between the servers must be established.
- It is also recommended establishing load balancing and failover mechanisms between ICS/ SCADA servers and network components, such as switches/routers.
- ICS/SCADA servers should receive the appropriate configuration/patch management and secure importation and execution of only trusted patches which will help to secure the ICS/SCADA servers.

- **Security countermeasures at servers:**

  - strong multifactor authentication,
  - application whitelisting,
  - securing the hosts physically, and logically through adopting and implementing solid access controls using different tools, policies, and protocols to develop the most secure identification, authentication, authorization, and accountability mechanisms.

ICS/SCADA SECURITY REQUIREMENTS

Electronic and Physical Security Perimeter:

- These security perimeters must be able to identify and control the people's access that enters and exit the ICS/SCADA facility, specifically the restricted areas. The electronic perimeters must be able to efficiently track the most current location, movements, and activities of the ICS/SCADA building occupant and assets, particularly in the event of any incident that might occur and must be able to respond quickly and raise alarms in real time whenever it is required.

ICS/SCADA SECURITY REQUIREMENTS

- This unified security package should consist of video surveillance, access control, and perimeter detection tools that are tightly integrated with alarms and events raised in process and safety systems for intelligent, and a coordinated responses mechanism.
- The unified tool also should occupy with the human—machine interface (HMI) which give common look and feel results. The HMI is enhancing the decision-making because both ICS/SCADA control room consoles and security office desktops have visibility of the real-time events and lead to faster responds and feedbacks.
- Adopting Mantrap technique (see next slide)


Upon authorized credential, the door opens. Overhead system scans the compartment to ensure single access.

ICS/SCADA SECURITY REQUIREMENTS

- **Network Communication Security**: ICS/SCADA servers and network components work together to manage all communications, evaluate and examine the received data, and show the alerts and events on the HMI workstations.
- communication technologies include wired such as fiber optics, power line communication, copper-wire line, and wireless such as GSM/GPRS/WiMax/WLAN and Cognitive Radio.
- However, one of these communication technologies could represent a potential threat to the ICS/SCADA system

ICS/SCADA SECURITY REQUIREMENTS

- **Example**: using old remote connection technology such as leased-line and dial-up modems for ICS/ SCADA remote communication with distant field devices will facilitate the attacking efforts into the critical networks.
- These old communication technologies mostly have got no or weak authentication and encryption which can be utilized by attackers to gain access to the ICS/SCADA network.
- For example, an attacker can access to the old technology modem which is connected to the smart grid's breakers, disrupting the altering the control configuration settings causing power outages and damages various electrical equipment.

ICS/SCADA SECURITY REQUIREMENTS

- It is important to utilize network security monitoring (NSM), NDR (Network Detection & Response) and security information event management (SIEM)

- NSM is a mean of gathering, analyzing, and rising the right indications or warnings to detect and respond to intrusions attacks .

- NDR uses passive, behavior-based network monitoring to detect abnormal and malicious activity in SCADA and IT networks in real time, without impacting operations.

- SIEM system is similar to NSM in providing a real-time analysis and performing data aggregation, association, alerting, dashboards, compliance, maintenance, and forensics investigation

ICS/SCADA SECURITY REQUIREMENTS

- **Product, Software, and Hardening**:

➢ The ICS/SCADA infrastructure occupies a wide range of IT products and software, which should be evaluated and certificated to ensure the quality and to ensure that they are per the standing security standards.

➢ These IT-related products and software should be updated, stable versions, tested, verified, and patched regularly to solid the security of the OT operational requirements.

➢ Hardening of ICS/SCADA system involves eliminating idle, needless, or unknown components such as modules, services, or ports. The most important in system hardening is selecting and implementing the most secure configuration parameters, as well as installing the security patches.

ICS/SCADA SECURITY POLICIES

- The objective of ICS/SCADA security policy is to provide management direction and support security professionals in an alignment of the business requirements and relevant laws and regulations.
- The security policy document should include the individuals who are responsible for the implementing and managing the policy terms, and they should be identified by their names, position details, and the contacts information.
- Furthermore, the security policy should be systematically reviewed and updated to ensure its continuing suitability, adequacy, and effectiveness

ICS/SCADA SECURITY POLICIES

- ISO27001 Standard recommended several security policies such as: Clear Desk and Clear Screen Policy,
- Access Control Policy,
- Disposal of Information/Media/ Equipment Policy,
- Data Classification and Control Policy,
- Mobile Computing and Teleworking Policy,
- Password policy,
- Penetration Testing Policy,
- System/Data Backup and Recovery Policy,
- Physical Security Policy,
- System Usage Monitoring Policy,
- Third Party Access Policy, and
- Virus /Malware Policy.

AI-ENABLED SCADA

- AI-enhanced SCADA combines traditional monitoring and control capabilities with advanced analytics, enabling systems to learn from data, predict events, and automate decision-making.

Feature	Traditional SCADA	AI-Integrated SCADA
Monitoring	Reactive	Predictive and proactive
Maintenance	Scheduled or manual	Predictive maintenance
Decision-Making	Human-driven	AI-assisted or automated
Anomaly Detection	Rule-based	Machine learning-based
Data Analysis	Historical reports	Real-time intelligent insights
Security	Signature-based detection	AI-driven threat detection

GOVERNANCE AND COMPLIANCE

- Governance of the ICS/SCADA Environment
- Regulatory Compliance and Standard Requirements
- The Planning Phase to Protect ICS/SCADA

GOVERNANCE AND COMPLIANCE

- **Governance of the ICS/SCADA Environment:**

- Implementing the ICS/SCADA systems without proper planning processes with a poor risk management study, weak security countermeasures, and inappropriate access control, will lead to ICS/SCADA security program with unsuitable governance.

- One of the ICS/SCADA challenges is governance of OT (ICS/SCADA) security and IT security that are typically managed by different professionals.

- The **OT devices** are managed by the **controlling, operating, engineering, or automation department**, at the same time as the **IT components are maintained by the IT department**.

- Moreover, without good coordination, there is often a doubt about which department is responsible for the security of **ICS/SCADA infrastructure** which might lead to serious gaps in the organization's security competencies.

GOVERNANCE AND COMPLIANCE

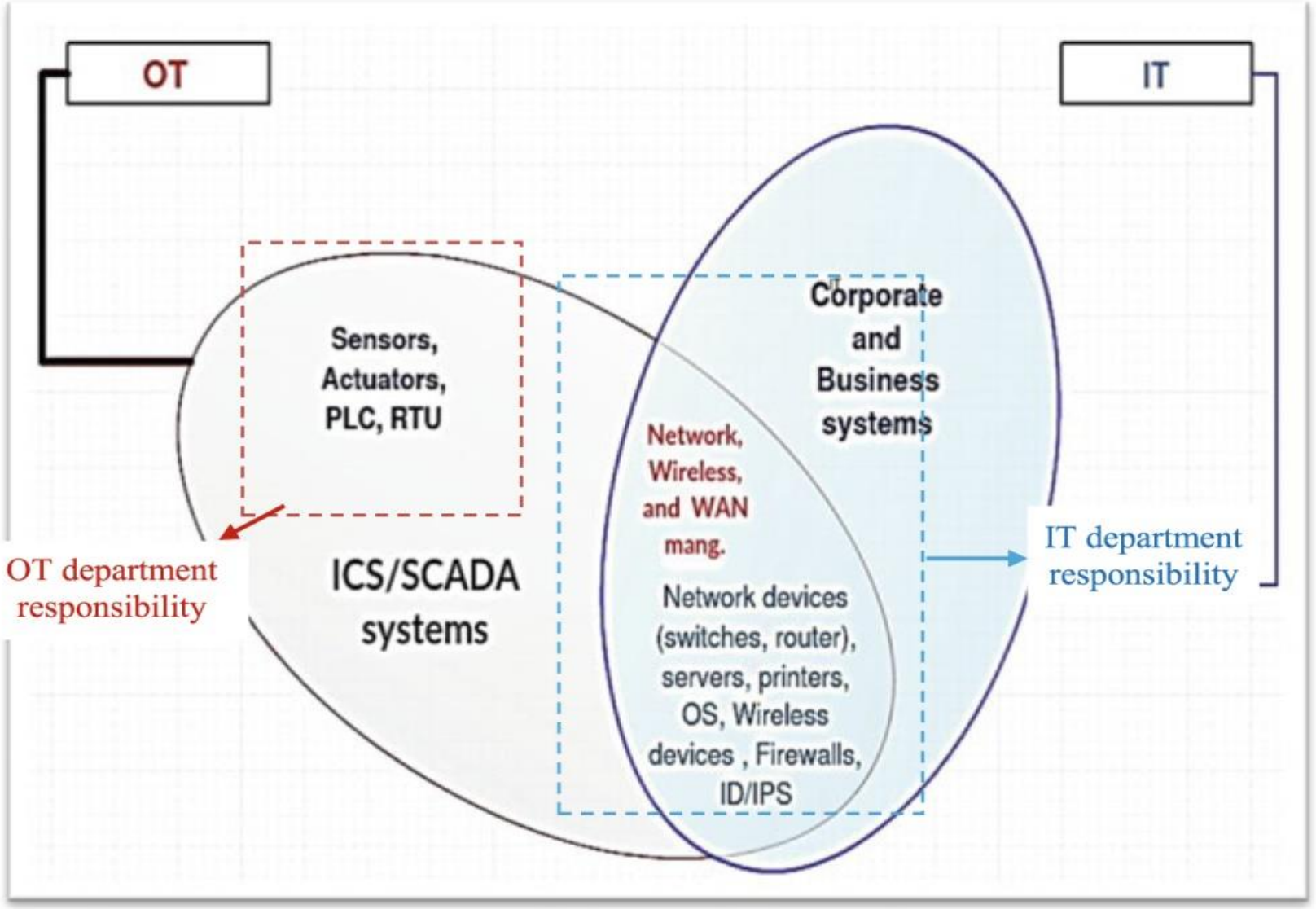


Fig. 5.2 Responsibilities of IT and OT to maintain and manage the corporate and ICS/SCADA networks

GOVERNANCE AND COMPLIANCE

- **Importance of Governance of the ICS/SCADA Environment:**

- Integrating well-known **security standards, best practices, frameworks, and guidelines** will give good guidance to develop a satisfactory governance structure for the security of ICS/SCADA infrastructure.

- The developed **governance policy** will help the decision-makers to make a better view of the ICS/ SCADA possible **threats**. It leads to know how to **mitigate** them, **enhance** the stakeholder's internal communications and **resources optimization**, and **clear the roles** and responsibilities for the OT and IT

- Official governance for the management of ICS/SCADA security will help to ensure that stakeholders and departments follow a steady and appropriate security strategy.

- Besides, the governance delivers clear roles and responsibilities, latest and up-to-date approaches to manage ICS/SCADA security threats, and guarantee that the supportive standards, guidelines, and policies are appropriate and are being implemented and followed.

GOVERNANCE AND COMPLIANCE

- **Regulatory Compliance and Standard Requirements:**

- Several standardization bodies and governmental agencies have developed various standards, guidelines, and policies to protect ICS/SCADA systems
- DHS catalog of control systems security, which was developed by Homeland Security of USA (2011).
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards 002-009 and National Institute of Standards and Technology (NIST) Special Publication 800-82 have good guidance to ICS/SCADA security (NIST 2011).
- Also, NIST organization has developed the "NISTIR 7628 Guidelines for Smart Grid Cyber Security.

GOVERNANCE AND COMPLIANCE

- The Planning Phase to Protect ICS/SCADA:

  Preparing a comprehensive security program to secure the ICS/SCADA system is not an easy task because it involves so many procedures and steps

  A suggestion of seven phases to develop a new security plan for the ICS/SCADA system given as follows:

  ① Assessing the existing systems,

  ② Documenting the policies and procedures,

  ③ Training the employees and contractors,

  ④ Segmenting the ICS/SCADA system network and security,

  ⑤ Controlling the access to the ICS/SCADA system,

  ⑥ Hardening the components of the ICS/SCADA system,

  ⑦ Monitoring and maintaining the security of ICS/SCADA system

REFERENCES:

- Cyber-security of SCADA and Other Industrial Control Systems

https://www.springer.com/gp/book/9783319321233

- National Institute of Standards and Technology (NIST) framework for cyber security for SCADA

https://www.pcvuesolutions.com/index.php/featured-articles/567-national-institute-of-standards-and-technology-nist-framework-for-cyber-security-for-scada

- Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector

https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf

- Security and Privacy in Smart Grids

https://www.taylorfrancis.com/books/e/9781439877845/chapters/10.1201/b15240-14