

## Learning Objective 1

### Session 1: Industrial Control Systems Overview

An industrial control system (ICS) is a generic term used to describe any system that gathers information on an industrial process and modifies, regulates, or manages the process to achieve a desired result.

#### LO1: Describe basic industrial control systems

The term “industrial control system” or “ICS” refers to a broad set of control systems, which include:

- SCADA (Supervisory Control and Data Acquisition)
- DCS (Distributed Control System)
- PCS (Process Control System)
- EMS (Energy Management System)
- AS (Automation System)
- SIS (Safety Instrumented System)
- Any other automated control system.

#### SCADA or DCS?

Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS) have historically been different.

SCADA:

- The key word in SCADA is “Supervisory.”
- This indicates that decisions are not directly made by the system.
- The system executes control decisions based on control parameters by operators or management.
- SCADA systems are typically deployed across large geographical areas (e.g., electric grid).

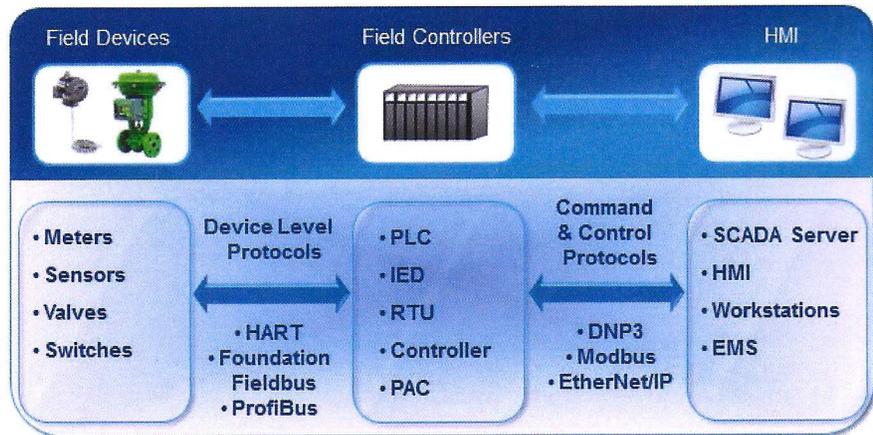
DCS:

- DCS provides real-time monitoring and control of a given process within a plant.
- All major components of the system are usually confined to one or several close-by facilities (e.g., refinery).

As technology advances, the terms are getting blurred. Policy makers often refer to “SCADA” when they are actually referring to another type of ICS. The difference between SCADA systems and DCS are shrinking as SCADA vendors incorporate DCS functionality in their systems and vice versa.



## ICS Basics



The primary purpose of an ICS is to measure and control a process. ICSs collect information about some process or function using a communications infrastructure to send the data back to an operator. The operator reviews the data, typically in a graphical format, assesses the operational status of the process, and tunes the system for optimal performance.

**Field devices** (shown above on the left) are the instruments and sensors that measure process parameters and the actuators that control the process. This is the interface between the ICS and the physical process. These sensors or measuring instruments are often referred to as input devices because they “input” data into the ICS.

**Field controllers** are responsible for collecting and processing input and output information, sometimes referred to as I/O. They also send the process data to the human machine interface (HMI) and process control commands from the operators. They are often located close to the field devices.

Some examples of different types of field controllers:

- Programmable Logic Controllers (PLCs)
- Intelligent Electronic Devices (IEDs)
- Remote Terminal Units (RTUs)
- Distributed Controllers and Process Automation Controllers (PACs).

Finally, servers, **HMIs**, and engineering workstations take the information from field controllers and display the data in a manner that depicts what is happening in the process. The user interface is usually referred to as the HMI and allows the operator to have a real-time, or near real-time, operational view of the process.

These three components are linked using networks or communication channels.

## Field Controllers – Environmental

Unlike office workstations and servers, field controllers are located in industrial environments that are subject to all types of hazards and weather.

- Hazardous – Corrosive, flammable.
  - Weather – Temperature, rain, lightening, wind.
  - Miscellaneous – Vibrations, fire, floods, dust, dirt, animals, oil, etc.
- 
- 
- 
- 

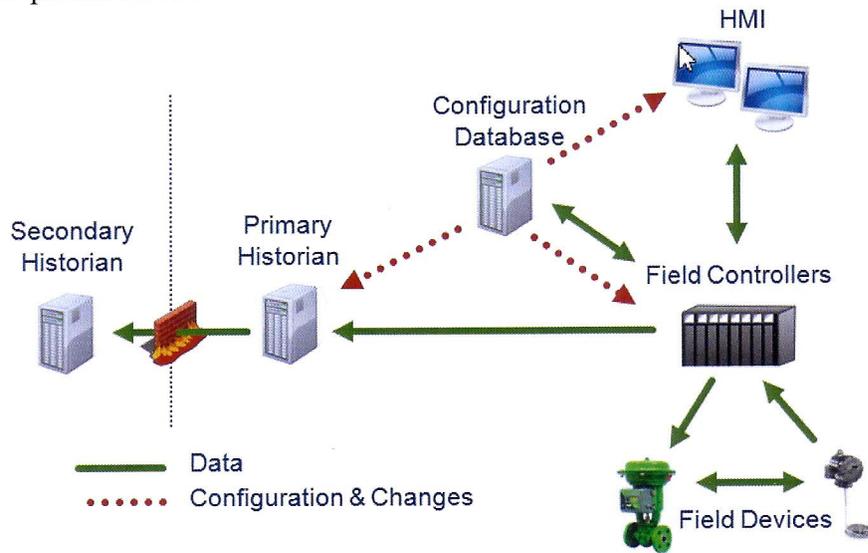
## Field Controllers – Hardware

- Power – Direct current (DC), alternating current (AC), solar, battery backup.
  - Processors – X86 (Intel), PowerPC (power.org consortium), ARM (ARM Holdings), MIPS (MIPS Technology).
  - Memory:
    - Nonvolatile memory: flash memory, EEPROM, EPROM, ROM, Firmware (boot code, real time operating system [RTOS], application programs).
    - Volatile memory: RAM, variables, stacks, and buffers.
  - Input/output – Discrete, analog, fieldbus.
  - Communication Ports:
    - Serial – RS232, RS422/485, USB, modems, radio.
    - Network – Ethernet radio, ControlNet, LonWorks.
  - User interface:
    - Internal – Status lights, small LCD screens, keypad, jumpers, dip switches, switches.
    - External – Browser, applications.
- 
- 
- 
-



## Data Flow in ICSs

Data flow can vary from vendor to vendor but the basic flows are depicted below.



The field devices communicate with the field controllers, or they can communicate with other field devices.

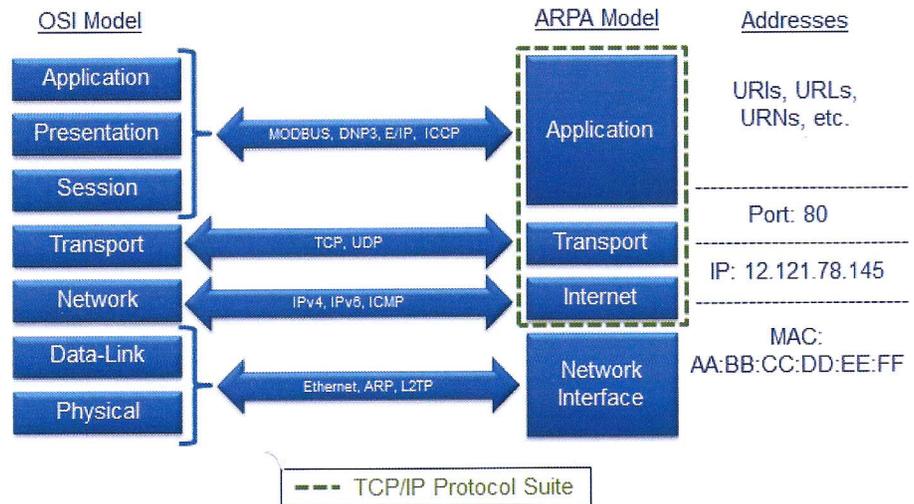
The field controllers consolidate the data and transmit this information to the HMI components. For instance, the field devices send real-time process data to be preserved in the historian, readiness and hardware error status to the configuration database, and real-time process data to the operator consoles (HMI).

Moving to the configuration database, this workstation or server sometimes performs double duty as an HMI or a platform for third-party applications (including historians). The configuration database typically stores information for setting up and configuring the various components in the ICS. From this station, the information is transferred to the respective devices on the network so they are configured properly.

The HMI stations present data from the field controllers using displays built either on the configuration database station or another engineering workstation/server. This is the operator's primary view into the system. Errors in this display can cause the operator to make poor decisions.

The last components shown are the historians. There are two historian servers shown on either side of a firewall. The primary historian collects real-time data in the protected ICS zone and replicates the data to the secondary historian, which resides on a separate network(s) segmented by a firewall.

## Network Models



The network models divide the functions of a protocol into a series of layers. Each layer has the property that it only uses the functions of the layer below, and only exports functionality to the layer above. A system that implements protocol behavior consisting of a series of these layers is known as a “protocol stack” or “stack.”

This OSI model is roughly adhered to in the computing and networking industry. Its main feature is in the interface between layers that dictate the specifications on how one layer interacts with another. This means that a layer written by one manufacturer can operate with a layer from another (assuming that the specification is interpreted correctly). These specifications are typically known as Request for Comments or RFCs in the TCP/IP community. They are International Organization for Standardization (ISO) standards in the OSI community.

Protocols are used in Information Technology (IT) architectures. There are hundreds of protocols in the ICS domain.

### Protocols (partial list)

Many protocols are available and used in ICSs, most of which are proprietary.

ANSI X3.28	Gedac 7020	DeviceNet
BBC 7200	ICCP	DH+
CDC Types 1 and 2	Landis & Gyr 8979	Profibus
Conitel 2020/2000/3000	<b>Modbus</b>	Tejas 3 and 5
DCP 1	<b>OPC (a standard)</b>	TRW 9550
DNP3	ControlNet	UCA

## OPC

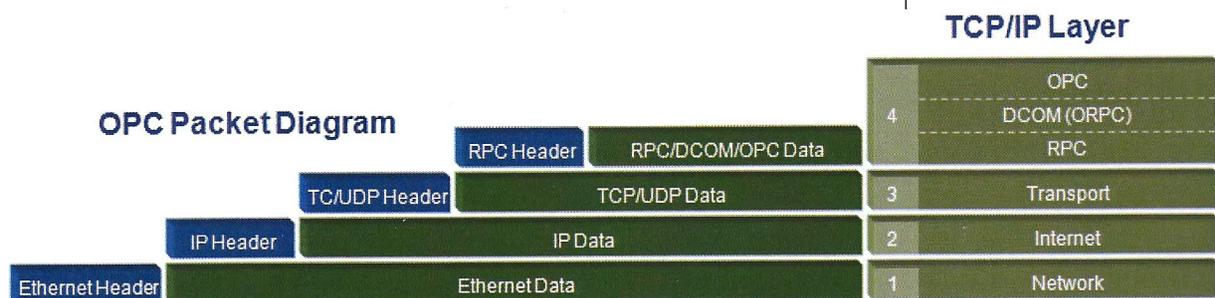
### The OPC Foundation – The interoperability Standard for Industrial Automation

OPC is open connectivity via open standards. It is based on client server technology. The client requests data from the server, which gets and sends the requested data to the client.

- Classic OPC
  - Originally developed in 1996.
  - Based on OLE, COM, and DCOM from Microsoft.
- OPC .NET 4.0 provides .NET interface to “Classic Servers.”
- OPC Unified Architecture (UA) – Based on open standards such as XML.

*For more information on OPC, visit:*

[www.opcfoundation.org](http://www.opcfoundation.org)



### Why is OPC Popular?

- Vendors use proprietary protocols to talk between their components (PLCs, controllers, data servers, HMI, etc.)
- Multiple specific drivers were required for integration of devices (typically with a 1:1 relationship between devices and drivers).



- OPC provides a single common framework or interface.



For more information on Modbus, visit: [www.modbus.org](http://www.modbus.org)

## Modbus

The Modbus protocol was initially created for use over serial connections and was adapted for use over TCP/IP. Numerous vendors have implemented their own versions of Modbus over TCP; however, there is no official standard to which these implementations are being built.

Modbus communications are simple: a client issues a single-packet request to a server to read or write data; the server acts on the request and returns a single-packet response that indicates success or failure of the request.

Modbus is one of the oldest and more popular ICS protocols in use today. Modbus is an application layer protocol used to communicate with field controllers. Because of its popularity most field controllers support Modbus. Unlike most protocols, however, Modbus is used for both command and control and device level communications.

The following highlights the various versions of Modbus as it evolved.

### Modbus ASCII

- Serial RS-232 or RS-485

### Modbus Plus (Modbus+, MB+)

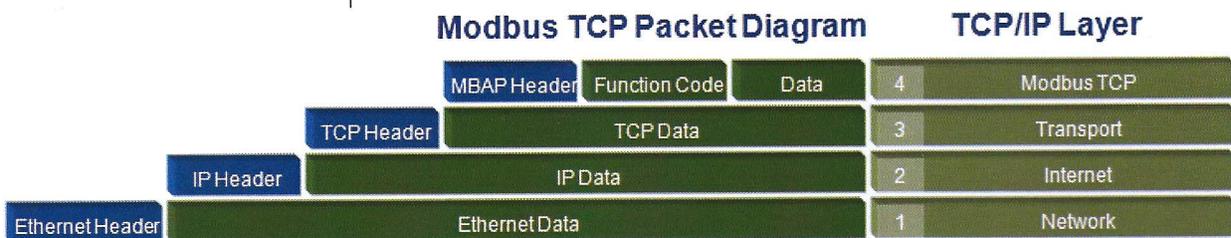
- Proprietary to Modicon
- Twisted pair up to 1 Mb/s
- Uses token rotation

### Modbus RTU (Most common)

- Serial RS-232 or RS-485

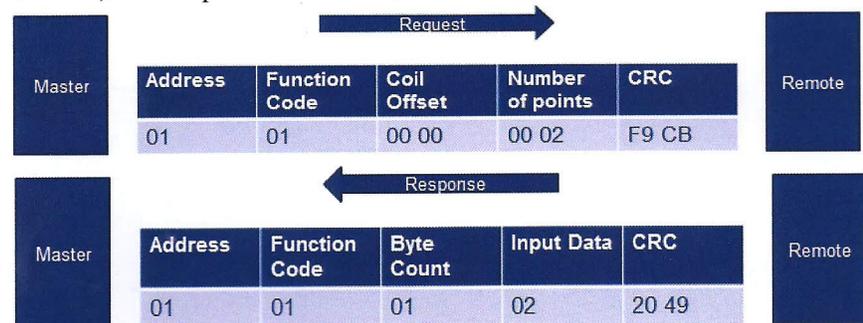
### Modbus TCP

- Transported within TCP/IP data packets
- Uses Port 502



## RTU Modbus Messages

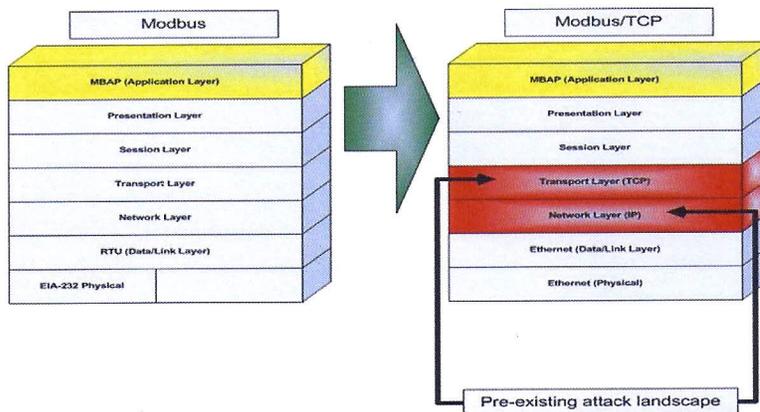
Messages are clear text (easy to view on a protocol analyzer), easy to decode, and require no authentication or authorization.



## Protocol Vulnerabilities: Expediting Attack Success

Vulnerabilities exist in each layer of the OSI stack. TCP/IP, as well as Ethernet, has significant vulnerabilities that facilitate some serious attacks, such as denial of service, session hijacking, routing attacks, impersonation attacks, and others, that directly impact the confidentiality, integrity, and availability of an IT system.

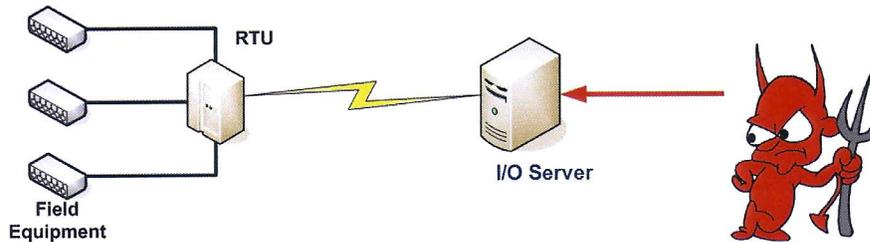
Many of these attacks are based on modifying the Ethernet or IP addresses as well as the TCP port number



- No authentication amongst “isolated” components.
- Modbus/ICCP/DNP3 fully published and open for review.

## Manipulation of the System

*Talk Directly to the Front-End Equipment*



- Attacker establishes presence on control network and issues commands to field controllers.
- No UserID/password required to issue control commands.
- Modbus is a well-understood and documented protocol.

---



---



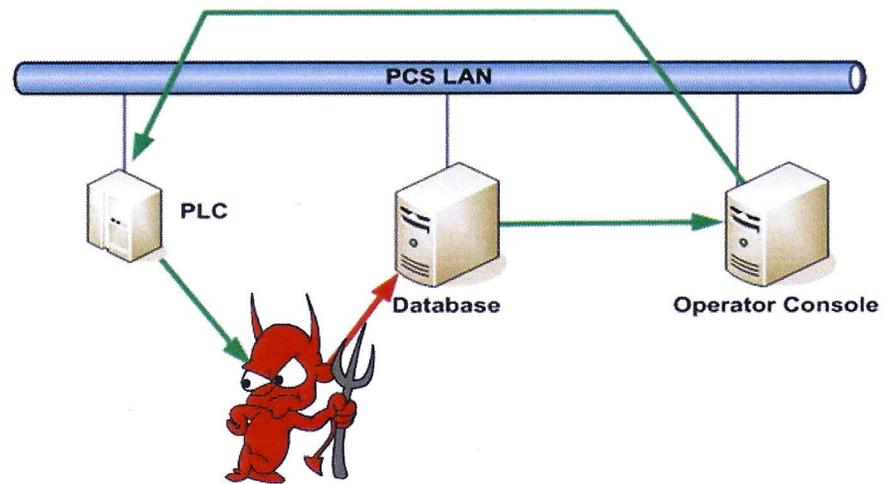
---



---

## Manipulation of the System

### *Changing Data in the Database*



- Attacker intercepts reply messages and makes changes to the message.
- Operator makes changes to the system based on bad data.

## Considerations

There are several basic control system security considerations.

- Knowledge of the process is key for long-term or “surgical” disruption.
- Field equipment generally doesn’t contain process knowledge such as:
  - Breaker 17A supplies power to Brookfield subdivision
  - Valve 4 controls water flows to Zone 18
- Direct access to field equipment without additional knowledge generally only results in nuisance disruption.

## Basic ICS Review

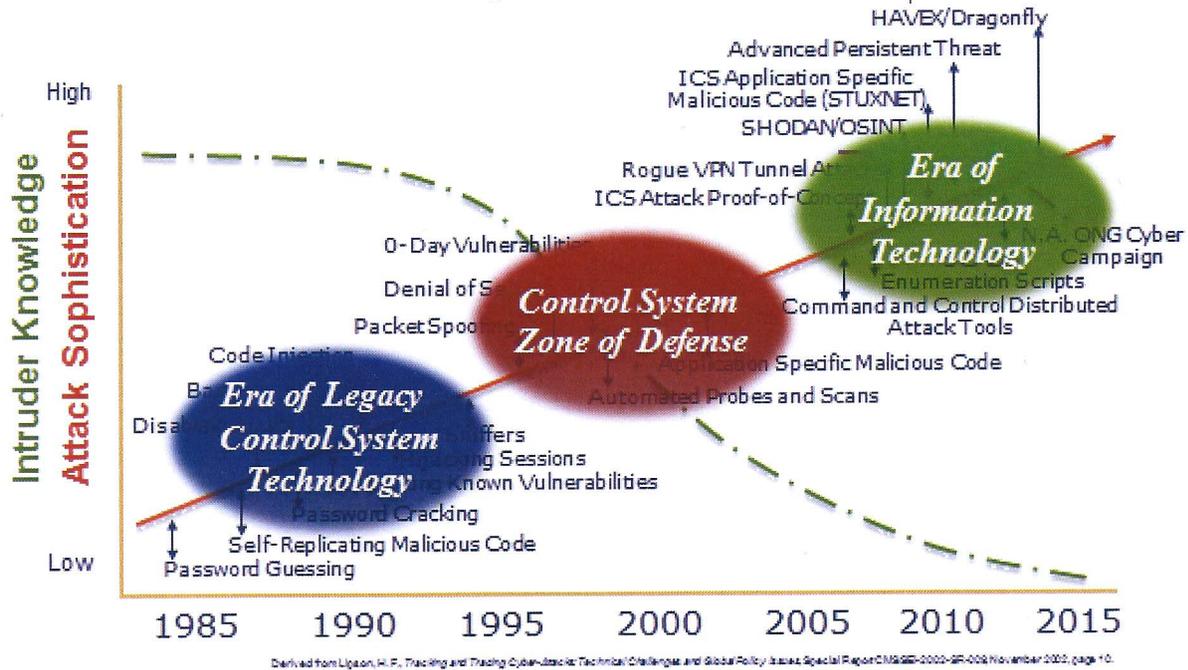
- SCADA and DCS systems are large (geographically) and complex
- Many unique devices are (embedded) connected to these networks
- Communications travel over a variety of physical media and utilize many different protocols
- Reliability and availability are number one.

## LO2: Discuss cyber risks to industrial control systems

## Learning Objective 2

The following section contains information on cyber risks to ICSs.

### Threat Trends for Control Systems

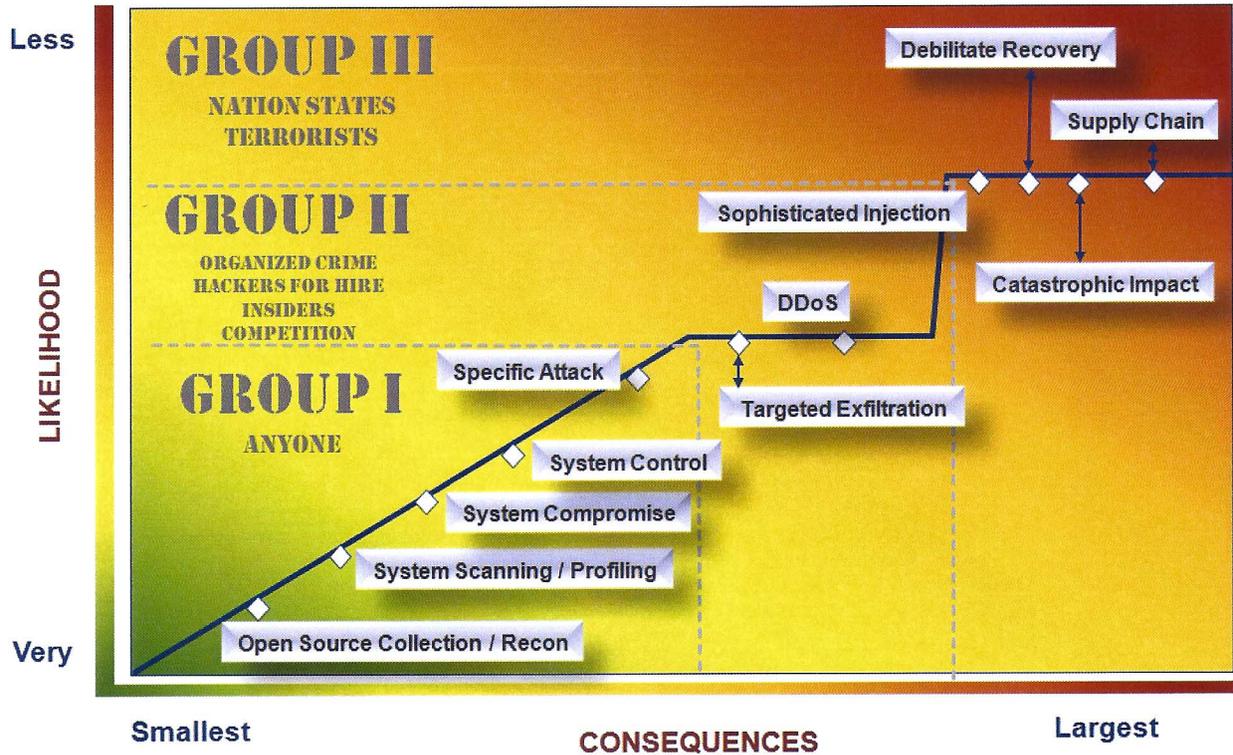


This graph plots the intruder knowledge and attack sophistication over time. The red diagonal line shows that the complexity/sophistication of cyber attacks increase over time. This is obvious because attackers are constantly learning and developing more complex and sophisticated techniques to exploit systems as a result of mitigation strategies that have been developed.

The green curve shows that the knowledge needed by adversaries in general to execute an attack decreases over time. Some advanced knowledge is required to create proof-of-concept code that exploits vulnerabilities, but analysis indicates that those attackers that use precompiled and packaged tools do now need to be skilled to launch sophisticated attacks.

The purple line indicates that these types of attacks on ICSs require a great deal of knowledge to execute. However, as with business systems, code writers will develop tools that will simplify the process of attacking ICSs and thus the knowledge required to execute an ICS attack will decrease.

# The Risk Curve



The risk equation for critical infrastructure is one that involves threat, vulnerabilities, and consequence. We can plot different types of threats and their associated elements against the likelihood of such activities happening. In its simplest form, we can plot consequence against likelihood and then plot the activities of the three types of groups discussed earlier.

On the above graphic, the more benign activities would occur in the bottom left-hand corner of the graph with the most critical actions or consequences in the upper right. As the plot moves toward the top, the top right-hand element of the curve is referred to as the “high impact low frequency” domain.

---

---

---

---

---

---

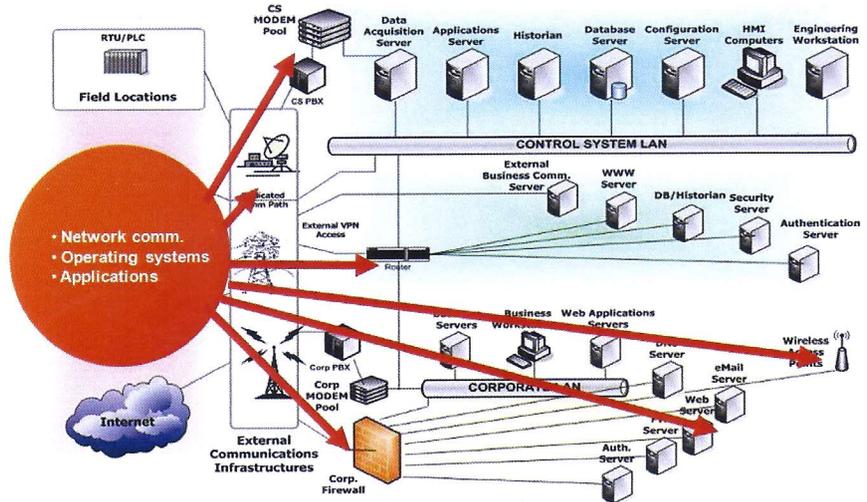
---

---

---

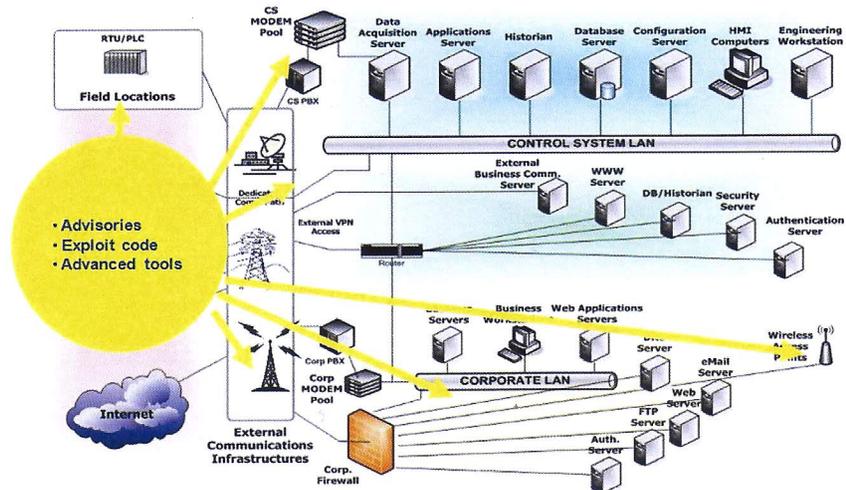
---

## Identify Vulnerable Components



The first step in securing an environment is to identify system components like the OS, applications, or communications that might be vulnerable based on where they are in the network, or what they do.

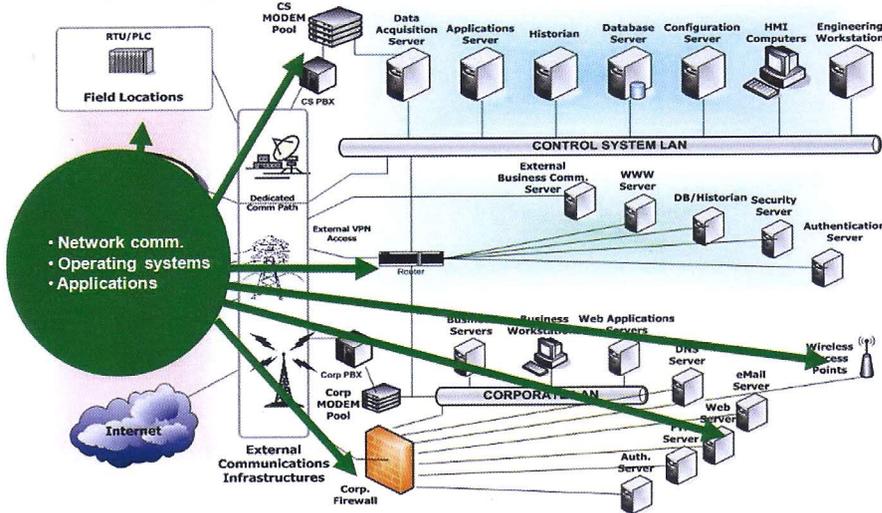
## Identify Threat Vectors



Next, look for the threat vector. Where can the attacker come from?

- Virtual private Network (VPN) connections
- Direct access
- Wireless
- Other network connections
- Dual NIC'd computers.

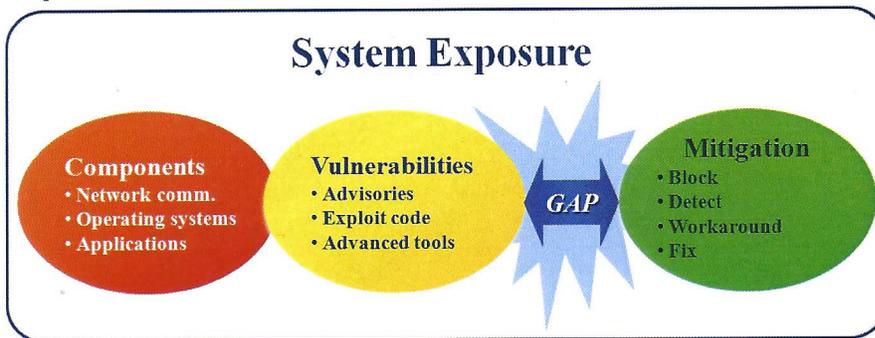
## Identify Mitigations



3

The next step is to mitigate all the vulnerabilities and threat vectors. Implement and follow a patch management strategy. Tighten firewall rules and monitor or remove modems and VPN connections.

## Exposure



4

Exposure is the gap between potential threat vectors and existing defensive capability of the network. By systematically identifying the exposure of a system, a user can start to make intelligent choices about raising the security bar. This in turn can help define a robust and effective cybersecurity strategy for the organization that will provide a balance between business operations and the most applicable defenses.

---



---



---



---



---



---



---

