UTeM

اونيۏرسيتي تيكنيكل مليسيا ملاک

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Chapter 12

Always A Pioneer, Always Ahead

Protecting Critical Infrastructure: Process Control and SCADA

Dr Zaheera Zainal Abidin

zaheera@utem.edu.my

MyUTeM

OVERVIEW

- Introduction to SCADA System
- Generation of SCADA system
- Components of SCADA System: MTUs and HMI, RTUs, Programmable Logic Controllers, Flow Computers and Modbus.
- Technology background: Process control system
- Threats and challenge

INTRODUCTION

INTRODUCTION

- Commonly referred as Supervisory Control and Data Acquisition (SCADA).
- Examines process control and SCADA systems and challenges.
- Supervisory Control and Data Acquisition system helps in managing this complex industrial procedure by maintaining efficiency, encouraging smarter decisions through data processing techniques and communication of system issues to mitigate downtime.

SCADA SYSTEM

INTRODUCTION - 1

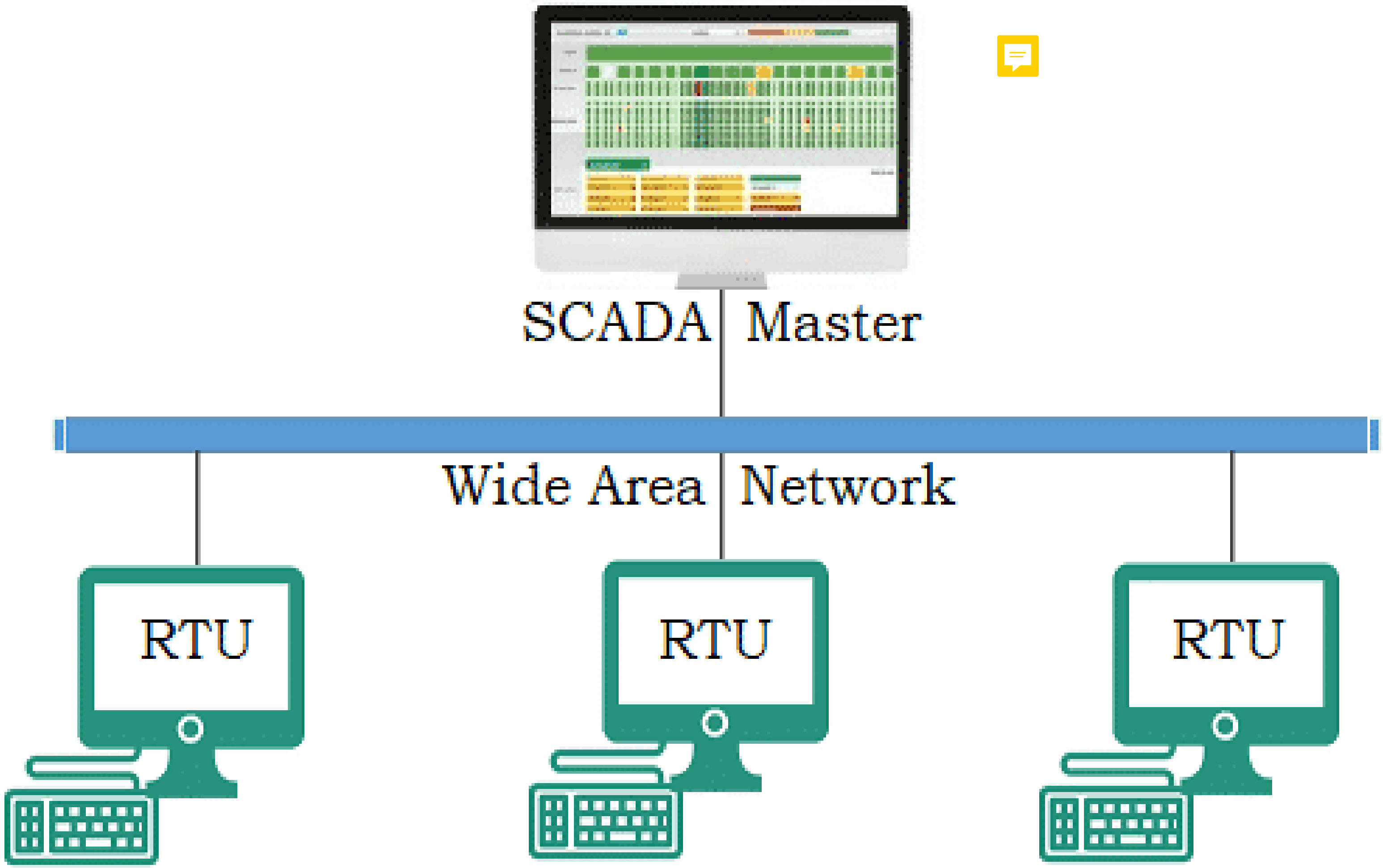
- SCADA system combines both hardware and software components. SCADA hardware includes MTU (master terminal unit) which is placed in a central location, communication equipment such as telephone line, radio, cable, or satellite, and one or more RTUs (remote terminal units) or PLCs which are placed at geographically distributed field sites.
- These RTUs or PLCs are connected with various sensors and actuators and are responsible for gathering the data and controlling the field parameters. The Master Terminal Unit (MTU) collects and processes the data from RTU or PLC inputs and outputs, while the PLC or RTU controls field devices or a local process.

INTRODUCTION - 2

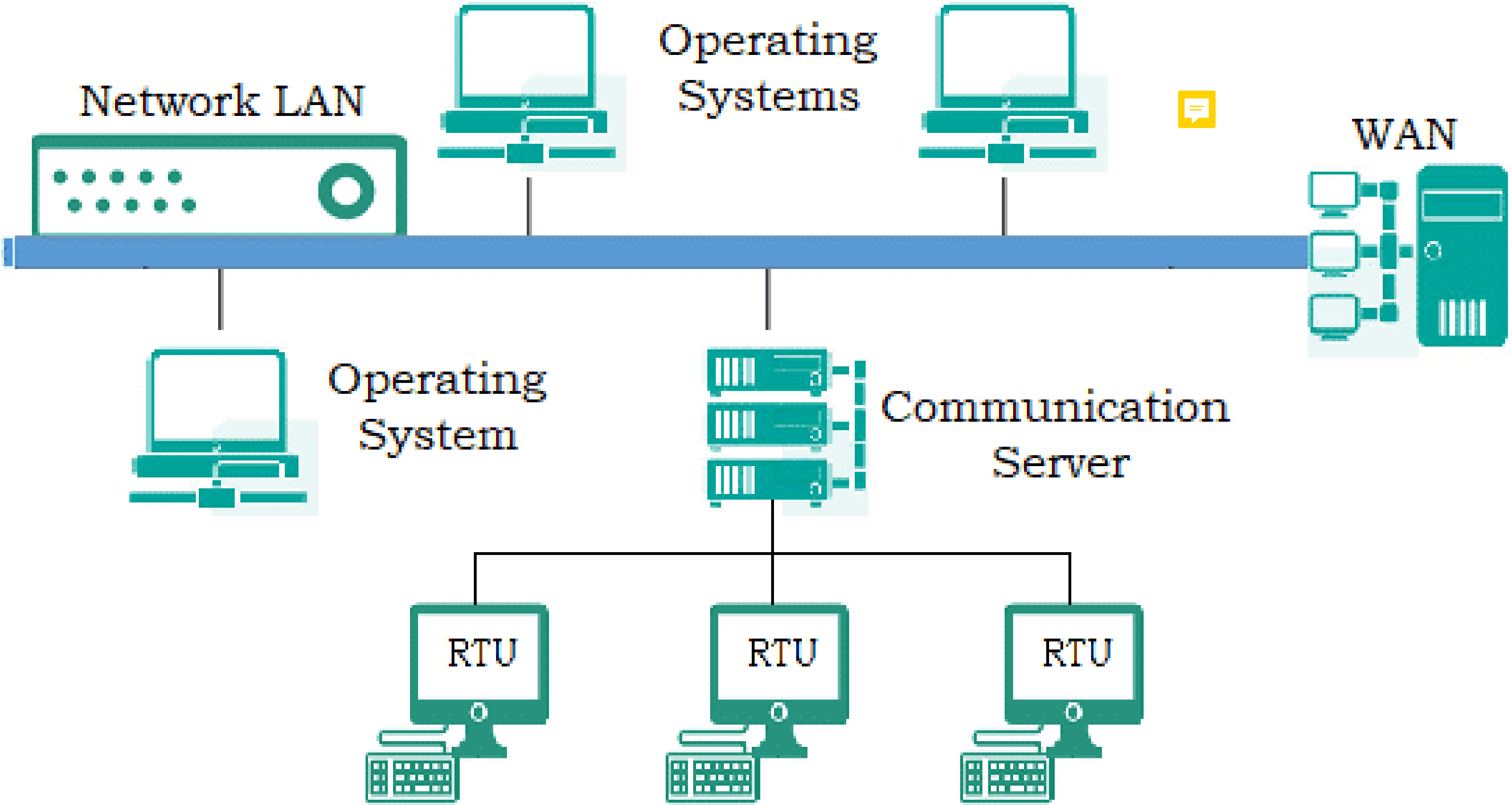
- Designed to enable the monitoring and control of processing systems that may be thousands of miles away from the controller.
- SCADA software performs the functionalities of a SCADA such as what and when to acquire and control, storing and accessing of acquired data, calculating parameters acceptable range (set limit checking), responding to parameter violations (beyond the range), providing HMI, reporting and accounting, generating alarms, etc.
- There are different SCADA vendors, some of those include Siemens, ABB, Honeywell, Rockwell, Schneider Electric, Technomatix and Tibbo Systems.

GENERATIONS OF SCADA

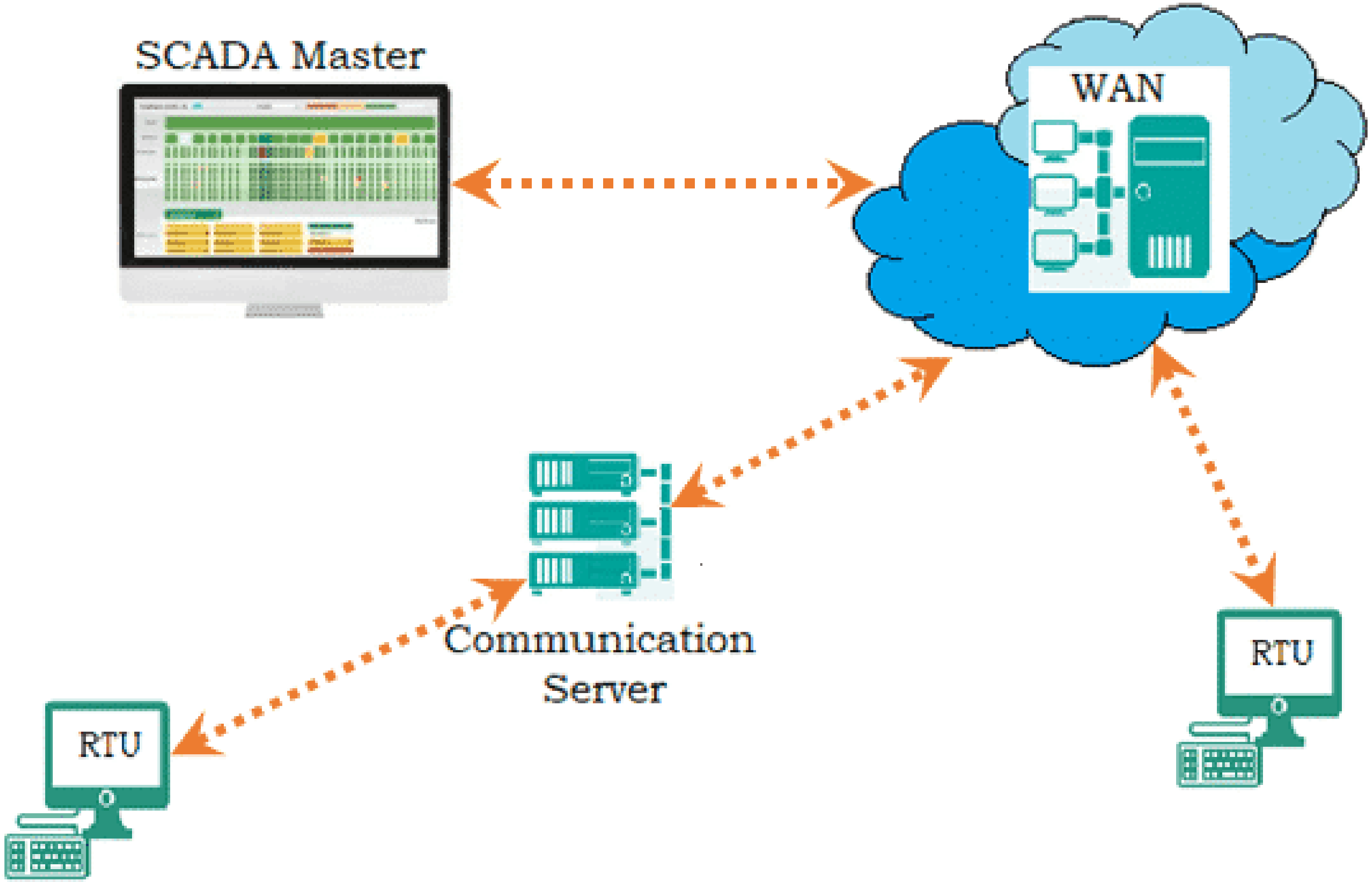
FIRST GENERATION – MONOLITHIC



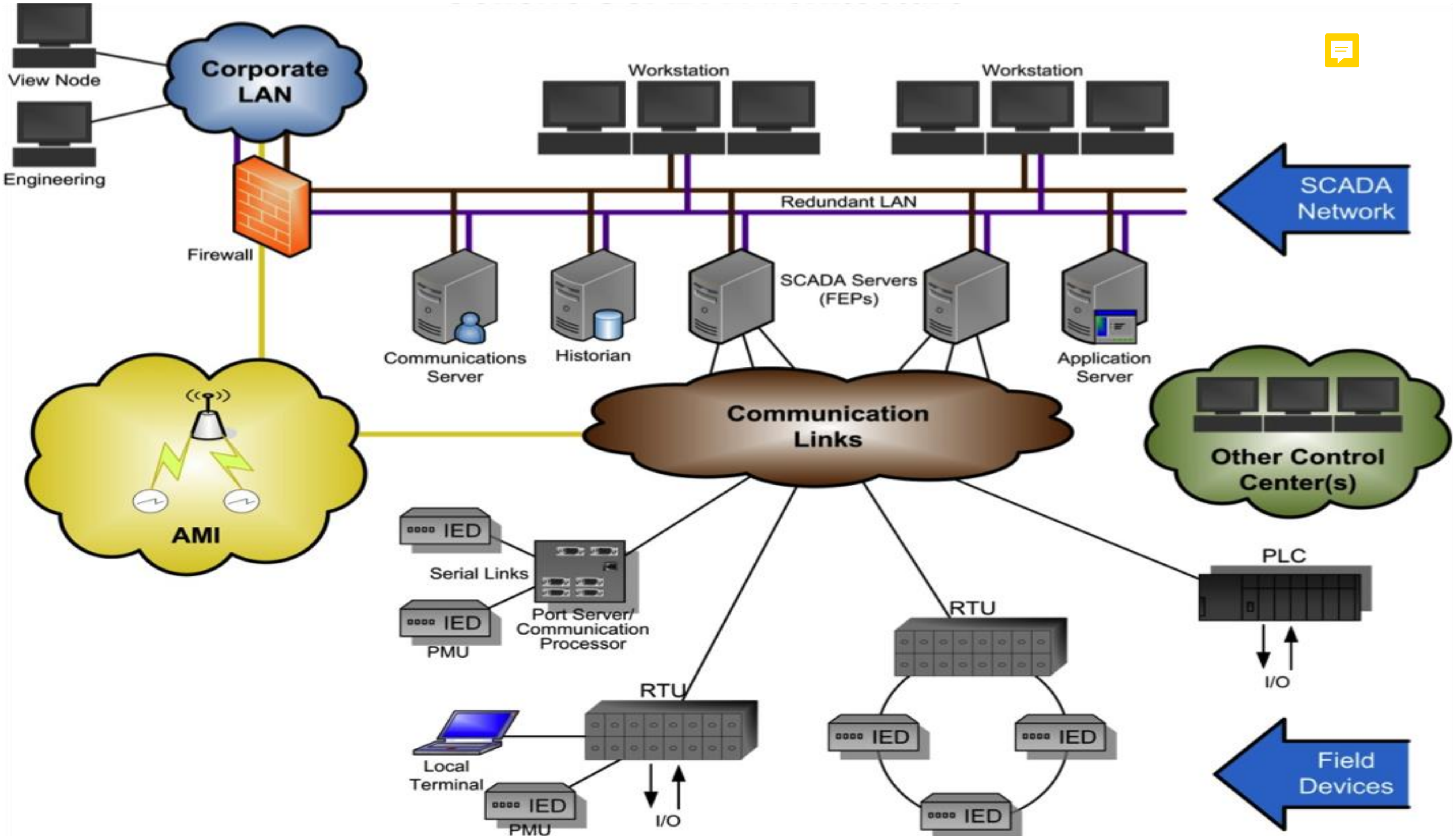
SECOND GENERATION – DISTRIBUTED



THIRD GENERATION – NETWORKED

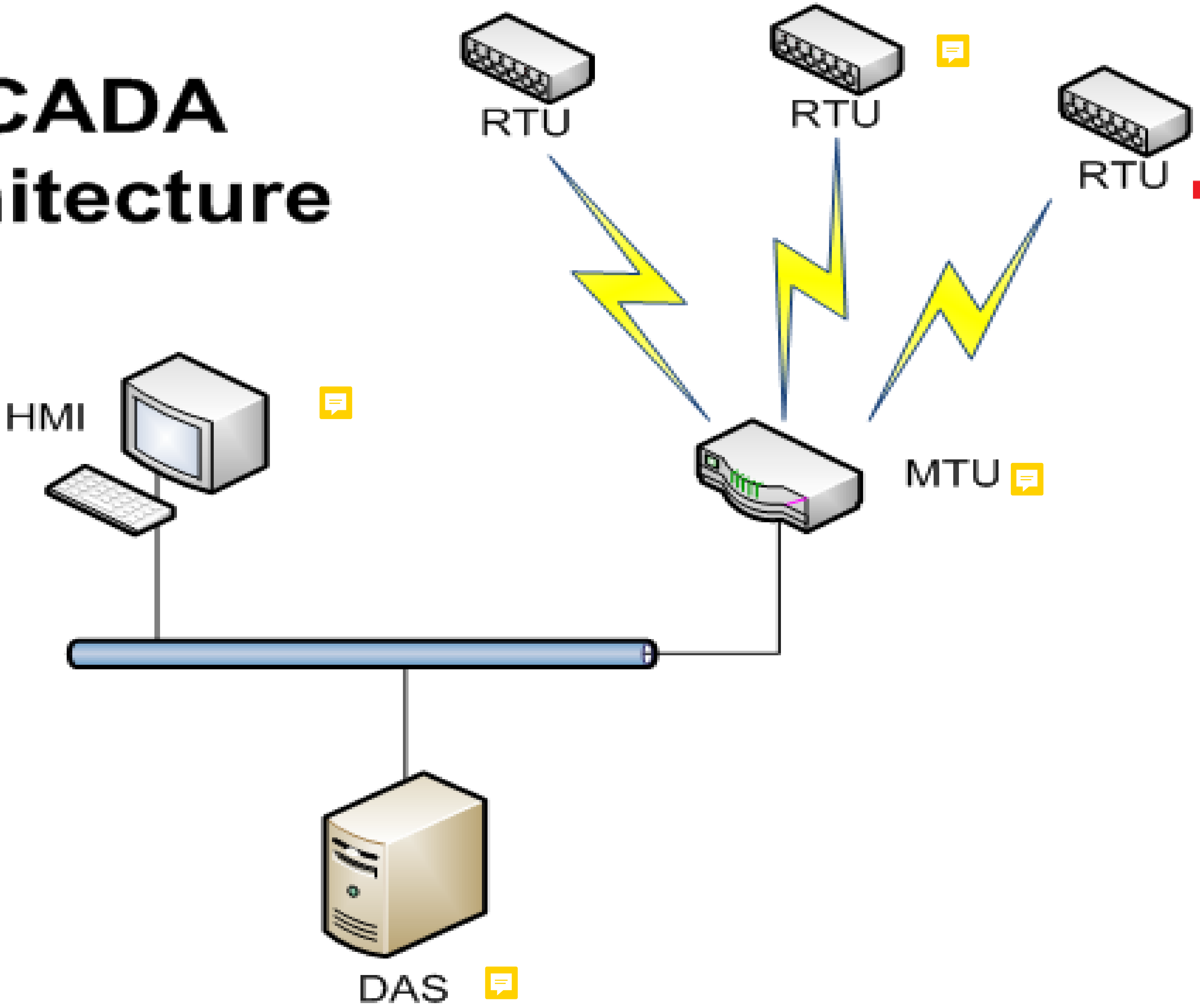


FOURTH GENERATION – IoT

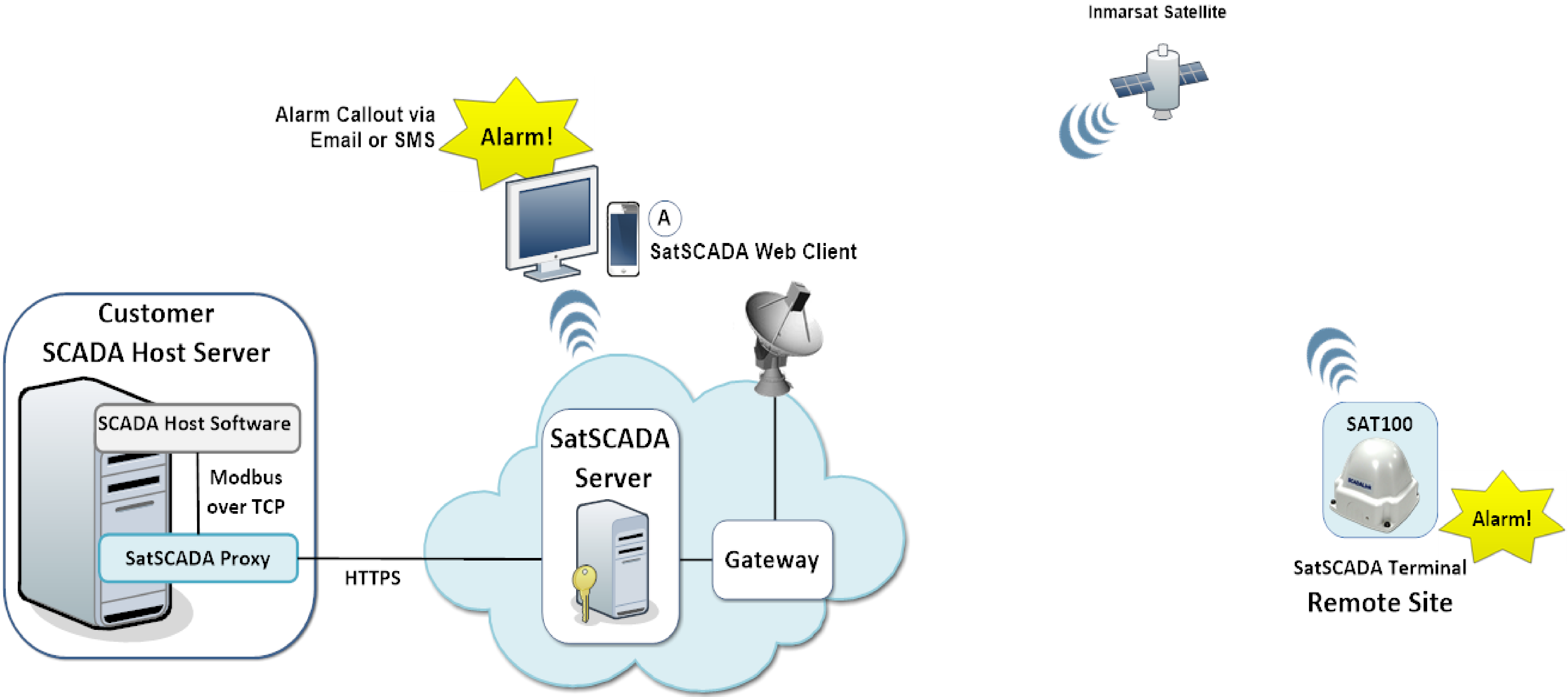


COMPONENT OF SCADA SYSTEM

SCADA Architecture



Satellite based SCADA



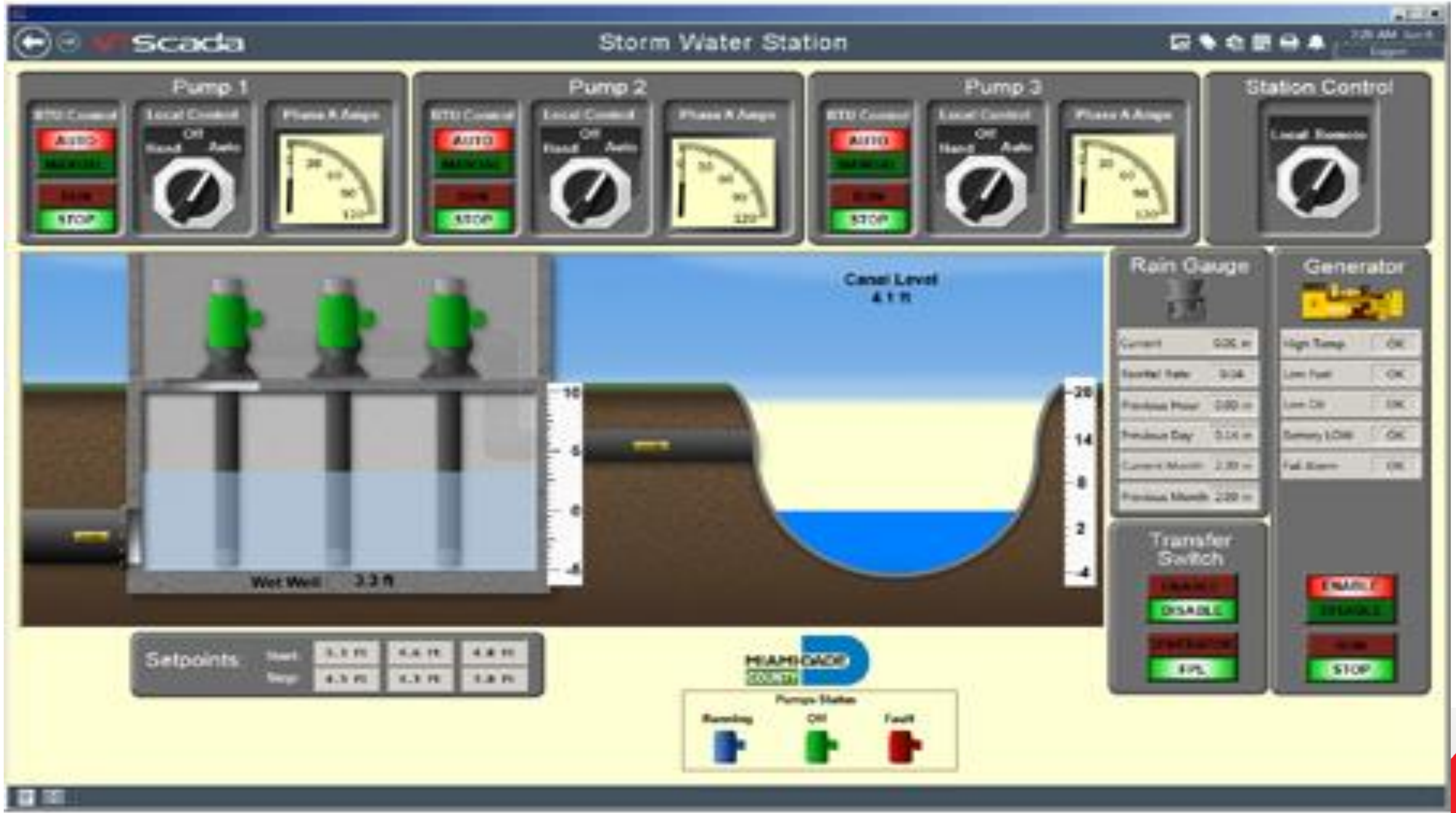
MTU – Master Terminal Unit

MTU

- MTU initiates communication with remote units and interfaces with the DAS and the HMI.
- Interface where the operator logs on to monitor the variables of the system.
- MTU is the heart of the SCADA system which is located at the operator’s central control facility.

MTU and HMI

Single point of human interaction for the entire operation

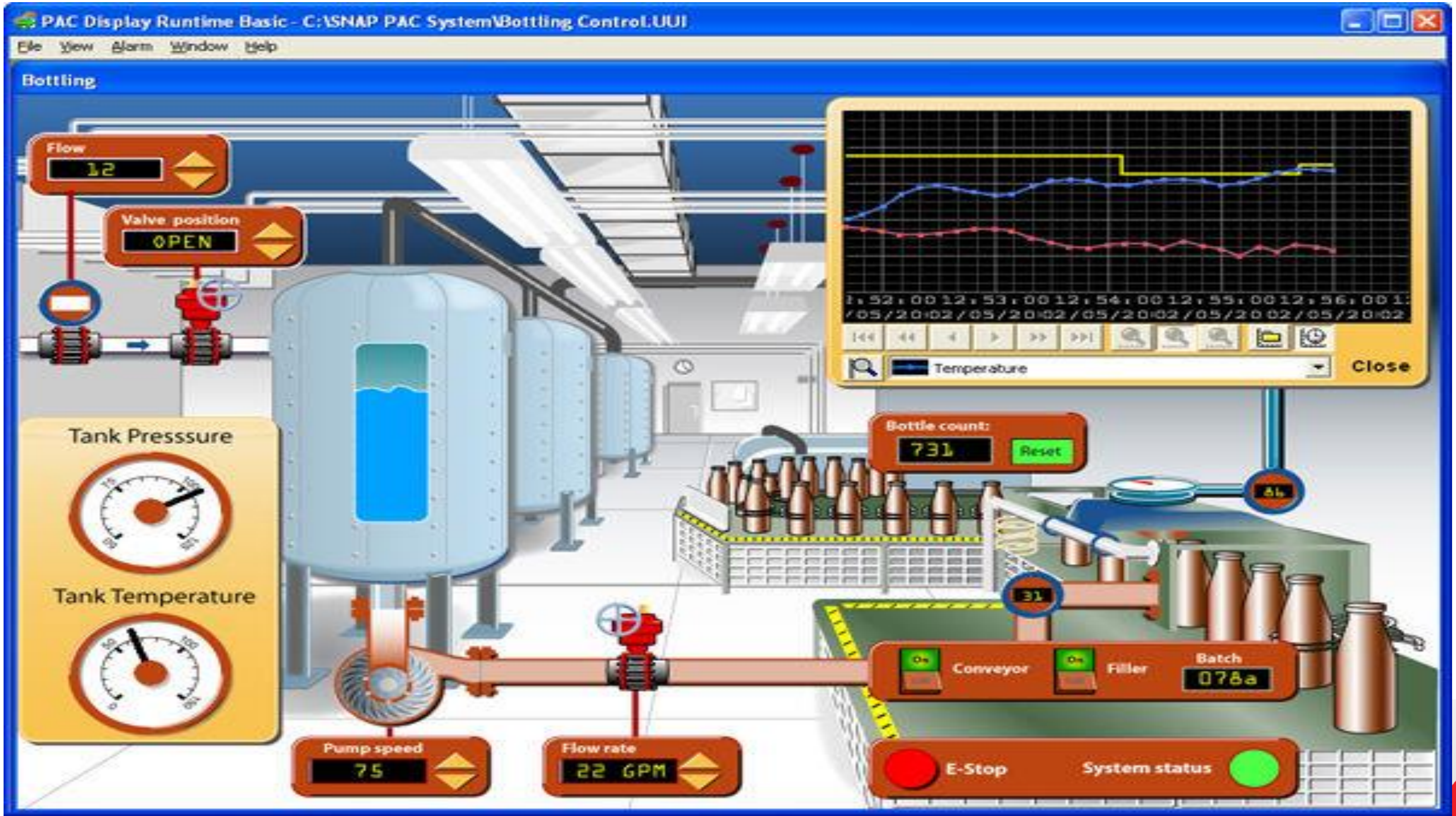


Rain Gauge	
Current	0.06 in
Rainfall Rate	0.04
Previous Hour	0.00 in
Previous Day	0.14 in
Current Month	2.30 in
Previous Month	2.00 in

Generator	
High Temp	OK
Low Fuel	OK
Low Oil	OK
Battery LOW	OK
Fail Alarm	OK

MTU and HMI

Used to monitor and control the RTUs and collect data from RTUs and the flow computer



PAC Display Runtime Basic - C:\SNAP PAC System\Bottling Control.UUI

Bottling

Flow: 12

Valve position: OPEN

Bottle count: 731

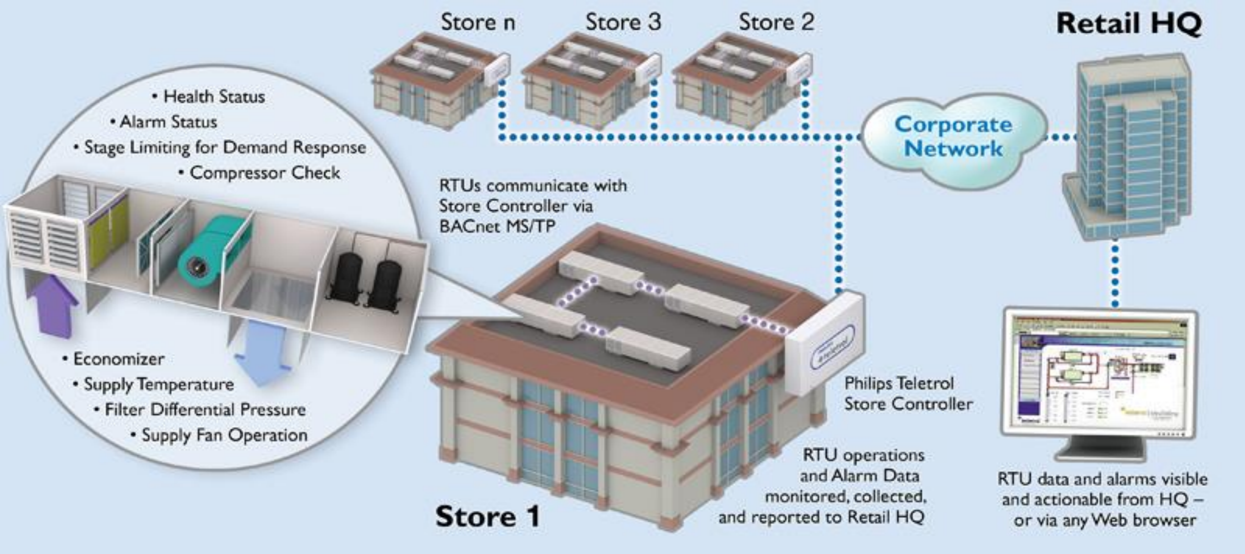
Batch: 078a

Pump speed: 75

Flow rate: 22 GPM

RTU- Remote Terminal Unit

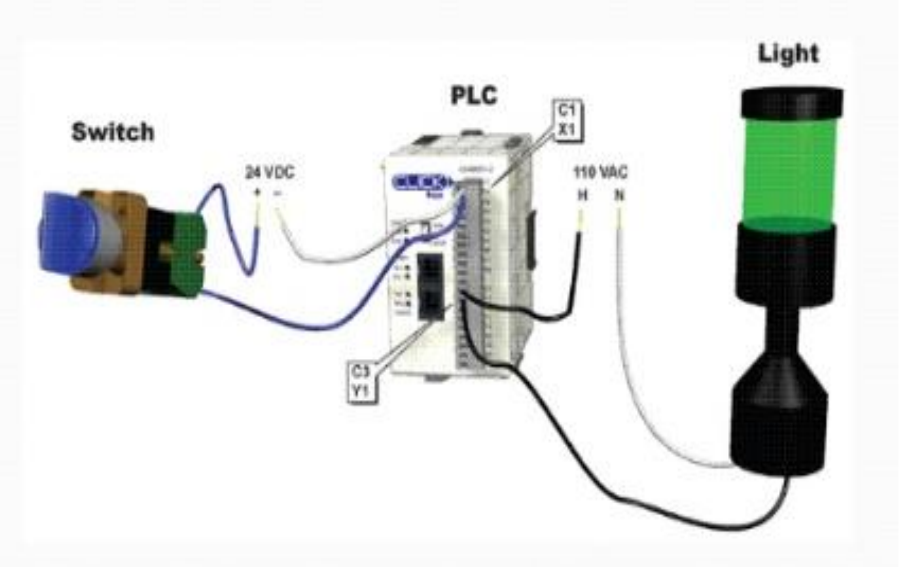
- Small computer designed to withstand harsh environmental factors such as water, salt, humidity, temperature, dirt and dust
- Consists of a real-time clock, input/output interfaces, electrical spikes protector, a restart timer and a power supply with battery backup
- It will write its data to memory and send it to the controller


Store n
Store 3
Store 2
Retail HQ
• Health Status
• Alarm Status
• Stage Limiting for Demand Response
• Compressor Check
Corporate Network
RTUs communicate with Store Controller via BACnet MS/TP
• Economizer
• Supply Temperature
• Filter Differential Pressure
• Supply Fan Operation
Philips Teletrol Store Controller
RTU operations and Alarm Data monitored, collected, and reported to Retail HQ
RTU data and alarms visible and actionable from HQ – or via any Web browser
Store 1

AutoLog® RTU Remote Terminal Unit

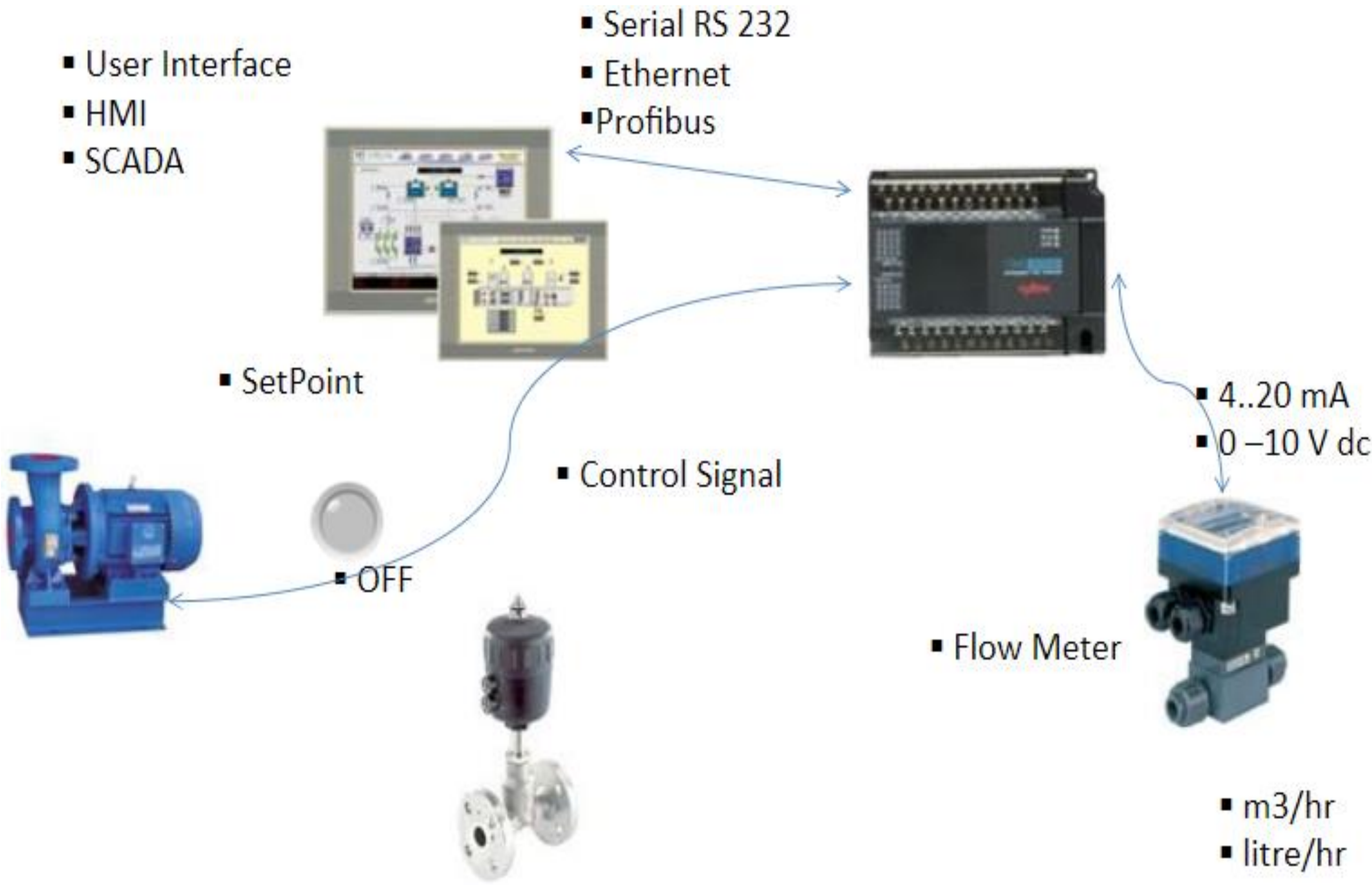
Programmable Logic Controllers (PLC)

- PLC is a programmable module which is integral part of industrial process control.
- Have both serial and Ethernet adapters.
- Commonly equipped with modems.
- Have hundreds of thousands of sensors, switches, controllers and valves.
- PLC allows the monitoring and control of different aspects of processing facilities from a centralized location.



Flow of Computer

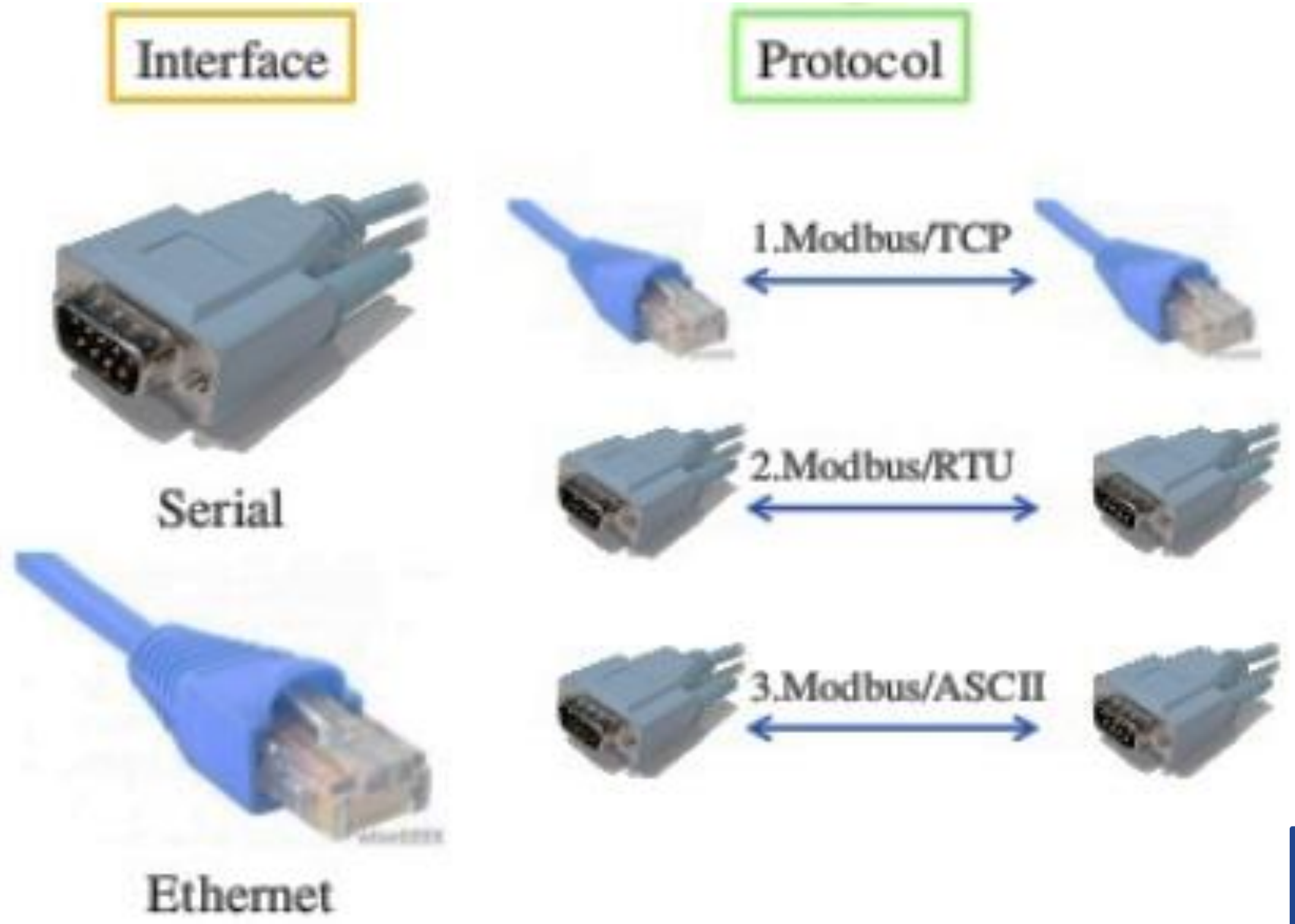
- A flow computer is an electronic computer which implements algorithms using the analog and digital signals received from flow meters, temperature, pressure and density transmitters to which it is connected into volumes at base conditions. They are used for custody or fiscal transfer.



Modbus

- Open protocol that do not need media or physical layer since Modbus is built on common infrastructure or serial communication, that typically used one of three electrical interfaces such as RS485, RS232 and RS422.
- Communication between PLCs, valves and switches.
- Operate over wireless serial or TCP/IP network.
- Compatible devices communicate with a master controller that send commands and receives data back from the end devices.
- The speed of Modbus message send at is known as the baud rate or bit per second. Make sure all device on the network use the same baud rate typically 9600-19200 is used.
- Modbus not supported ring topology or star topology.

Modbus


Interface
Protocol
Serial
Ethernet
1.Modbus/TCP
2.Modbus/RTU
3.Modbus/ASCII

Technology Background: Process Control Systems

- Commonly referred as SCADA systems in the context of security
- Designed to allow for automation in industrial process such as controlling the flow of a chemical into a processing plant. Eg: used in automated manufacturing and refinement production
- Consists of sensors that are used to detect changes in conditions, controls which can respond to those changes in condition and a human interface that allow operators to make manual changes

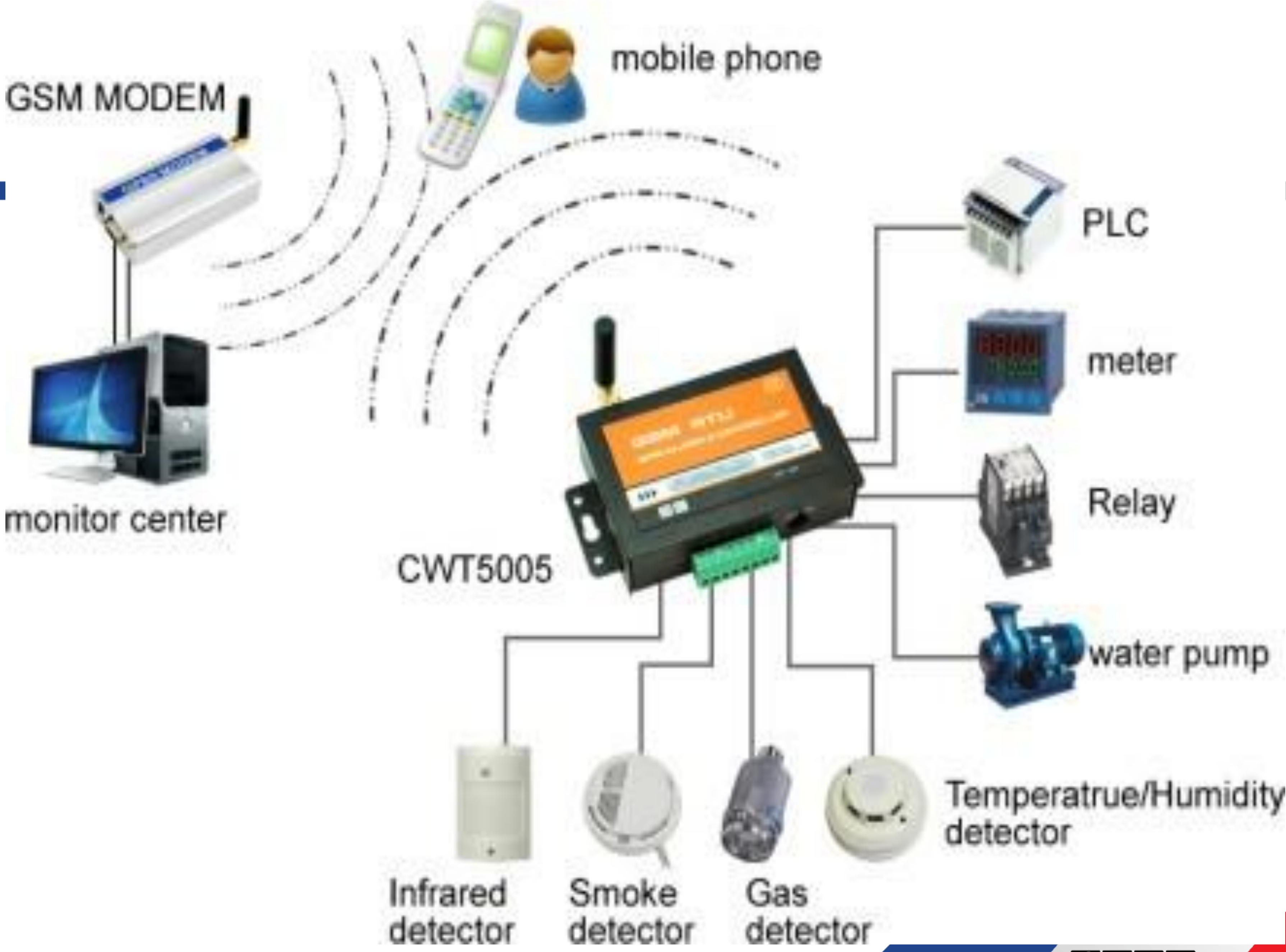
Technology Background: Process Control Systems

- The sensors provide feedback to the control and the control can reply with commands based on the feedback. Eg: air compression system, heating system, programmable logic controllers (PLCs)

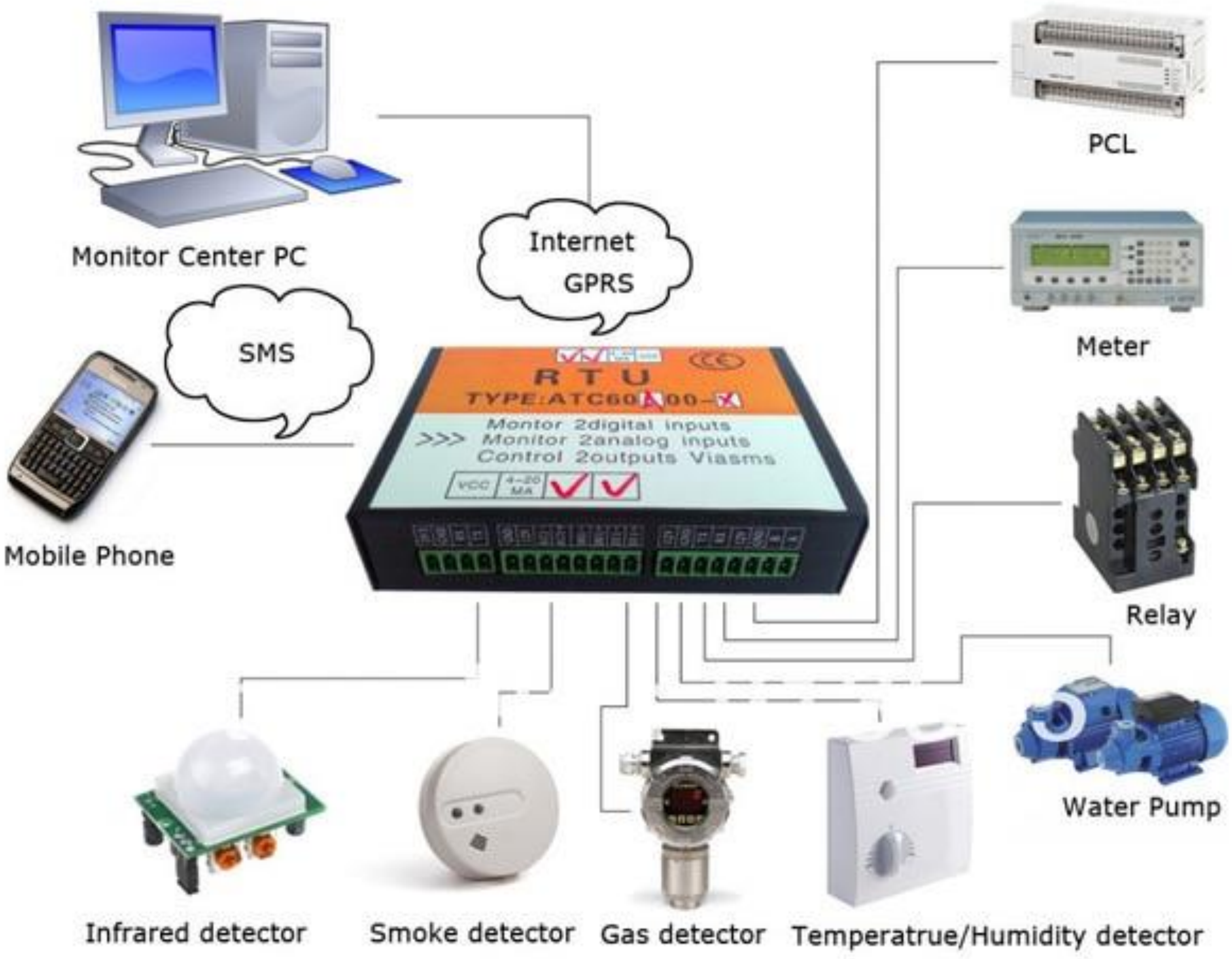
APPLICATION OF SCADA

Oil and Gas

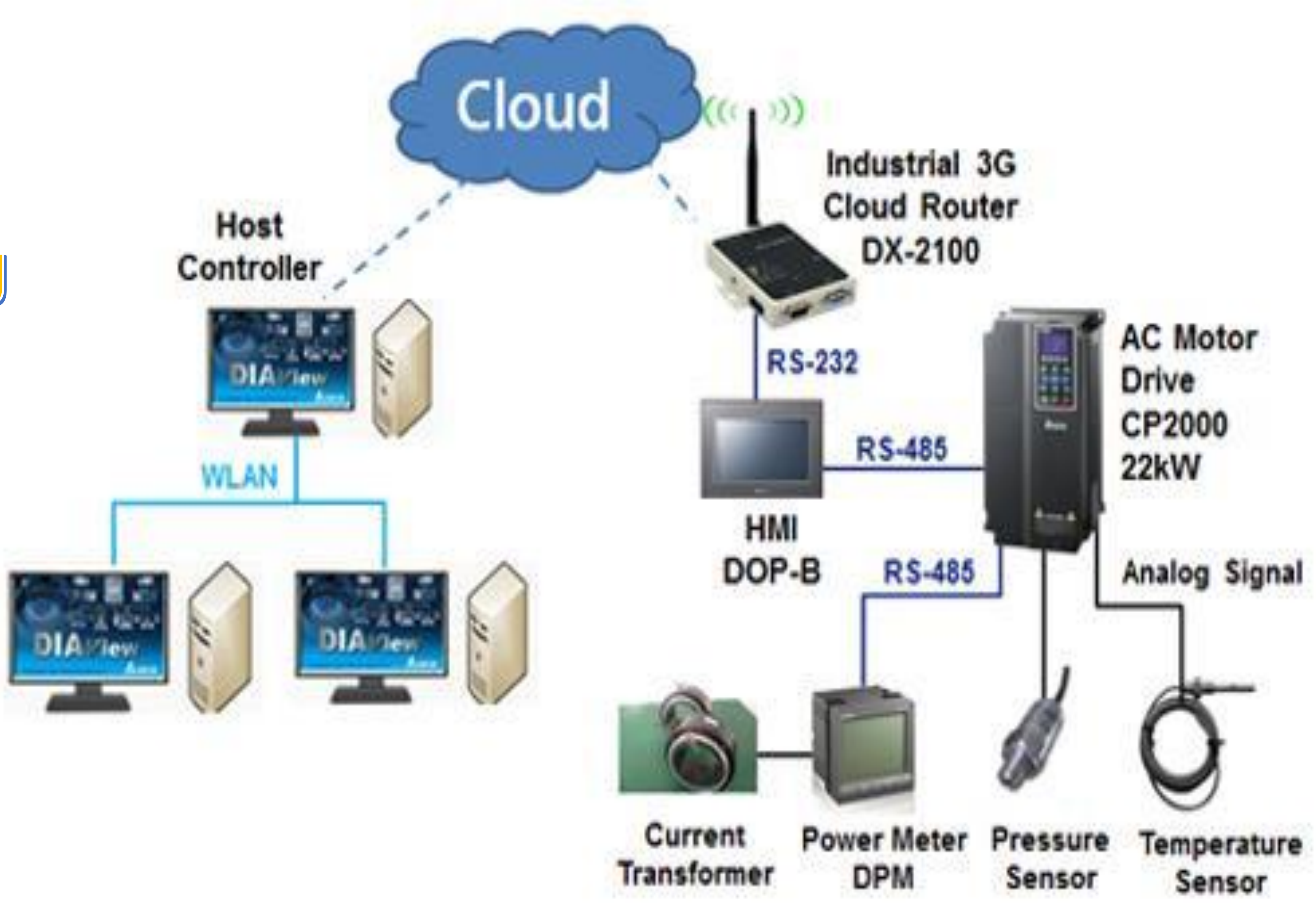
Water Level for Flood Detection

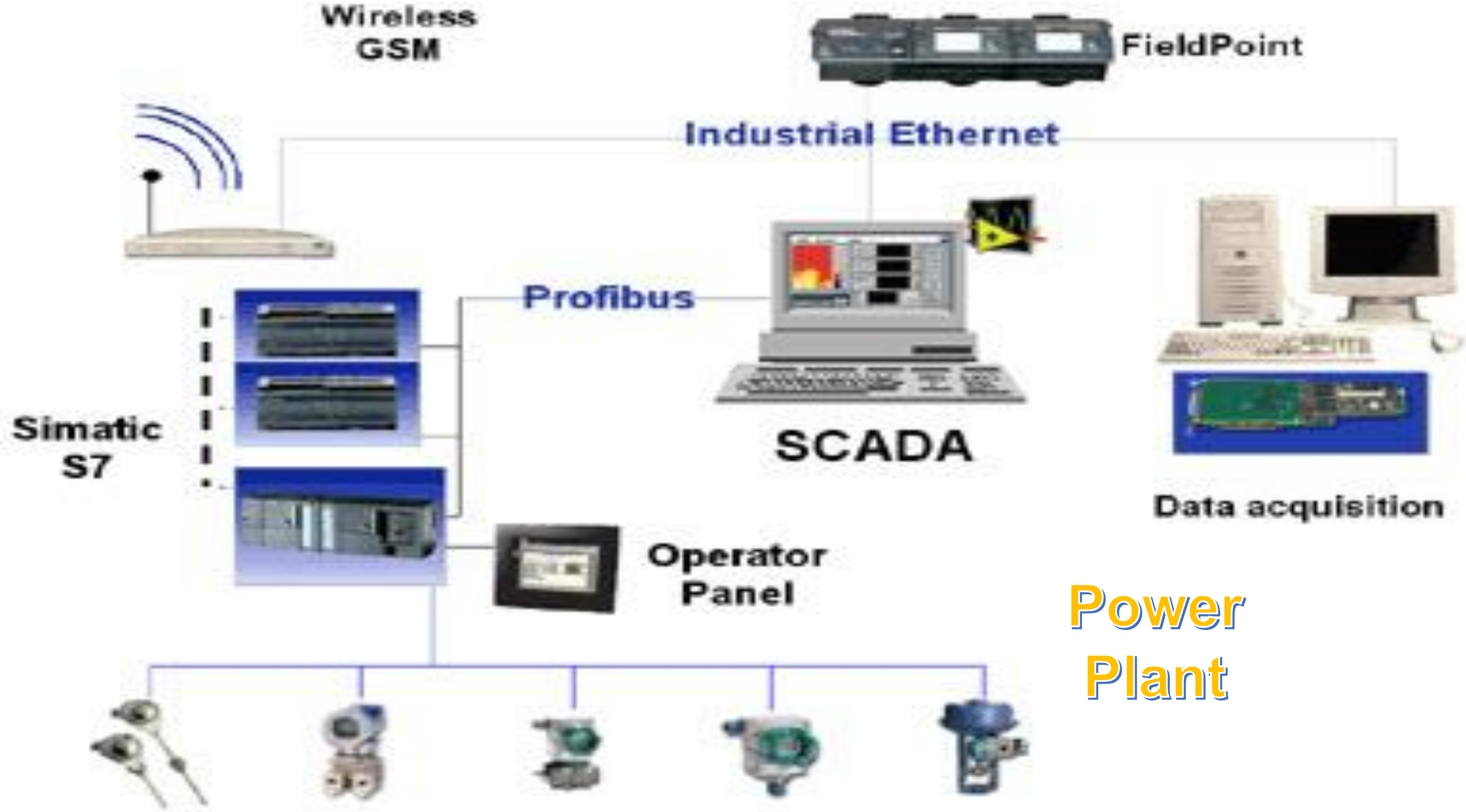


Water Supply System



Manufacturing




Wireless
GSM
FieldPoint
Industrial Ethernet
Profibus
SCADA
Simatic
S7
Data acquisition
Operator
Panel

Power
Plant

SCADA Security

- Common myths surrounding SCADA security:
- Myth 1: Our process control systems are safe because they are all isolated
- Myth 2: My network aren’t connected; my server uses a separate network to connect to the process control network and the corporate network
- Myth 3: Antivirus can’t be applied
- Myth 4: Our system isn’t vulnerable, as it uses proprietary protocols
- Myth 5: I have a firewall, so I’m safe

Threats and Challenges

- Interconnectivity issues in process control networks and corporate networks
- Weaknesses in standardizing on common OS and protocols. Mostly used Windows and Linux with TCP/IP communication
- Issues on patching and upgrading the system
- Vulnerability testing leads to simply crashing or needing to be restarted on the application
- Migration to the ‘wireless plant’

CONCLUSION

Conclusion

- SCADA has been widely used in various critical infrastructure.
- SCADA has evolved to meet the demand from the industry and user requirements.
- Control system within critical infrastructure is exposed to threats and risks. Thus, SCADA integrates the different components and deployments from various manufacturers to protect the security level at device and the overall environment.

Thank You

MyUTeM

www.utem.edu.my