SCADA Security (**S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition)

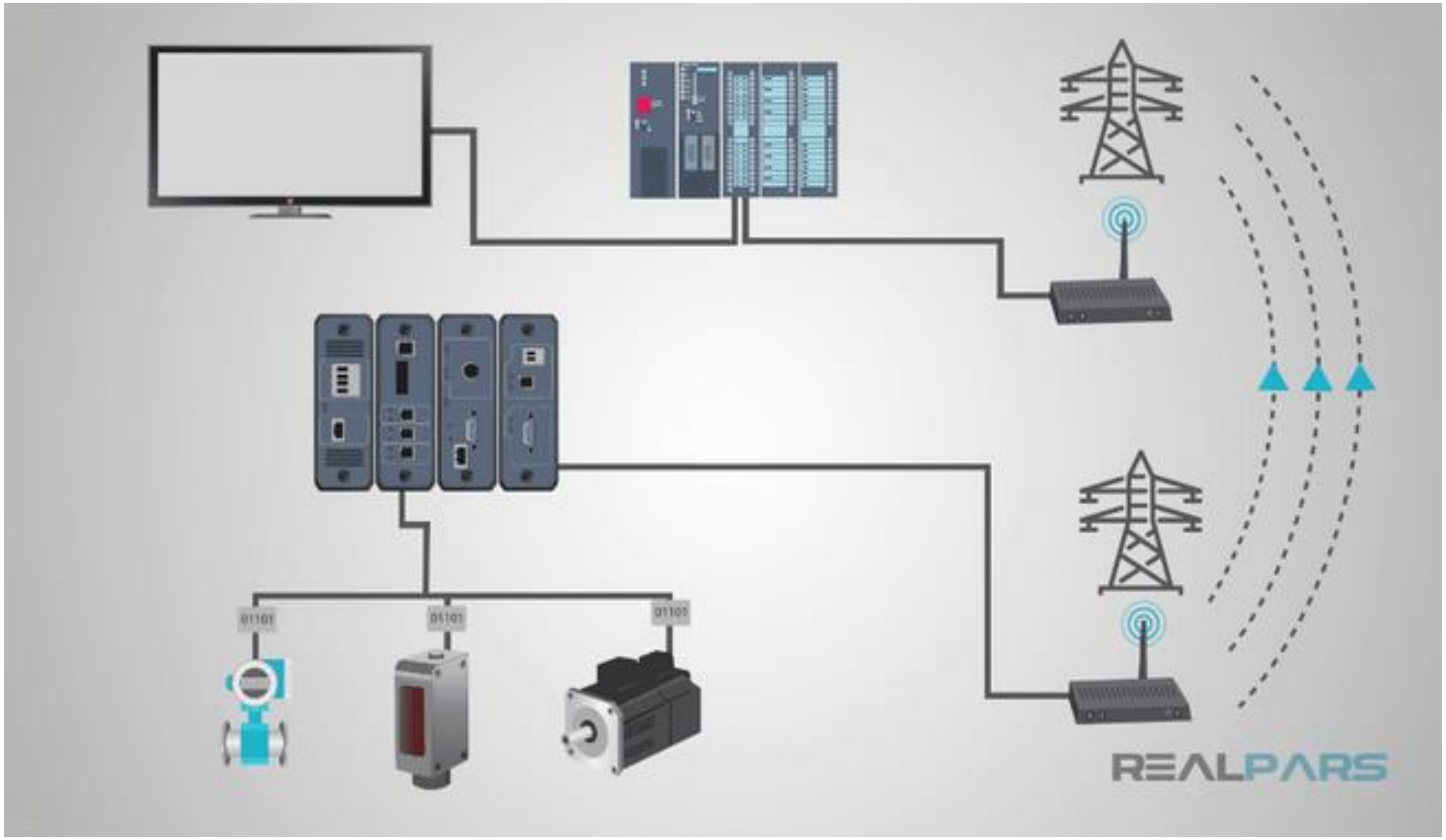
TCS 591: Unit 5

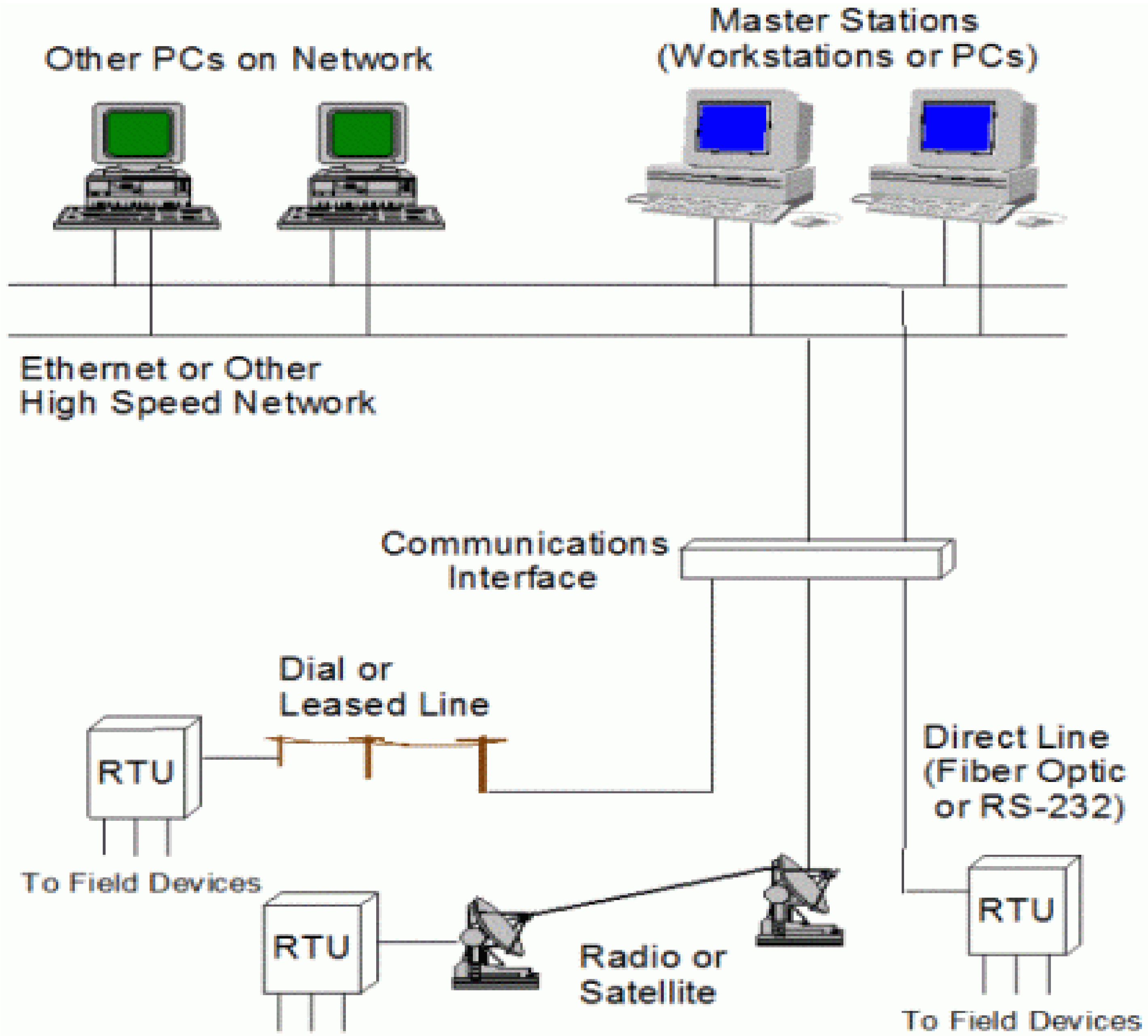
SCADA :-Supervisory Control And Data Acquisition

SCADA (Supervisory Control and Data Acquisition) is a combination of **software and hardware** components that work together to monitor and control industrial processes.

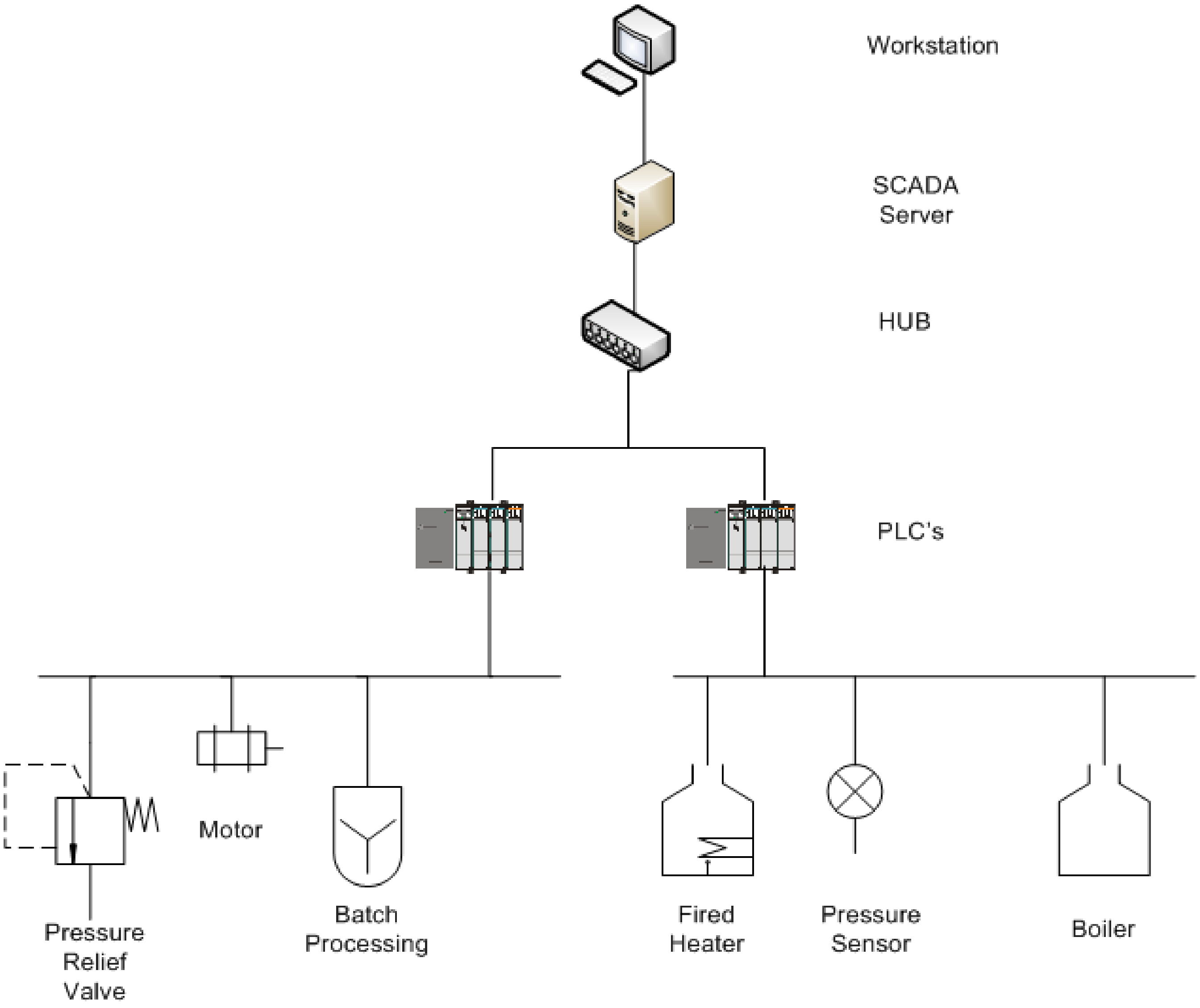
They are used to monitor and control large-scale industrial processes, such as power generation, **water treatment**, and manufacturing.

SCADA provides a **high level** of supervision, data acquisition, and analysis, enabling operators to monitor the status of various devices and processes, detect anomalies, and make informed decisions.


01101
01101
01101
REALPARS

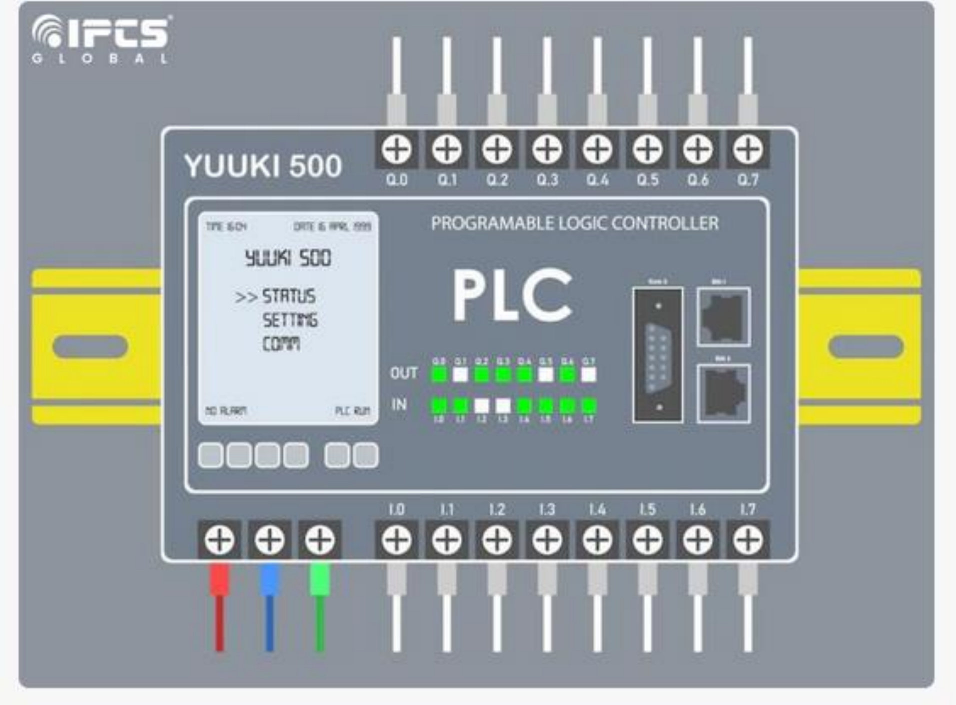

Master Stations
(Workstations or PCs)
Other PCs on Network
Ethernet or Other
High Speed Network
Communications
Interface
Dial or
Leased Line
RTU
To Field Devices
Direct Line
(Fiber Optic
or RS-232)
RTU
Radio or
Satellite
RTU
To Field Devices

SCADA Overview

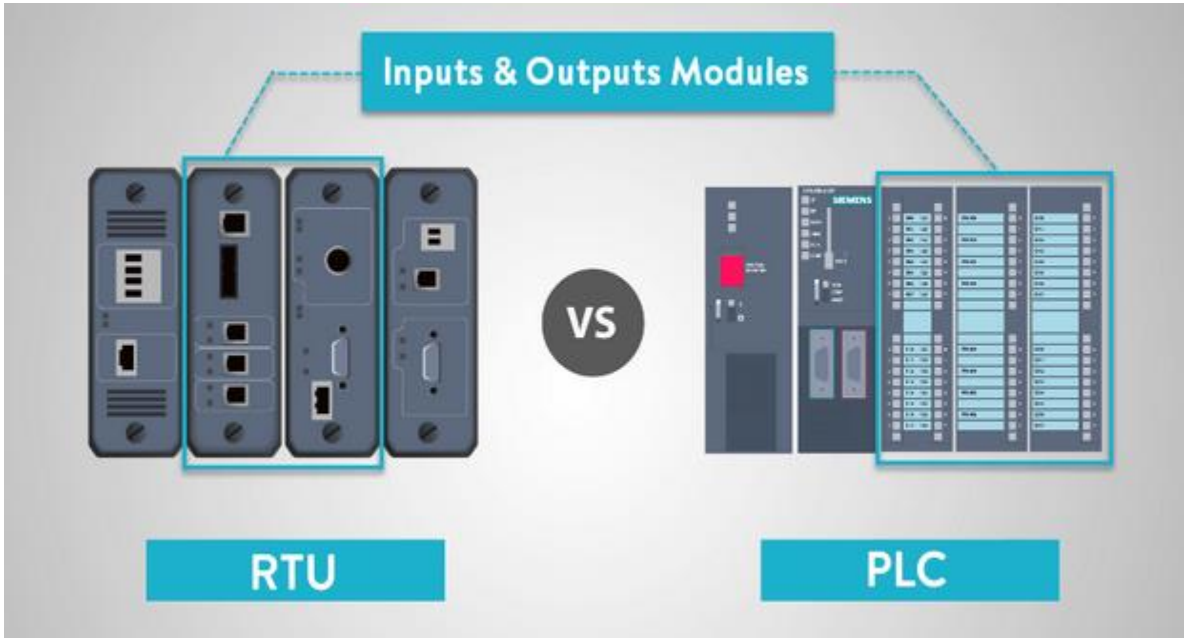


Programmable Logic Controller (PLC)

- A Programmable Logic Controller (PLC) is a **specialized computer designed** for industrial automation and control.
- PLCs are used to manage and control various processes, including manufacturing, assembly lines, and material handling systems.
- Considering a water treatment plant environment, PLCs control various sensors like pumps, valves, and actuators which are the main driving factors in the process.
- They are designed to be robust, reliable, and capable of operating in harsh industrial environments.


IFCS GLOBAL
YUUKI 500
Q.0 Q.1 Q.2 Q.3 Q.4 Q.5 Q.6 Q.7
PROGRAMABLE LOGIC CONTROLLER
PLC
YUUKI 500
>> STATUS
SETTING
COMM
NO ALARM
PLC RUN
OUT
IN
I.0 I.1 I.2 I.3 I.4 I.5 I.6 I.7

L
N
24V


Inputs & Outputs Modules
VS
RTU
PLC
SIEMENS

RTU(Remote terminal Unit)

- RTU stands for remote terminal unit. An RTU is a control device typically installed in a remote location as part of a large system.
- The main purpose of an RTU is to monitor and control field devices, such as valves, actuators, sensors, and more. RTUs are essential components of supervisory control and data acquisition (SCADA) systems, establishing interfaces between SCADA control and physical processes

Unique Characteristics of SCADA

1. **Real-time Operations**: SCADA systems operate in real-time, controlling and monitoring physical processes that require immediate attention.
2. **Geographic Distribution**: SCADA systems often span large geographic areas, making it difficult to implement and manage security controls.
3. **Legacy Systems**: Many SCADA systems are based on legacy technologies that were not designed with security in mind.
4. **Limited Resources**: SCADA systems often have limited processing power, memory, and bandwidth, making it challenging to implement robust security controls.

SCADA Security Threats

1. **Cyber attacks**: Malware, ransomware, phishing, and other types of cyber attacks can compromise SCADA systems.
2. **Unauthorized access**: Unauthorized access to SCADA systems can allow attackers to manipulate or disrupt industrial processes.
3. **Data breaches**: SCADA systems store sensitive data, and a data breach can compromise this data.
4. **Physical attacks**: Physical attacks on SCADA systems, such as vandalism or sabotage, can disrupt industrial processes.
5. **Insider threats**: Insider threats, such as employees or contractors with authorized access, can intentionally or unintentionally compromise SCADA

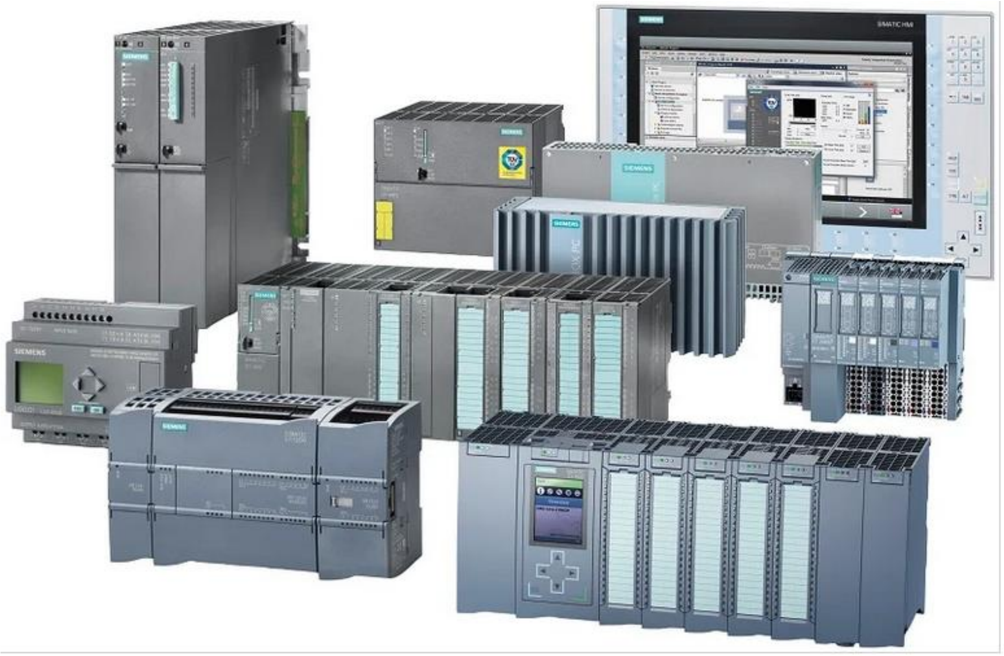
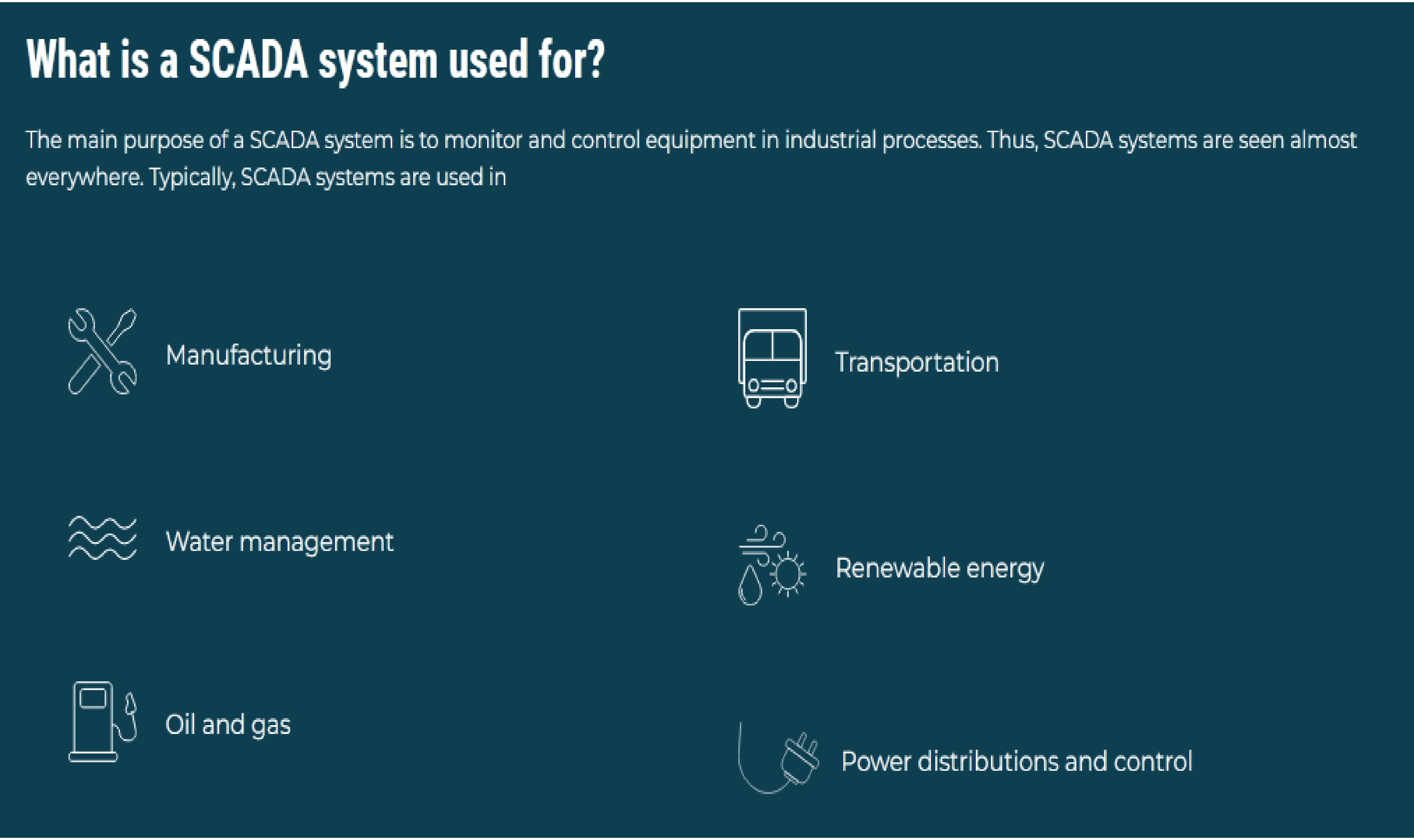


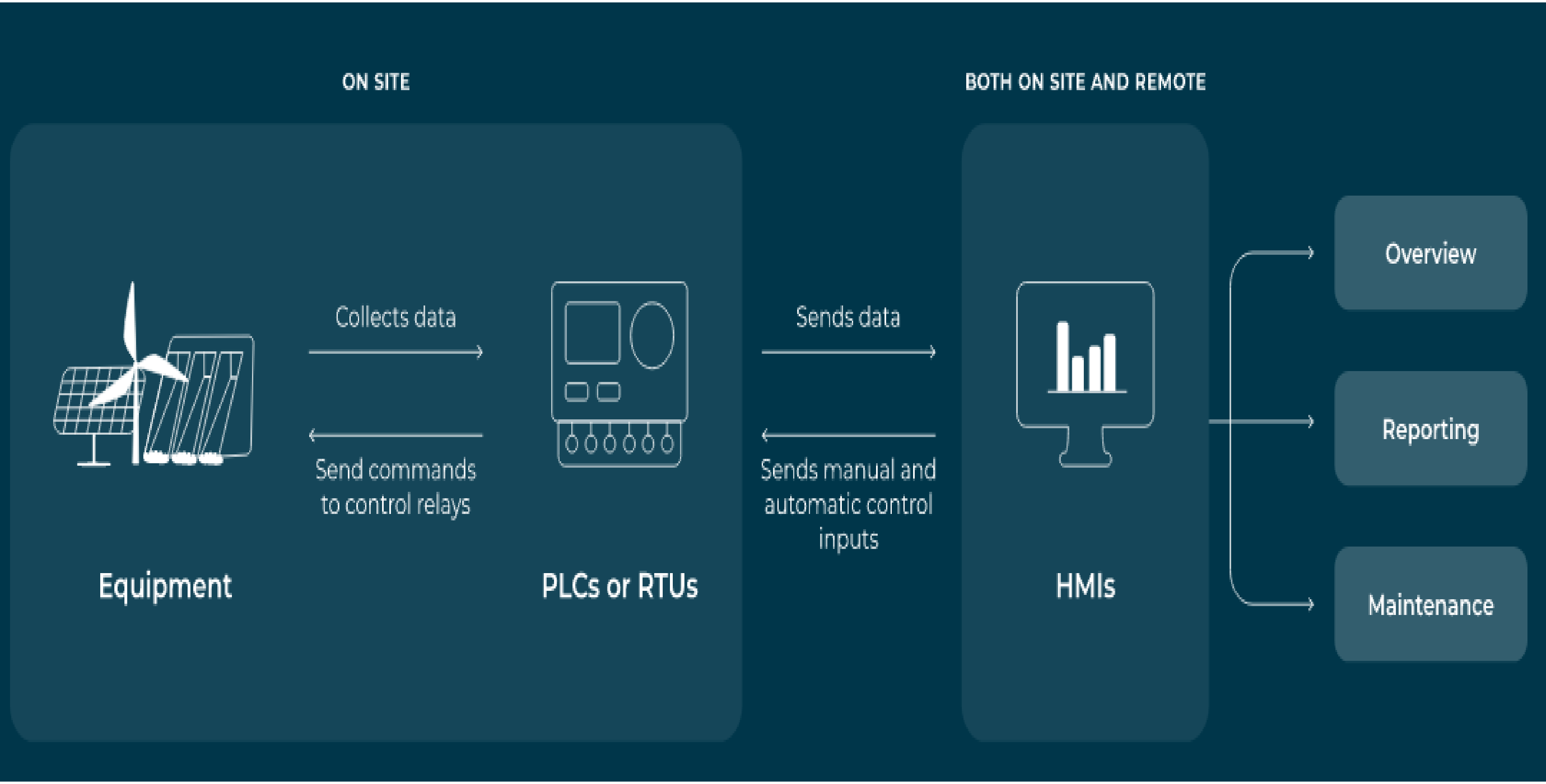
Figure 1. *A modern set of industrial PLCs. Image used courtesy of Siemens*



What is a SCADA system used for?

The main purpose of a SCADA system is to monitor and control equipment in industrial processes. Thus, SCADA systems are seen almost everywhere. Typically, SCADA systems are used in

- Manufacturing
- Transportation
- Water management
- Renewable energy
- Oil and gas
- Power distributions and control



ON SITE

BOTH ON SITE AND REMOTE

Equipment

Collects data

Send commands to control relays

PLCs or RTUs

Sends data

Sends manual and automatic control inputs

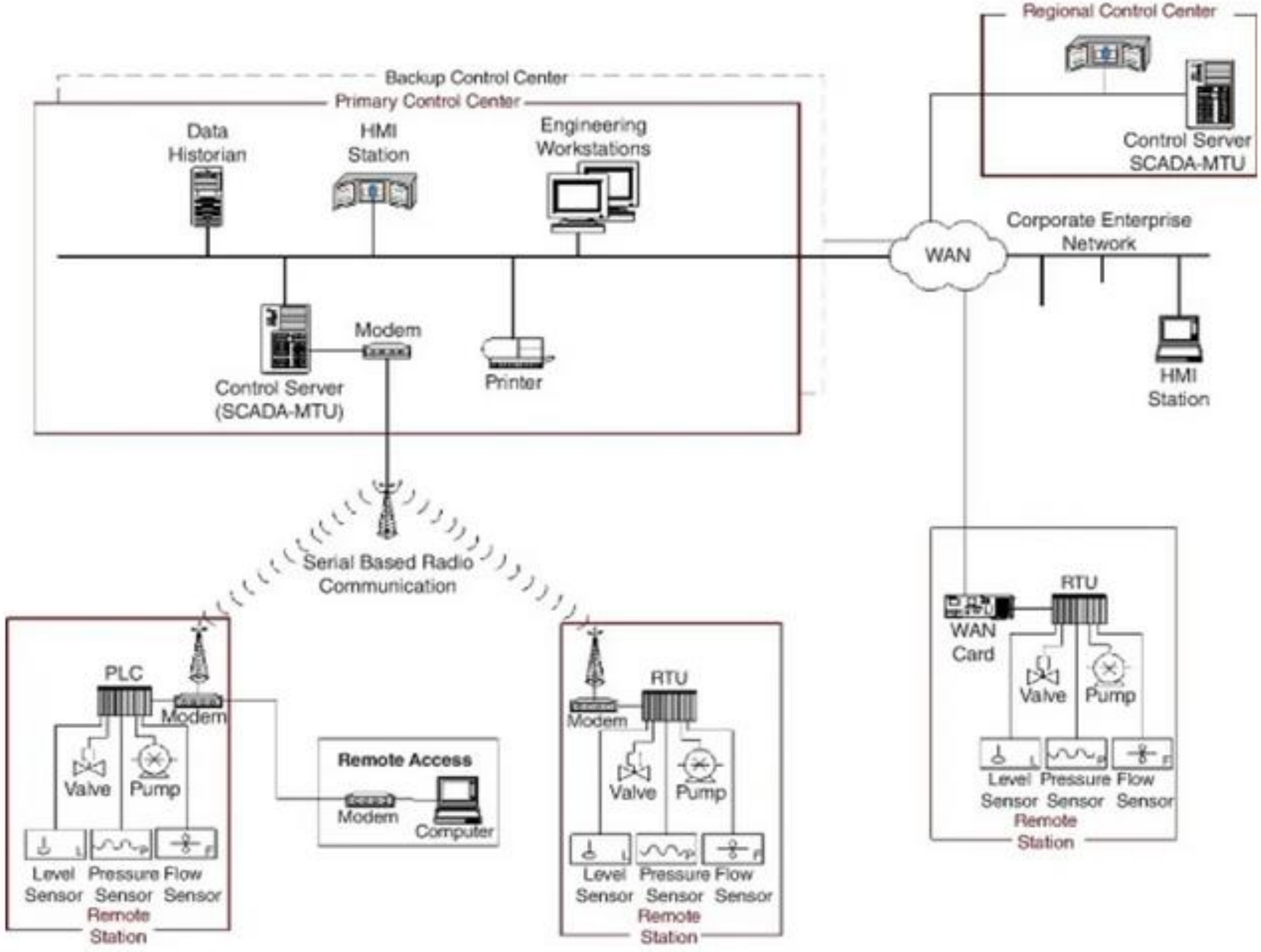
HMIs

Overview

Reporting

Maintenance

SCADA Components



SCADA Components. *Credits: ScienceDirect.com*

SCADA Security

- SCADA security is the practice of protecting supervisory control and data acquisition (SCADA) networks, a common framework of control systems used in industrial operations.
- These networks are responsible for providing automated control and remote human management of essential commodities and services such as water, natural gas, electricity and transportation to millions of people.

SCADA Security

- They can also be used to improve the efficiencies and quality in other less essential real-world processes such as snowmaking for ski resorts and beer brewing.
- SCADA is one of the most common types of **industrial control systems (ICS).**

PLC vs SCADA

What is the main difference between PLC and SCADA systems?

- PLCs are designed for real-time control tasks, controlling individual devices or small-scale processes, while SCADA systems provide a higher level of supervision, data acquisition, and analysis for large-scale industrial processes.

Challenges in SCADA

- SCADA systems can cost an organization from tens of thousands to millions of dollars. For these reasons, it is essential that organizations implement robust SCADA security measures to protect their infrastructure and the millions of people that would be affected by disruption caused by an external attack or internal error.

Who would attack SCADA?

Attackers

- Script kiddies
- Hackers
- Organized crime
- Disgruntled insiders
- Competitors
- Terrorists
- Hactivists
- Eco-terrorists
- Nation states

SCADA Security

- Perimeter Protection
  - Firewall, IPS, VPN, AV
  - Host IDS, Host AV
  - DMZ
- Interior Security
  - Firewall, IDS, VPN, AV
  - Host IDS, Host AV
  - NAC
  - Scanning
- Monitoring
- Management

SCADA vs Traditional Security

SCADA security has evolved dramatically in recent years. Before computers, the only way to monitor a SCADA network was to deploy several people to each station to report back on the state of each system. In busier stations, technicians were stationed permanently to manually operate the network and communicate over telephone wires.

Simple Protocols

- Because SCADA devices with embedded controllers tend to have limited computational power, and have historically been connected via low speed serial lines, SCADA protocols tend to be quite simple, with little or no protection against spoofing, replay attacks, or a variety of denial of service attacks.

Challenges in SCADA

- Industrial plants, and the instrumentation they include, tend to be long life cycle projects – ten, fifteen or twenty year project lives are by no means uncommon. As a result, the devices that may be deployed as part of that construction may be virtual antiques by the time the facility is finally decommissioned, and there's no provision for refreshing those devices the way you might upgrade out of date PCs in an office.
- ‘"Anti-virus software doesn't work on these SCADA systems,“ "Many of these systems are based on old Intel 8088 processors, and security options are limited .“’

Challenges in SCADA

- SCADA devices are often controlled from central monitoring stations (MTUs, or “master terminal units”). Historically those were Unix-based systems, but many contemporary MTUs are now Microsoft Windows based.
- “The end-of-life for Windows NT is having a big impact on manufacturers.”

Hard-to-Upgrade Remote Devices

- Remote devices (RTUs and PLCs) also tend to be hard to upgrade :
  -- the device may use an OS and application that was burned to ROM, and which is not rewritable (“upgrade” == replacing ROMs)
  -- the device may be physically sealed and not upgradeable, or be located in a difficult location, or have no removable media
  --- the vendor may no longer be in business, or may not be producing upgrades, or the vendor may not be allowing upgrades

Certifying Patches

- An example from the embedded system world:

"Health care IT professionals say medical device makers prohibit them from changing the systems and even from running anti-virus software in some cases. These IT administrators say manufacturers often are slow to supply software patch updates and routinely claim the Food and Drug Administration (FDA) requires approval of patch-base changes. However the FDA says it has no such rules…"

Need For Positive Control ==> Simple Known/Shared Passwords

- Because of the need for positive access and control, there is a trend toward simple, known, and shared passwords. Users like to avoid situations such as: “Do you know the password to turn off the nuclear reactor before it melts down? I forgot mine today…”

Common Passwords Across Multiple Devices

- There’s also the sheer issue of managing passwords for thousands of devices – passwords will tend to be common across devices as a practical matter (this is much like SNMP community strings)
- And of course those passwords aren’t changed very often (if at all), even when staff transitions occur or years have gone by…

Access Control Granularity and Accountability

- Related to the problem of shared, simple passwords is the issue of poor access control granularity; again, like SNMP, in most cases access control is “read” (everything) or “read/write” (everything).
- Accountability with common passwords is poor/non-existent, which may be one reason that transaction logging also may be limited. (Any bets how long it will take to get something like syslog-ng or SDSC Secure Syslog for SCADA systems?)

Few Firewall Options

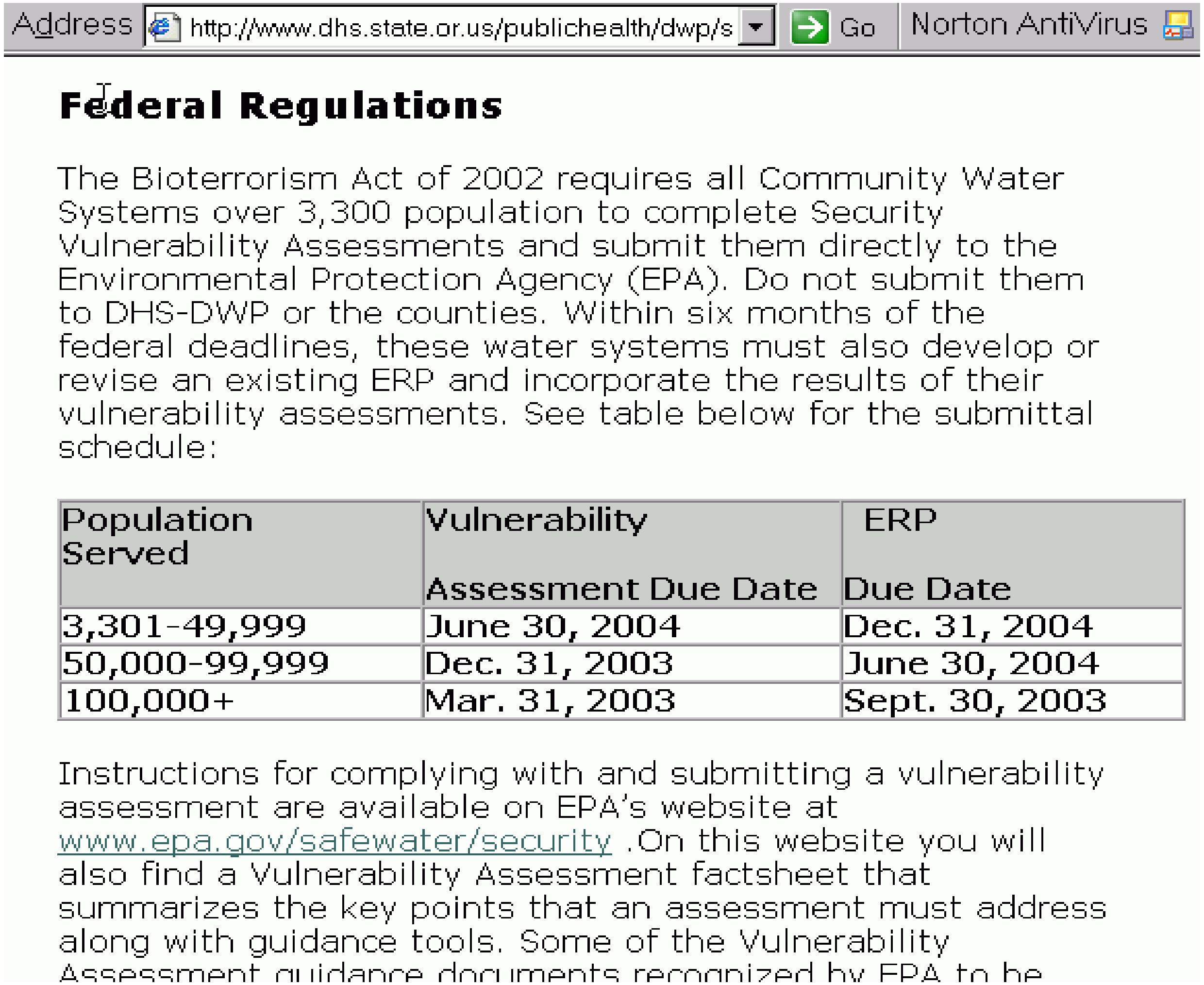
- Speaking of firewalls, SCADA-protocol aware firewall choices are pretty limited out there right now

SCADA Systems Must Be Hardened

- All the security areas just mentioned need to be reviewed and addressed on a system by system basis, which in some cases will mean substantial new investments/forklift upgrades

Do Vulnerability Assessment/Security Auditing/Penetration Testing of SCADA Systems

- Some named industries are already required to do this sort of thing…



Address http://www.dhs.state.or.us/publichealth/dwp/s

Federal Regulations

The Bioterrorism Act of 2002 requires all Community Water Systems over 3,300 population to complete Security Vulnerability Assessments and submit them directly to the Environmental Protection Agency (EPA). Do not submit them to DHS-DWP or the counties. Within six months of the federal deadlines, these water systems must also develop or revise an existing ERP and incorporate the results of their vulnerability assessments. See table below for the submittal schedule:

Population Served	Vulnerability Assessment Due Date	ERP Due Date
3,301-49,999	June 30, 2004	Dec. 31, 2004
50,000-99,999	Dec. 31, 2003	June 30, 2004
100,000+	Mar. 31, 2003	Sept. 30, 2003

Instructions for complying with and submitting a vulnerability assessment are available on EPA's website at www.epa.gov/safewater/security .On this website you will also find a Vulnerability Assessment factsheet that summarizes the key points that an assessment must address along with guidance tools. Some of the Vulnerability Assessment guidance documents recognized by EPA to be

Improve Remote Monitoring of Key Sites

- If you have fiber to remote facilities, you have sufficient bandwidth to allow for extensive video and audio instrumentation of that facility, and for reports from sophisticated intrusion detection systems. Those systems should be tied into SCADA systems, and system responses should be recalibrated in response
  to identification of active or potential threats.
- Alternatively, aren’t key remote facilities (many of which cost millions to build, and which are virtually irreplaceable) important enough to justify round-the-clock on-site technical and security personnel?