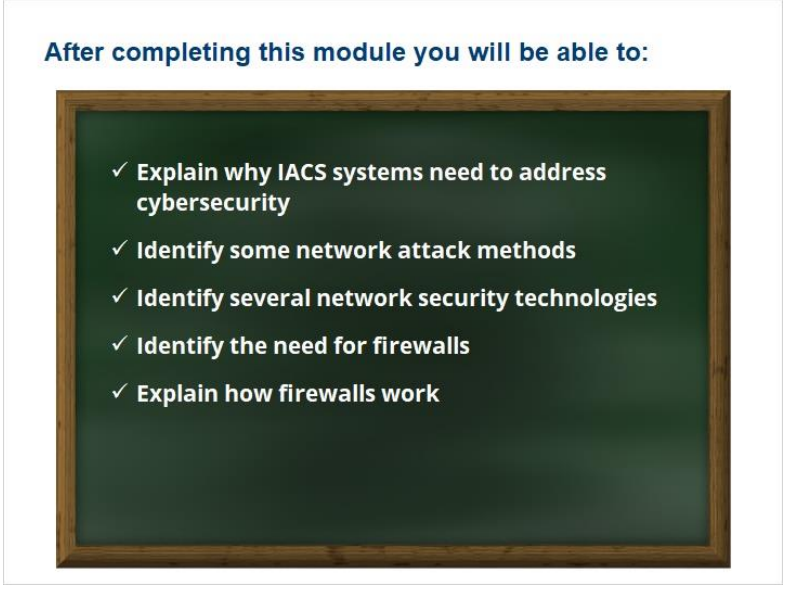
Week 5

Week 5

Week 5

Setting the Standard for Automation™

IC32M Module 7



Fundamental Issue

Network Attack Methods (Threats)

- Known vulnerabilities not patched
- Storms/Floods
- Spoofing
- Man-in-the-Middle
- Replay attacks
- Sniffing
- Session hijacking
- Buffer or stack overflow
- Brute force or dictionary

Notes:

- There are numerous ways in which a network can be attacked. A broadcast storm or flood can be instigated for the purpose of a denial of service (DOS). Other ways networks can be attacked is by taking advantage of known vulnerabilities in operating systems and applications.
- Some examples of attacks using known vulnerabilities are:
- **Smurf** sends a large amount of ICMP Echo Requests (ping) traffic to a broadcast address, with each ICMP Echo packet containing the spoof source address of the victim host. When the spoofed packet arrives at the destination network, all hosts on the network reply to the spoofed address. The initial Echo Request is multiplied by the number of hosts on the network which generates a storm of replies to the victim host tying up network bandwidth, using up CPU resources or possibly crashing the victim.
- **Fraggle** is essentially a rewrite of Smurf.
- A **LAND** attack is a denial of service attack that consists of sending a special poison spoofed packet to a computer, causing it to lock up. The security flaw was actually first discovered in 1997 by someone using the alias "m3lt" and has resurfaced many years later in operating systems such as Windows Server 2003 and Windows XP SP2.
- **A Teardrop** attack involves sending mangled IP fragments with overlapping, over-sized payloads to the target machine. This can crash various operating systems because of a bug in their TCP/IP fragmentation re-assembly code.
- **Spoofing** is a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host.

Network Security Technologies

Network Security Devices

- ✓ Switches/Routers
- ✓ Firewalls
- ✓ Unidirectional Gateways (Data Diodes)

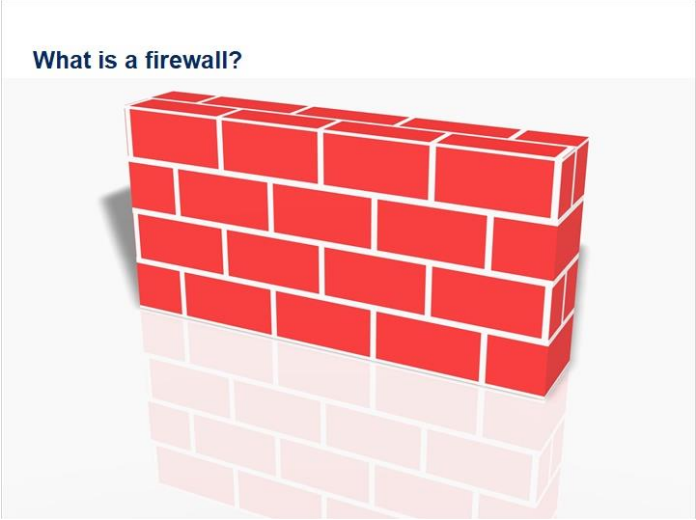
Network Architectures

Cryptography

- ✓ VPN
- ✓ Hashes
- ✓ Secure Protocols

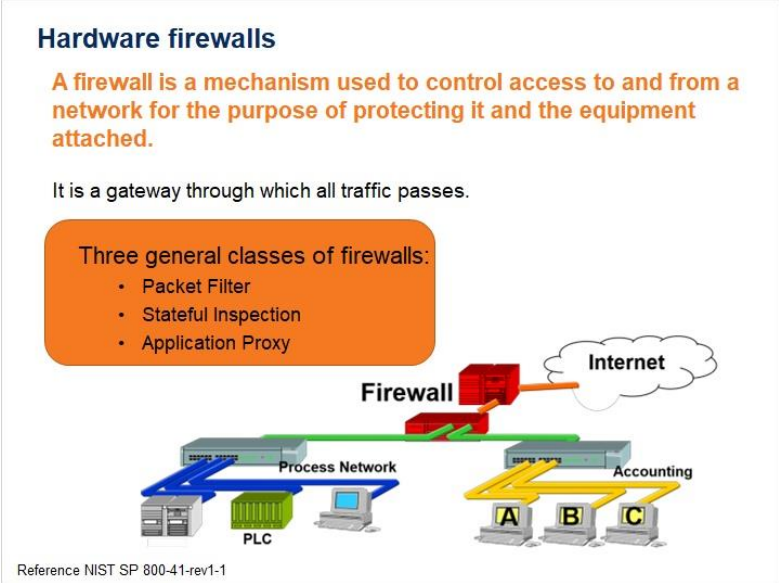
Intrusion Detection Systems

- ✓ Network
- ✓ Host



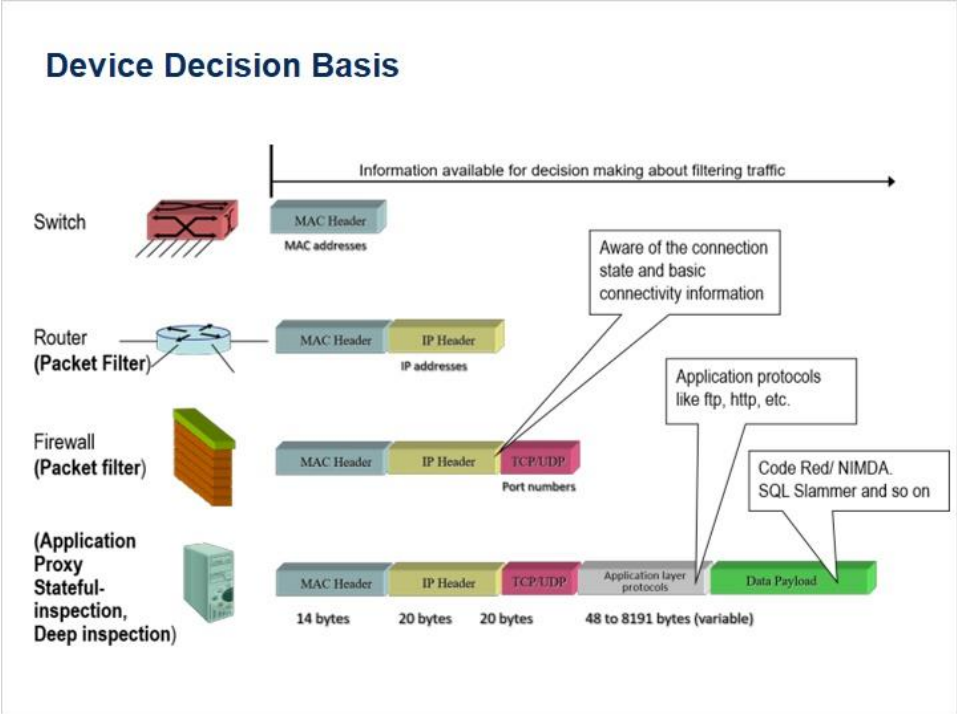
Notes:

- ISA99 Master Glossary definition:
    - A firewall is an inter-network connection device that restricts data communication traffic between two connected networks
- NOTE: A firewall may be either an application installed on a general-purpose computer or a dedicated platform (appliance), that forwards or rejects/drops packets on a network. Typically, firewalls are used to define zone borders. Firewalls generally have rules restricting which ports are open.



Notes:

- Packet Inspection Firewalls work at the Network level (Layer 3):
    - Examines only the headers of each packet of information (source, destination, function)
    - Accepts or rejects based on ACL's
    - Pros: Fast and cheap
    - Cons: only looks at header info
- Stateful Inspection
    - Tracking the relationships between packets in a session
    - Inspecting the packet's structure and sequence
    - Can be either hardware-based (e.g. Cisco ASA, Tofino) or server-based (e.g. CheckPoint Firewall-1).
    - Pros: Relatively Fast, Flexible, Improved Security
    - Cons: Overall network performance cost; false sense of total security; may need to consider Application level appliance
- Proxy Firewalls are basically working at the Application Level
    - Firewalls act as an intermediary that accepts connections and requests from a client and then issues them.
    - Basically, interprets every incoming packet up to the application layer, checks it and then reissues it to the target device.
    - Pros: Very strong security model
    - Cons: Slower and process intensive
      Only handles well-known services (web traffic or email) and not industrial protocols
    - Generally, not an option for control systems (exception is special purpose gateways)

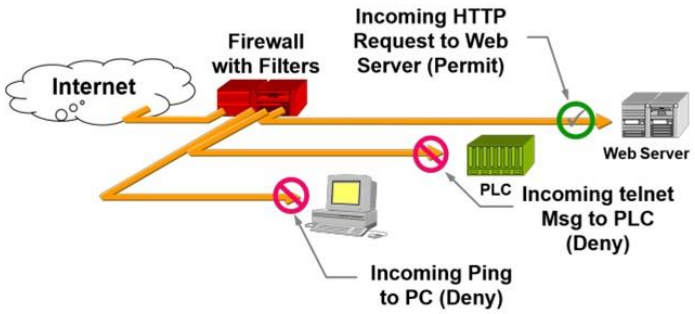


Notes:

- The more sophisticated the checking performed, the greater the delay (latency) introduced and the greater processing overhead required
- We need to be focused on what we need to do, then pick the right appliance that will help us get it done.

Firewall Policy

A firewall is relatively easy to install
Configuring is more difficult
Deciding how it should be configured is most difficult
A firewall is only as good as its rules



IACS Firewall Configuration Best Practices

Default rule

- Block all traffic by default
- Explicitly allow only specific traffic to known service
- Ingress and Egress (inbound and outbound)
- IACS devices should not be allowed to access the Internet
- Prevent traffic from transiting directly from the IACS network to the enterprise network

Clean up unused rules

Rules must be exhaustively tested before deployment

Management/Out of Band ports secured

This list is not all inclusive

1.15 IACS Firewalls

IACS Firewalls

Companies offering IACS firewalls to protect traditionally vulnerable components such as PLCs and DCS controllers

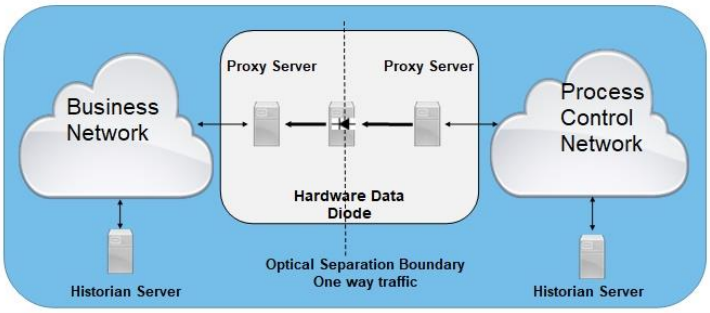
- Industrial form factor and robustness
- Electrician / Control Tech friendly
- Knowledge of industrial protocols
- Extensibility beyond just packet filtering

Sample of IACS Appliance Vendors:

- Tofino (Belden)
- Hirschmann Eagle (Belden)
- Moxa EDR-8xx and EDR-G9xx series
- Secure Crossing Zenwall Line (5, 10, 2500, etc)
- mGuard (Phoenix Contact)
- Scalance S (Siemens)
- Connexium (Schneider Electric)

Unidirectional Gateway (a.k.a. Data Diode)

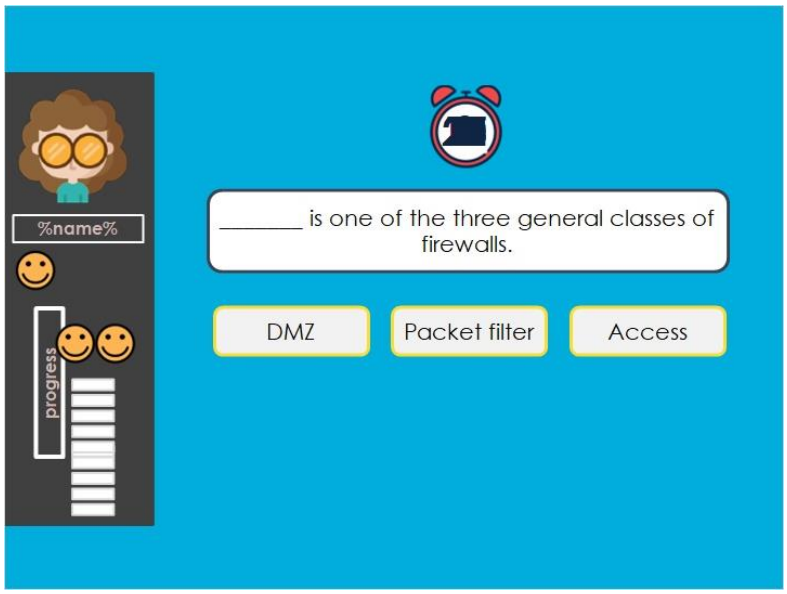
- Network device allowing data to travel only in one direction
- Normal flow control SYN ,SYN-ACK, ACK must be emulated
- Defense and nuclear power plants
- Finding their way into IACS



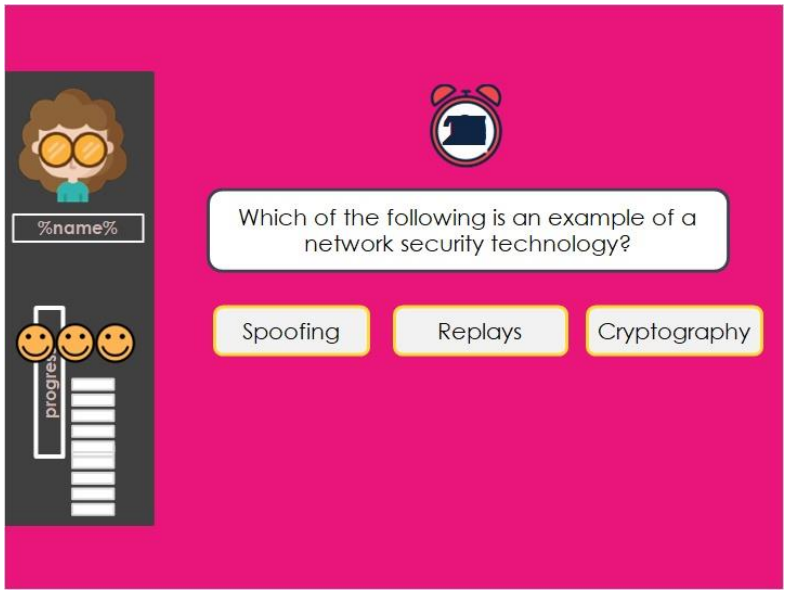
Notes:

- A data diode is more secure than a firewall but far less flexible
- can also support TCP transmission
- data diode devices can only transmit data in a single direction,
- normal flow control that is typically handled by the TCP layer in a TCP/IP network must be emulated
- Thus more equipment (servers, clients) deployed and all require care and feeding
- provide armor for one attack vector: the network.
- they impose a level of difficulty in performing occasional, yet routine, tasks that generally doesn't justify the purported increase in security over a well-managed firewall.

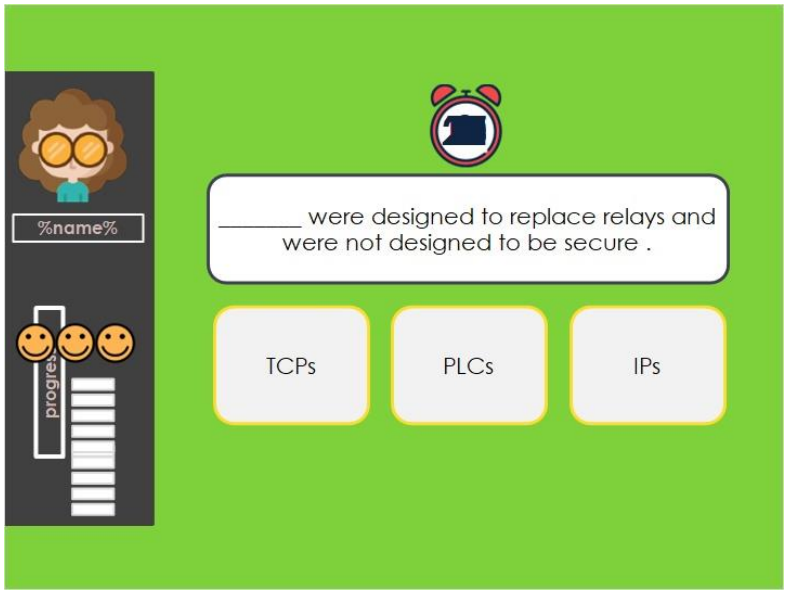
- benefit of data diodes over firewalls is they **almost** remove the negligent user and developer factor.
- Waterfall, OWL among list of vendors



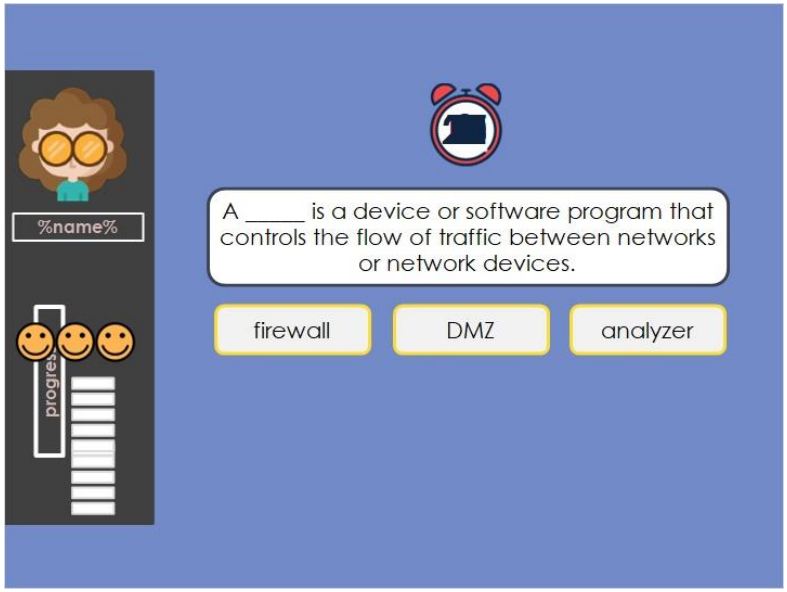
Correct	Choice
	DMZ
	Access
X	Packet filter



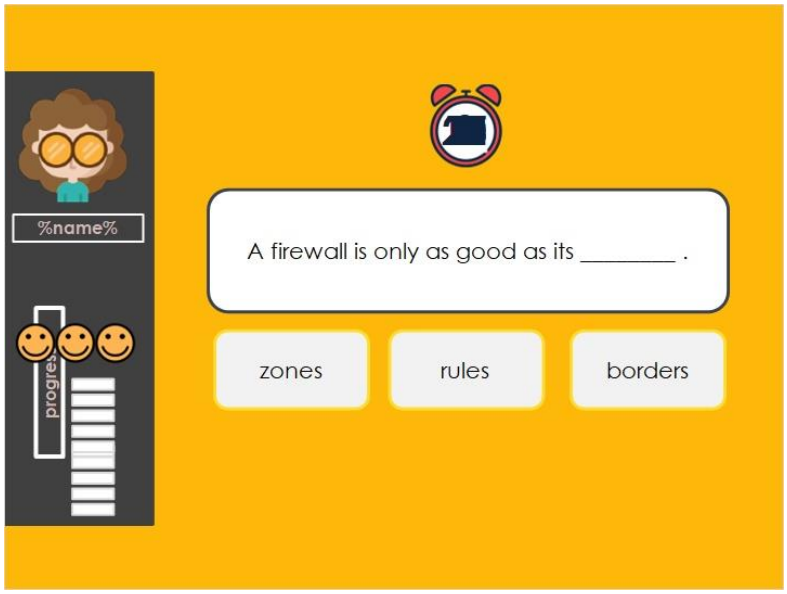
Correct	Choice
	Spoofing
	Replays
X	Cryptography



Correct	Choice
	TCPs
	IPs
X	PLCs

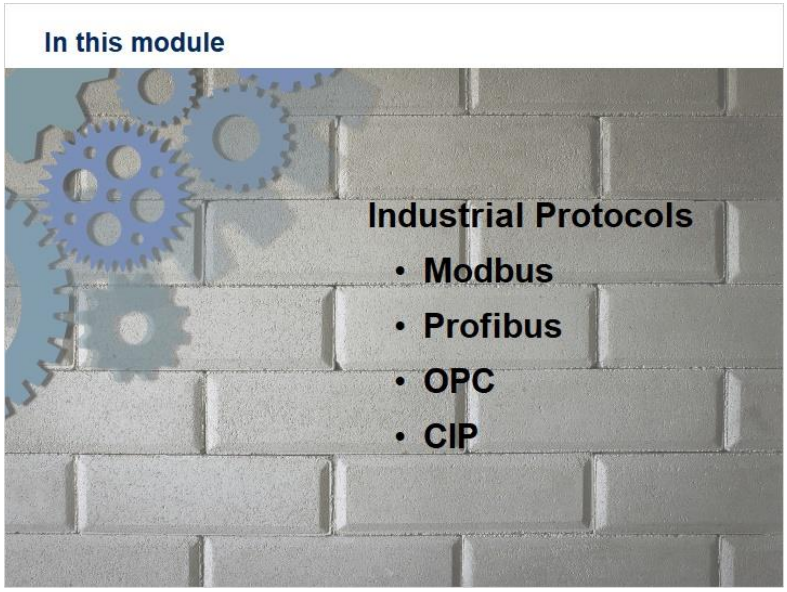


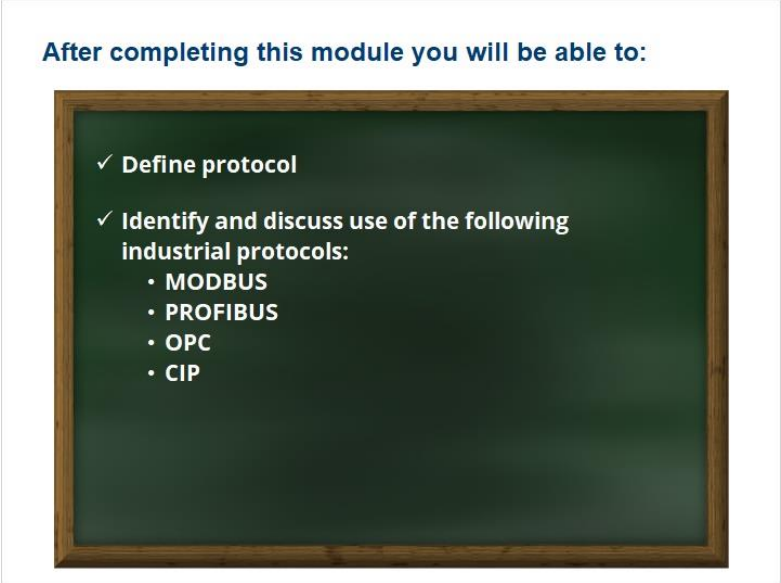
Correct	Choice
	DMZ
	analyzer
X	firewall

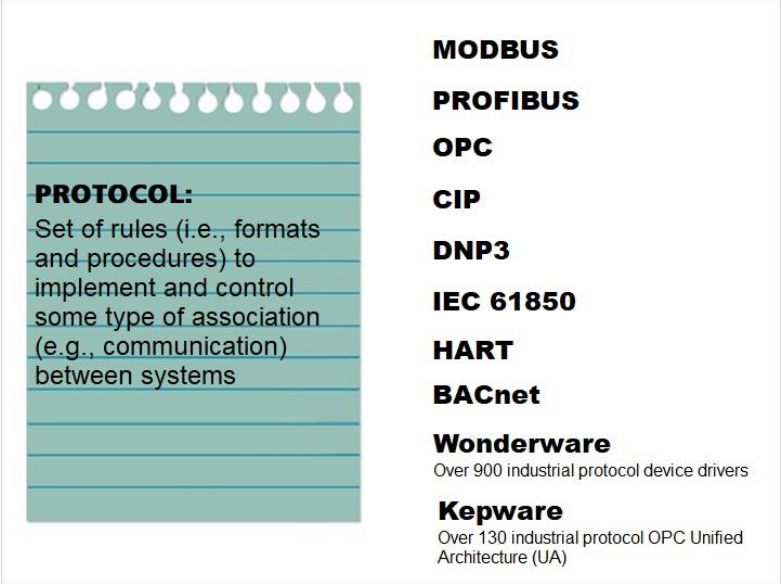


Correct	Choice
	zones
	borders
X	rules

IC32M Module 8



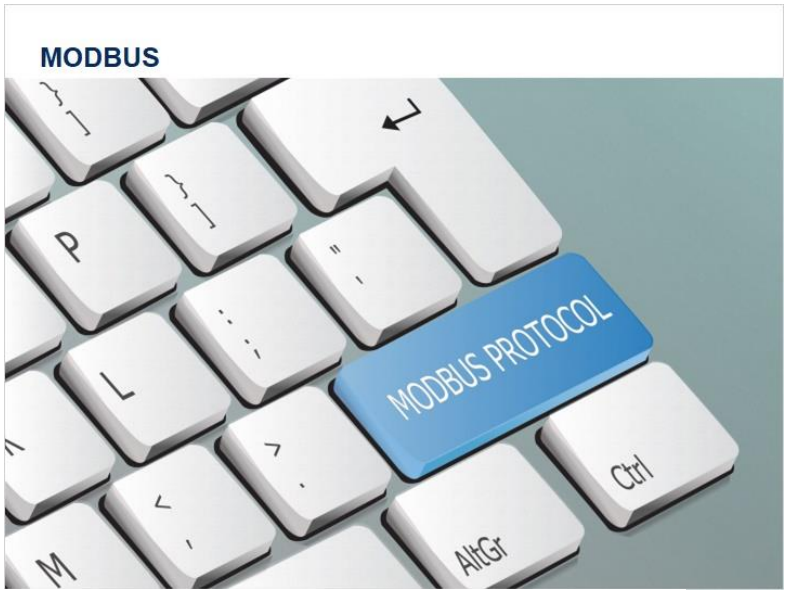




Notes:

- Protocol defined in ISA99 master glossary as “set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems” (retrieved 8 Dec 2016)
- Depending on the definition of “Industrial Protocol” or “Automation Protocol” there are over 80 protocols listed in various web sources such as wiki, digitalbond, vendor sites
- We shall take a high level look at four of the popular IACS protocols
- Depending on what type of IACS you support you may need to look up the protocols that are popular in your world

---

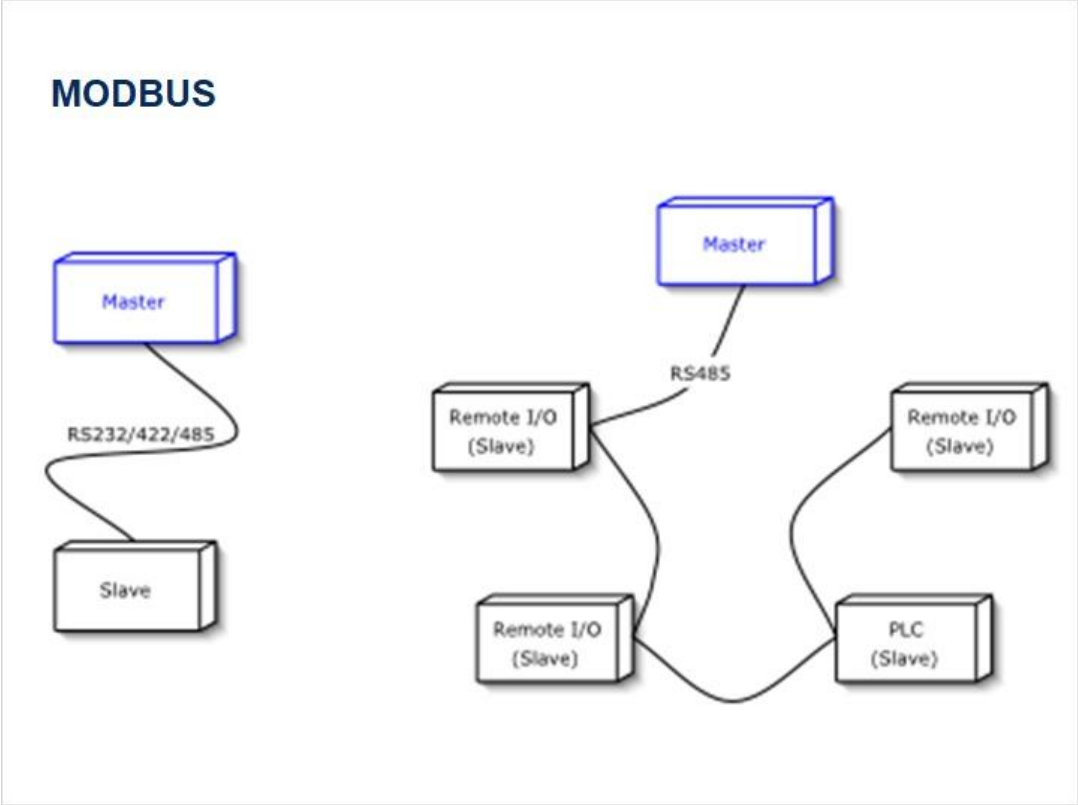


MODBUS

- Serial communications protocol originally published in 1979 by Modicon (now Schneider Electric)
- De facto standard, openly published and royalty free
- Widely used network protocol in the industrial manufacturing environment (over 7 million nodes)
- Basic functions support reading and writing of PLC registers and I/O
- Caution----Variants exist

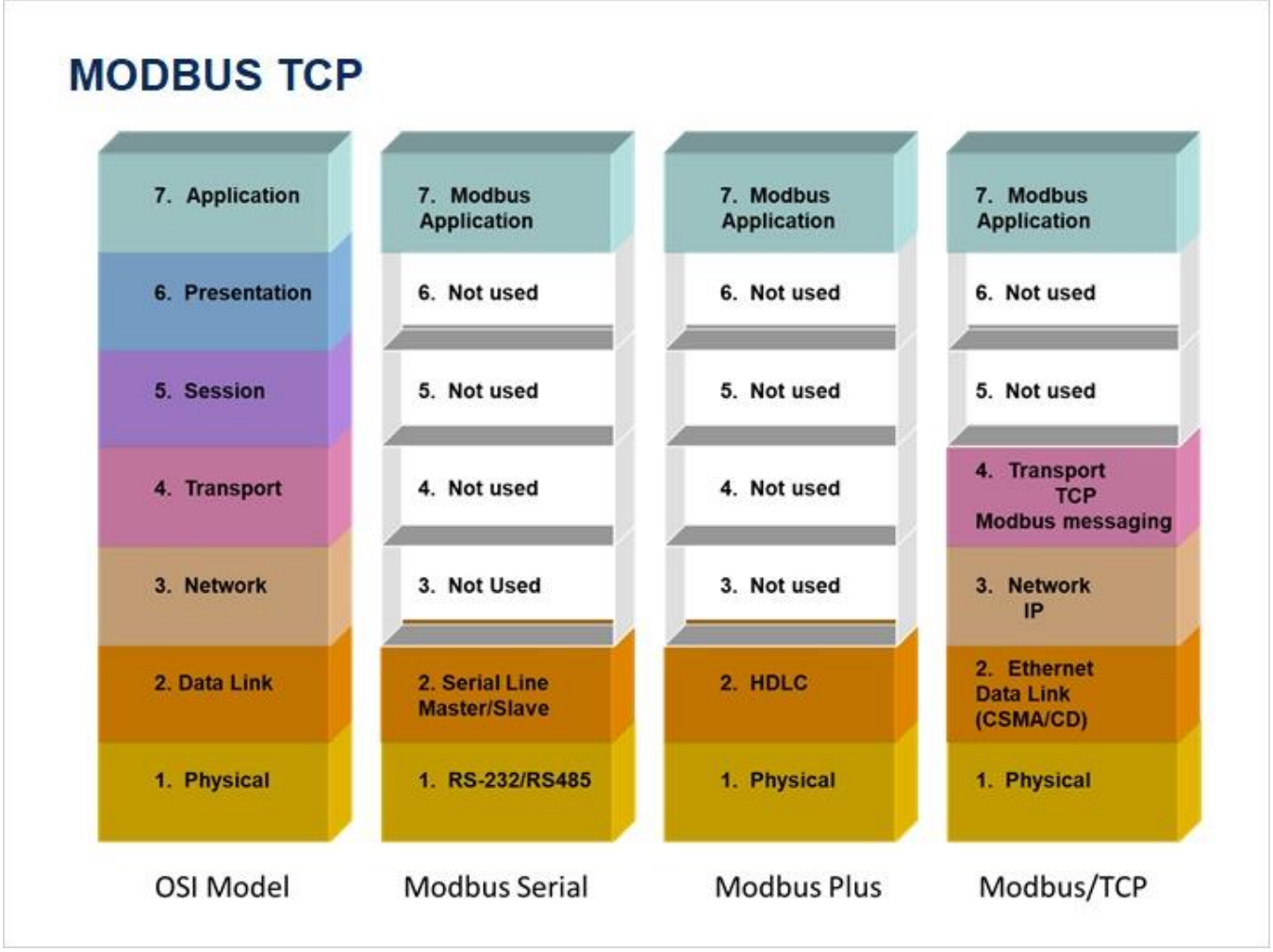
Notes:

- Discuss “Variants exist” using following info
- Modbus doesn’t define exactly how the data is stored in the registers
    - High bytes or low bytes first?
    - It doesn't matter which order the bytes or words are sent in as long as the receiving device knows which way to expect it
- Enron Modbus is a modification developed by Enron
    - Support of 32 bit registers as well as 16 bit
    - Ability to transmit Event logs and Historical data
- Semiconductor industry has implemented a Network Communication Standard and an Object Messaging Protocol using Modbus TCP/IP
- 7 million node number comes from http://www.modbus.org/faq.php (retrieved 8 Dec 2016)
- Building, infrastructure, transportation and energy applications also make use of Modbus



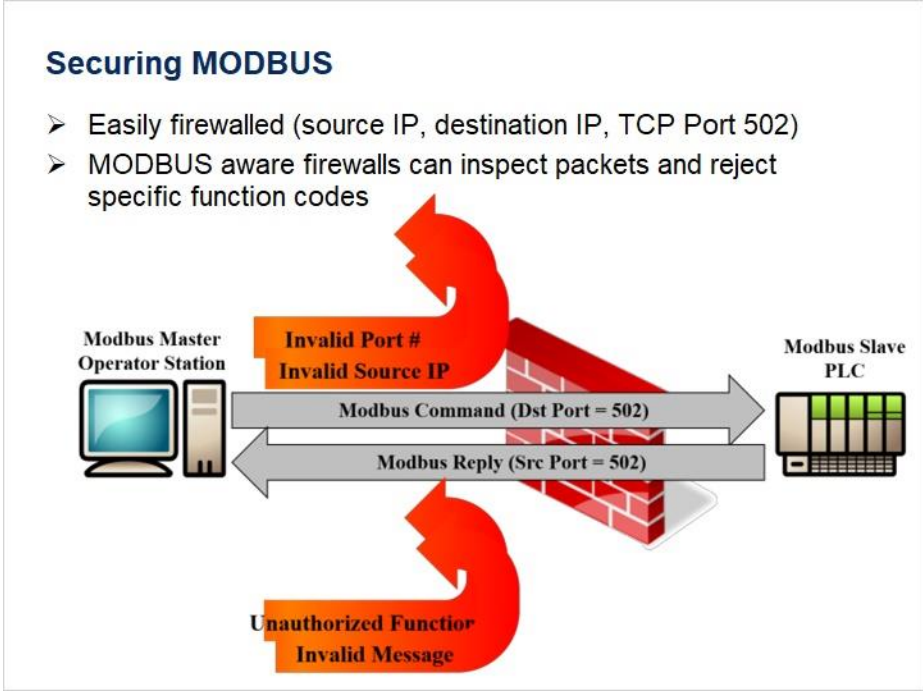
Notes:

- master-slave/client-server communication between intelligent devices
- Versions of the Modbus protocol exist for serial lines (Modbus RTU and Modbus ASCII) and for Ethernet (Modbus TCP)
- There are pros and cons for each of the protocols that are left to the student to explore



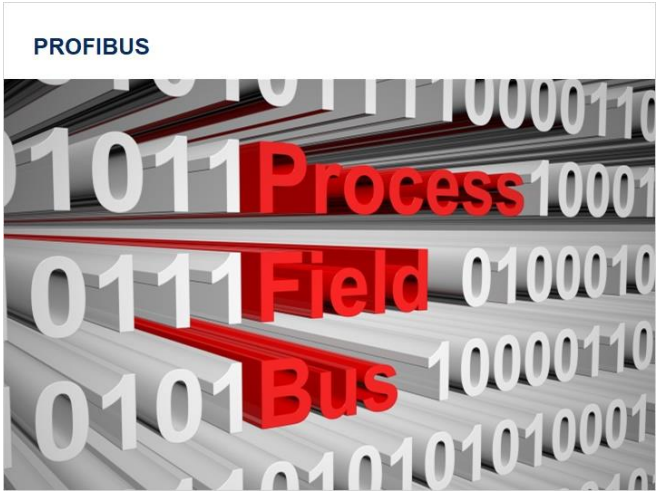
Notes:

- Modbus can run over any serial type media (copper, fiber, wireless, modem, etc..)
- Modbus is a serial master/slave protocol, however....
    - Modbus Plus is a peer-to-peer protocol which runs at 1 Mbp.
    - The Modbus Plus protocol specifies the software layer as well as the hardware layer
    - Proprietary cabling and terminators must be used with a Modbus Plus network
- ModbusTCP/IP is an EtherNet based protocol
    - ModbusTCP/IP products act in a master/slave capability



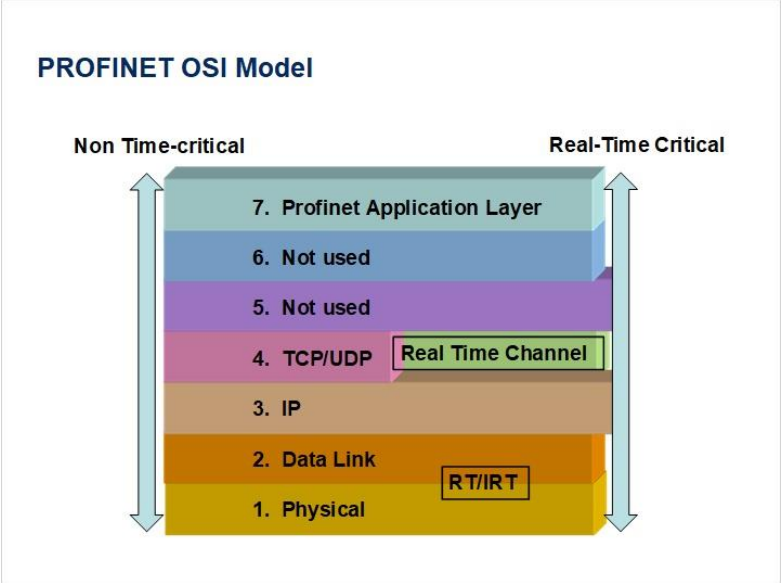
Notes:

- Modbus can be secured
- UDP port 502 not common



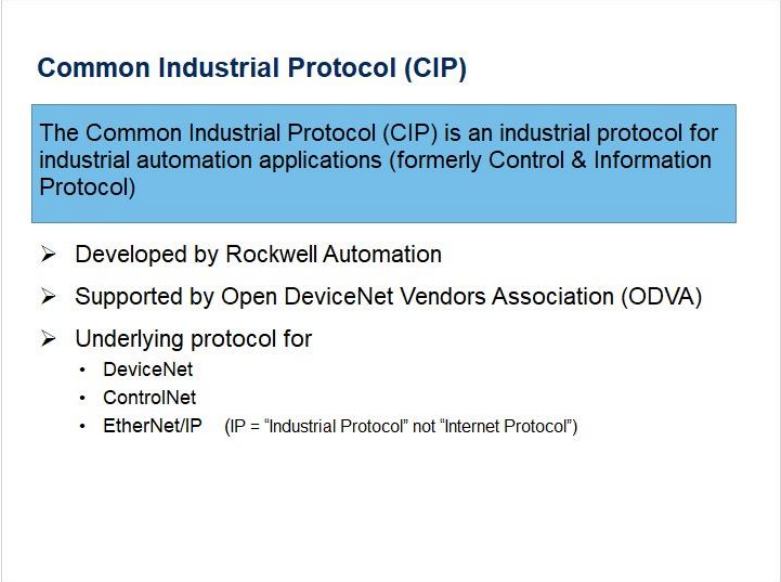
Notes:

- Profibus-DP (Distributed Peripherals) RS-485
- Profibus-PA (Process Automation) IEC 61158-2
- PROFIsafe (PROFIBUS safety or PROFINET safety) is a safety communication technology for distributed automation IEC 61508
- PROFINET provides a high-speed, high-bandwidth, backbone

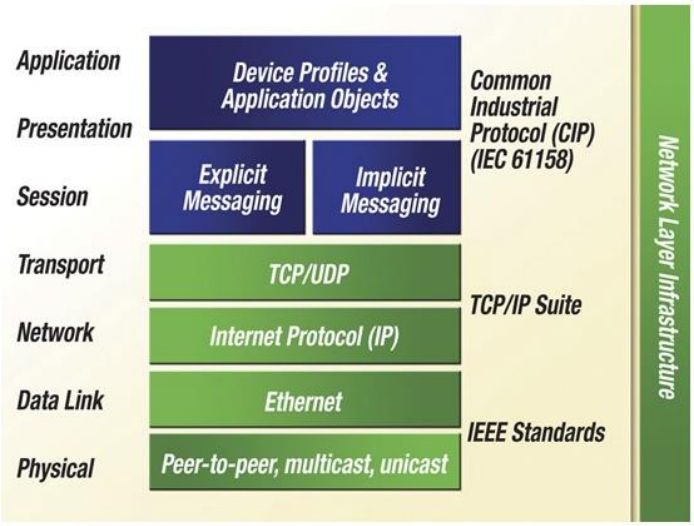


Notes:

- SEMI = Semiconductor Equipment and Materials Institute
- Isochronous Real Time (IRT) provides the highest degree of real time capability required for Motion Control
    - Max cycle time of 1 msec and a jitter max of 1 µsec



EtherNet/IP OSI Model



Ethernet/IP

Uses two communications mechanisms and two ports

Implicit Messaging

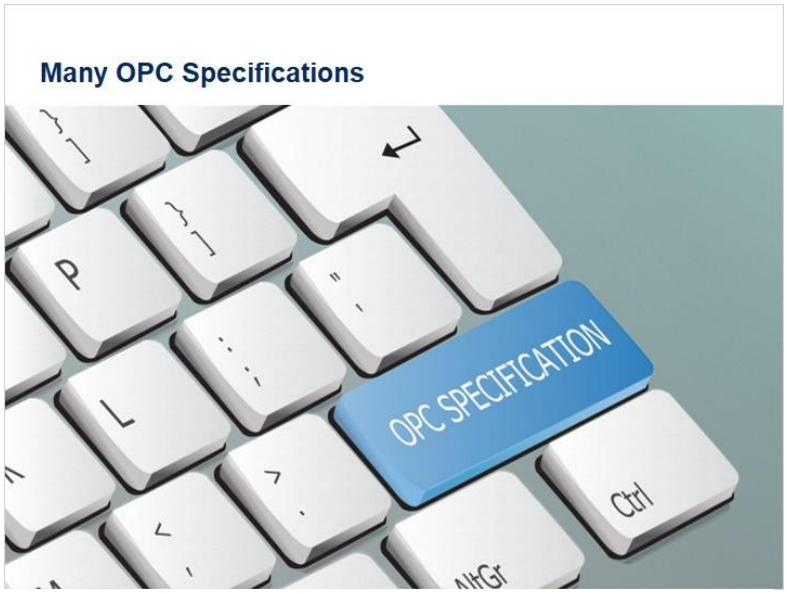
- ✓ Port 2222
- ✓ Producer/Subscriber
- ✓ Typically I/O messages
- ✓ Uses UDP Multicast and Unicast for I/O transfer

Explicit Messaging

- ✓ Port 44818
- ✓ Client Server – HMI to PLC
- ✓ Uses TCP Unicast for administration and data transfer

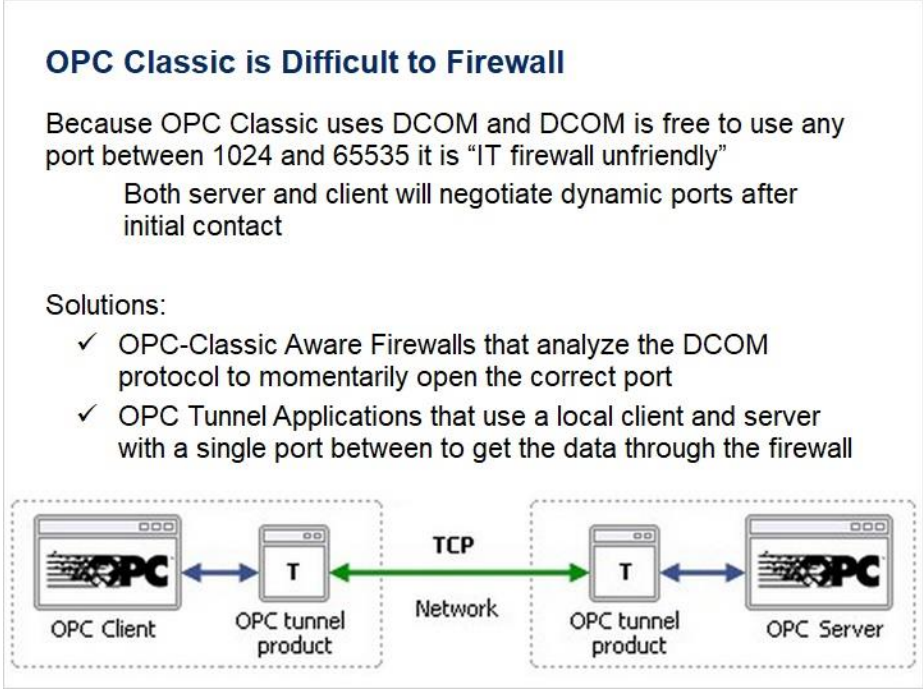
OPC

- Initially Object Linking and Embedding (OLE) for Process Control
- Today the acronym OPC stands for Open Platform Communications
- Communication standard developed in 1996 by an industrial automation industry task force
- Based on Microsoft OLE, COM, and DCOM technologies
- Specifies the communication of real-time plant data between control devices from different manufacturers
- The OPC Foundation maintains the standard



Many OPC Specifications

- ✓ OPC Data Access (a.k.a. “OPC Classic”)
- ✓ OPC Alarms and Events
- ✓ OPC Batch
- ✓ OPC Data eXchange
- ✓ OPC Historical Data Access
- ✓ OPC Security
- ✓ OPC XML-DA
- ✓ OPC Unified Architecture (UA)

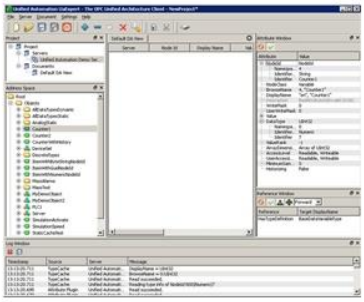


Notes:

- Just think of asking your firewall wall guy or gal to open up 64 thousand ports at one time
    - It will probably not happen
- OPC UA (Unified Architecture) overcoming deficiencies
    - Firewall-friendly while addressing security concerns by providing a suite of controls
    - Platform independent
    - Operating System independent
    - COM OPC Classic specifications are mapped to UA
    - Encryption, authentication, and auditing
- OPC UA is assigned TCP/UDP port 4840
- However, tunneling is still recommended

OPC Unified Architecture

- Not using DCOM anymore, just normal sockets using one (1) port
  - OPC directly on the IACS device
  - Siemens, Rockwell and other have OPC Servers directly on the device
- A Browsable Namespace with
  - Folders
  - Classes
  - Objects
  - Methods
  - Objects
- Companion Specifications
  - Specific namespaces
  - Like XML Schema Definitions



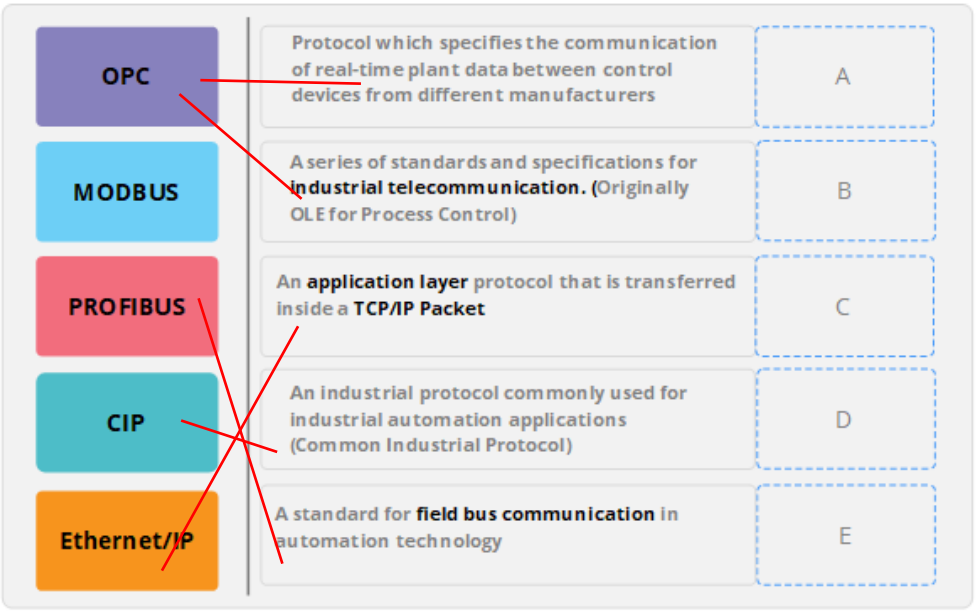
OPC Unified Architecture

Designed from the ground up to be secure

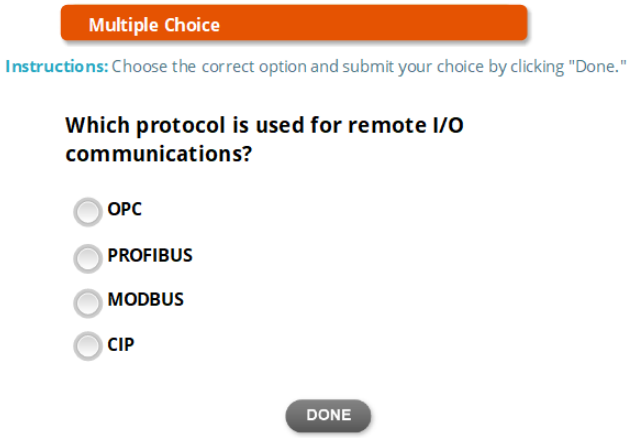
- ✓ Session Encryption: messages are transmitted securely at 128 or 256-bit encryption levels
- ✓ Message Signing: messages are received exactly as they were sent
- ✓ Sequenced Packets: exposure to message replay attacks is eliminated with sequencing
- ✓ Authentication: each UA client and server is identified through OpenSSL certificates providing control over which applications and systems are permitted to connect with each other
- ✓ User Control: applications can require users to authenticate (login credentials, certificate, etc.) and can further restrict and enhance their capabilities with access rights and address-space “views”
- ✓ Auditing: activities by user and/or system are logged providing an access audit trail

Knowledge Check

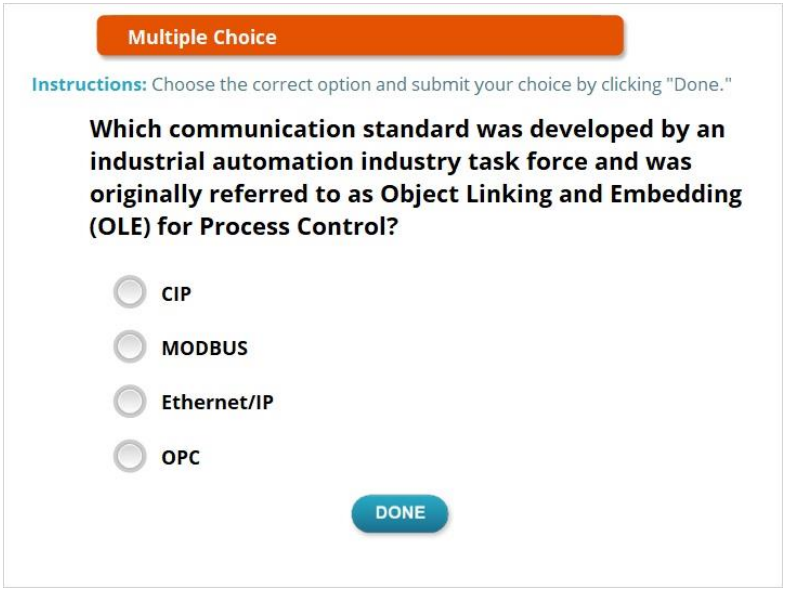
Drag each protocol to its matching definition.



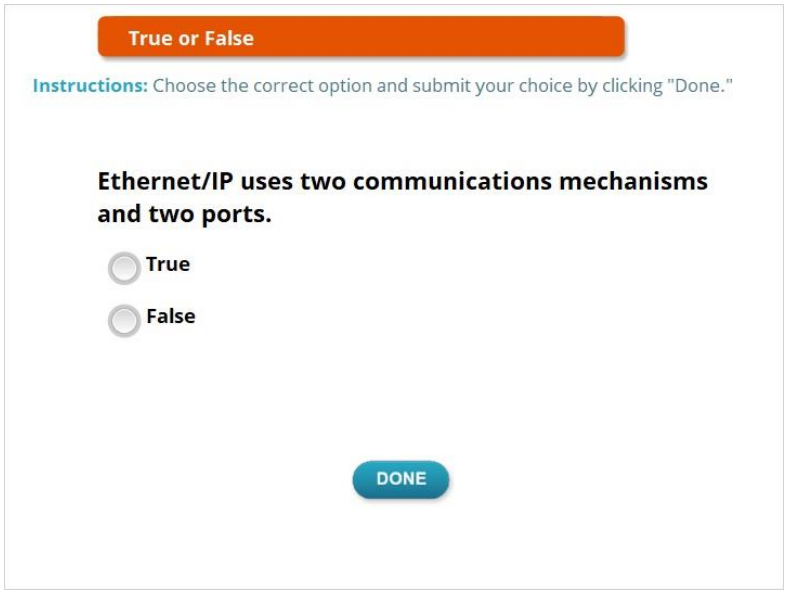
Drag Item	Drop Target
OPC	B
MODBUS	A
PROFIBUS	E
CIP	D
Ethernet/IP	C



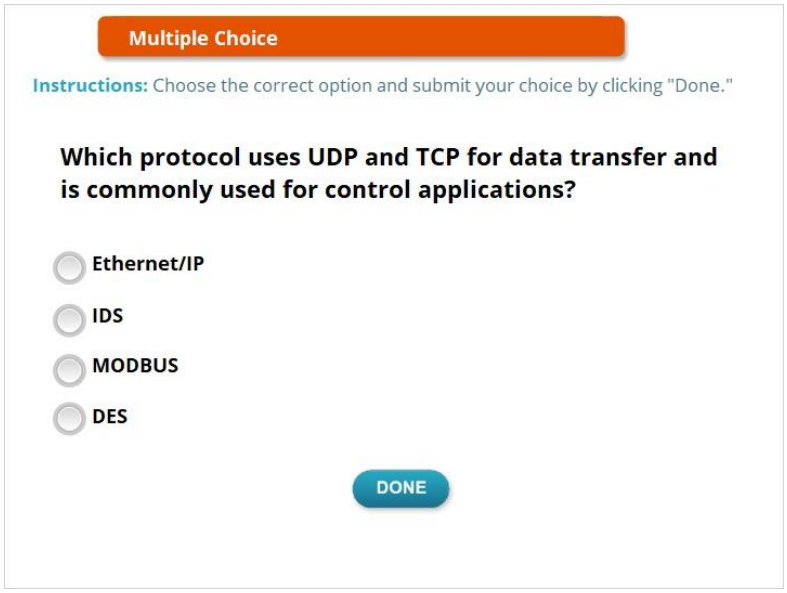
Correct	Choice
X	Radio Button 3



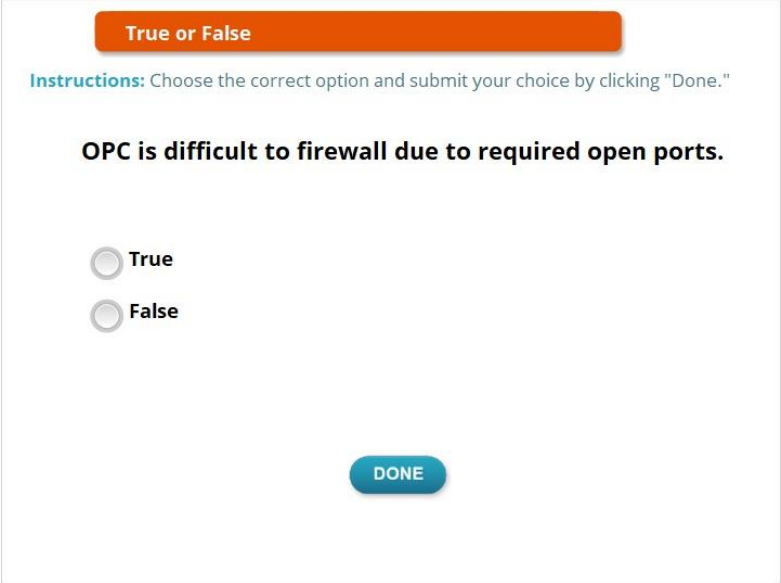
Correct	Choice
X	Radio Button 4



Correct	Choice
X	Radio Button 1



Correct	Choice
X	Radio Button 1



Correct	Choice
X	Radio Button 1

8.0

Ethernet Industrial Protocols, Fieldbuses, and Legacy Networks

I can't tell you how many times over the years I've had someone ask "what is the best Ethernet protocol?" That's like asking who has the best pancakes, what is the most exciting sporting event, and what is the best Christmas movie of all time? (FYI, the answers are: 1. Pancake Place in Green Bay, Wisconsin, 2. NCAA Basketball Tournament, and 3. *It's a Wonderful Life*.)

The truth, of course, on the question of factory floor protocols is simply "it depends." Do you want to move I/O data or information? How fast do you need to move the data? How much data do you need to move? How many devices have the data now? There is no end to the questions you should ask and answer.

In practice, it is not that complicated. In the great majority of cases, it just comes down to the brand of programmable logic controller (PLC) used in your building, or used by the majority of your customers, that drives the Ethernet protocol. If you are using Siemens PLCs, the "best" Ethernet protocol is PROFI-

NET IO. If you're using a Rockwell ControlLogix or CompactLogix, it is EtherNet/IP. If you want to keep everybody happy, or at least not too unhappy, use Modbus TCP.

From a purely technical standpoint, Ethernet and any of these Ethernet protocols are not necessarily more ideal for automation applications than any other network. Even if there was one that was superior to the others, the nature of capital equipment is still such that no one is going to rip out existing equipment and wiring just because something better exists.

But ignoring the PLC brand issue, there is a series of questions that you could ask to determine if you should use an Ethernet protocol or another type of industrial communication system (CAN, Modbus Serial, PROFIBUS DP, etc.). These questions include:

- What is the distance requirement?
- What kind of physical cabling arrangement makes sense for this application? All the Ethernet formats except 10BASE2 and 10BASE5 use a star topology. This is fine for applications where devices are clustered together in groups but for others, such as a long conveyor with many nodes spaced 20 m apart, it is quite inconvenient. For the conveyor, a trunk/drop topology (such as that used by DeviceNet™ and CANopen) is much better.
- What is the actual speed (response time) requirement for the most time-critical devices? Do all of the devices require that level of speed or should some devices have a higher priority than others?
- Does your application require that you prioritize messages?

- Do the devices you want to use support the same network standard? Are there open versus closed architecture considerations?
- If you are developing a network-capable product, what is the hardware bill of materials and the cost of software development for that network?
  - How much electrical noise is present in the application and how susceptible is the cabling?
  - What is the maximum required packet size for the data you are sending? If the data can be fragmented over several packets, how fast does a completed message have to arrive?
  - What types of device relationships are desired (master/slave, peer-to-peer, broadcast)?
  - Does the network need to distribute electrical power? If yes, how much current?
  - What kind of fault tolerance must be built into the network architecture?
  - What is the total estimated installed cost?

With the answers to these questions you can make a reasonably good choice on an industrial networking protocol.

8.1 The Two Most Important Points to Understand

This chapter describes the leading industrial automation protocols. To understand those protocols, you need to understand two key points that apply to all industrial Ethernet protocols. The first key point is that the most important differentiator from one Ethernet protocol to another is the data representation. The data representation—how data is organized in

devices and implemented in the address space of the protocol—is what makes the protocol unique. It is the key to a genuine understanding of any of these technologies. Everything else that describes the protocol—how data is transported, how connections are made, and what services exist to provide one device (usually the client) with access to the data in the address space of another device (usually the server)—is actually similar from protocol to protocol. For example, both EtherNet/IP and PROFINET IO use synchronous messaging and both EtherNet/IP and Modbus TCP make more extensive use of TCP. There are a lot of commonalities but the way data is accessed in the address space of a device is the key differentiator.

The second key point is that industrial Ethernet protocols are simply a way of defining messages that pass through the "pipe" known as the *TCP/IP stack*. You can think of a TCP/IP connection between two devices as a phone connection. The connection can exist even if no one is talking (sending data) over the connection. That is why these Ethernet protocols are known as *application layer protocols*, they are the "applications" that uses the TCP/IP stack.

Each of the industrial protocols make use of the TCP/IP stack and TCP/IP connections in different ways, but they all send messages through the pipe in one way or another. All protocols use the IP layer. Some solely use TCP (Modbus TCP), some use both TCP and UDP (EtherNet/IP), and one uses TCP but also has another channel that bypasses the TCP/IP layer.

When reading the following sections on these Ethernet application layer protocols, make special note on how the data is organized, the object model of the protocol, and how each protocol makes use of the services of the TCP/IP stack.

8.2 Modbus and Modbus TCP

Saying that you want to discuss Modbus can sometimes bring to mind chats about buggy whips, the rotary telephone, or that new innovation, the color television. What is there to say? What hasn't been said about Modbus over the last 40 years?

Modbus is hardly a new technology. Historians can disagree about its actual birth, but it is certainly a product born in the 1970s. Success is such a trite word for how well it has done over those 40 years. Modbus has found its way into hundreds of thousands—if not millions—of devices. You can find it in everything from valve controllers, to motor drives, to human-machine interfaces (HMIs), to water filtration systems. It would be difficult indeed to name a product category in industrial or building automation that does not use Modbus.

Yet even in the automation world, Modbus isn't just old technology. ***It is ancient technology.*** Modbus is like that lovable old uncle that comes over every Thanksgiving. He's retired now, he putters around his garden, he's no longer the handsome debonair man of 40 years ago, but he's there when we need him and that is why we love him.

Prior to Modbus, all we had was electrical signaling. Modbus changed that. In fact, Modbus changed everything. Modbus introduced the concept of data on the factory floor. Modbus made it possible to connect an entire group of devices using only two wires on the controller. That alone saved a massive investment in wire, labor, and installation time. Instead of miles and miles of wire connecting hundreds of devices, a simple two-wire pair could be used to daisy-chain devices together. It was revolutionary for its time.

It wasn't just that Modbus was the first serial protocol. Modbus was the right technology at the right time. Remember that the first microprocessor wasn't invented until shortly before the birth of Modbus. Do you remember what those microprocessors were like? Simple 8-bit processors with severely limited code space and memory.

Modbus is the most pervasive communications protocol in industrial and building automation and the most commonly available means of connecting automated electronic devices. Why did that happen? Why did Modbus have such an impact on the industrial automation industry that it has survived for over 40 years and is to this day one of the leading industrial networks of the twenty-first century? There are three primary keys to its success:

- **Modbus Is an Open Standard** – Modicon, the inventor of Modbus, did not keep the standard proprietary. They released it as a nonproprietary standard and welcomed developers, even competitors, to implement it. They rightly assumed that it would be best for everyone, including them, if Modbus became successful in the marketplace. Because of this thinking, Modbus became the first widely accepted fieldbus standard. In a short time, hundreds of vendors implemented the Modbus messaging system in their devices and Modbus became the de facto standard for industrial communication networks.
- **Modbus Uses Standard Transports** – The transport layer for Modbus remote terminal unit (RTU) commands is simply RS-485, a differential communication standard that supports up to 32 nodes in a multi-dropped bus configuration. The RS-485 standard provided noise immunity that was superior to that in the RS-232 electrical standard.

The transport layer for Modbus TCP commands is TCP and only TCP.

- **Modbus is a Simple Protocol** – Modbus is quite easy to understand (see Figure 8-1). Its primary purpose is to simply move data between an RTU master device (a *client* in Modbus TCP) and one or more RTU slave devices (*servers* in the Modbus TCP world). There are only two kinds of data to move, register data, and coil data. Registers are 16-bit unsigned integers. Coils are single bits.

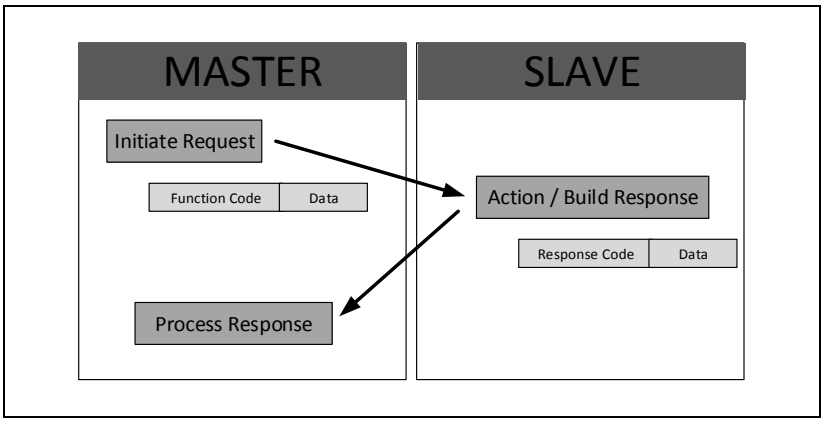


Figure 8-1. RTU Master/RTU Slave Modbus Architecture

Modbus uses a straightforward request/response command structure. A Modbus master requests or sends data to a slave and the slave responds. There are simple commands to read a register, read a coil, write a register, and write a coil

Modbus TCP and Modbus serial use ***exactly*** the same byte sequences to implement the command/response. The typical components of a Modbus message are presented in Table 8-1.

Table 8-1. Modbus Message Components

Function Code (FC)	The function code identifies the request to the Modbus slave. There are a large number of possible message requests, but about eight that are commonly used. These are the function codes that are detailed in this chapter.
Starting Address	The starting address is the index into the data area in the Modbus device. If the function code targets coils, this field specifies the index into the coils (bits) of the coil address space. If the function applies to registers, this field specifies the index into the registers for that part of the address space. Note: Modbus address spaces are one-based—the first register or coil is one. The Modbus protocol is zero-based. The first register or coil is zero. The address on the wire is always one less than the address in the Modbus data request.
Bit Length	The number of bits to read or write.
Word Count	The number of registers to read or write.
Byte Count	The number of data bytes included in the message request or response.
Response Code	This byte indicates the successful completion of the message request. It is identical to the original message request.
Exception Response (FC)	An exception response is indicated by combining the response code of the original Modbus function request with 80 hexadecimal. For example, a Modbus exception response to function code 3 is 83 hexadecimal. A single data byte value with the Modbus error code always follows the exception response byte.

For Modbus TCP, this set of message components is inserted as the data bytes of a standard TCP message as shown in Figure 8-2.

Modbus messages can be encoded, meaning turned into a series of bits, in one of two ways: Modbus ASCII or Modbus RTU. Modbus ASCII is a relic of the days of teletypes; every

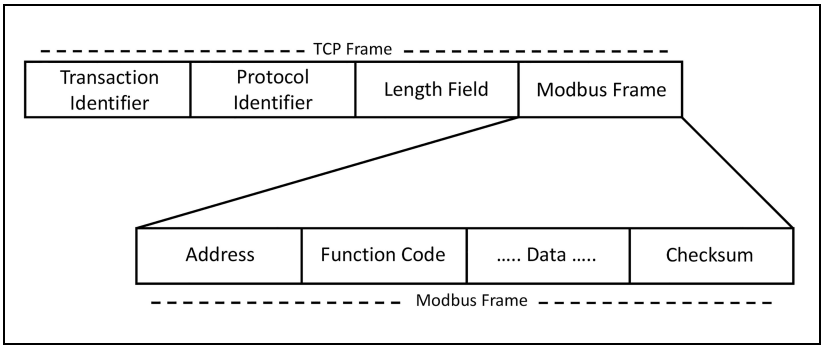


Figure 8-2. Format of a Modbus/TCP Frame (Courtesy Schneider Automation, www.modbus.org)

byte is transmitted as two ASCII characters. Few devices today use Modbus ASCII. Modbus RTU, on the other hand, is very popular and almost all Modbus serial and Modbus TCP devices use it. Modbus RTU encodes each byte of a message as a binary data value, which greatly enhances performance over Modbus ASCII. Modbus TCP devices always use Modbus TCP.

Modbus on a *serial* network is not fast—response times of a fraction of a second are not at all uncommon. Which, of course, is why Ethernet is an attractive alternative to serial—10, 100, or even 1,000 Mb performance is possible. Also, the simple Modbus protocol does not support complex objects and sophisticated device profiles. The master/slave orientation does not prevent peer-to-peer communication, but it requires separate "sessions" to be opened up between devices.

The power of Modbus has always been its simplicity. Modbus fit well in the era of limited RAM and FLASH. It required little code space (FLASH), often as little as 1K. Memory (RAM) varies with the size of the Modbus data space that you needed to represent the device's data. Simple automation devices with little bits of data—imagine a photo eye—could be implemented with hardly any RAM space. These devices could now, for the

first time, send their data to a control system as part of a daisy-chained 485 network, avoiding hardwired point-to-point communications.

The simplicity of Modbus has been both a blessing and a curse over the years. The simplicity has led to an incredible amount of activity and propagation of Modbus into many different industries around the world. There is probably no product category in the last 40 years that has not had an offering without Modbus.

The simplicity of Modbus has also led to many companies expanding the message structure, data representation, and transports. Some vendors have imposed any number of advanced structures and data types on the basic Modbus address structure. Others have used Modbus in other ways that go beyond the basic specification. These implementation extensions are not expressly prohibited by the specification, but they do not always make Modbus easily portable to many different applications.

8.3 EtherNet/IP

EtherNet/IP is an industrial Ethernet application layer protocol used by Rockwell Automation (Allen-Bradley) programmable controllers. EtherNet/IP uses standard Ethernet to organize the task of configuring, accessing, and controlling industrial automation devices. What does that mean? It means that EtherNet/IP is the highly structured protocol that uses Ethernet to move inputs from industrial end devices into an Allen-Bradly programmable controller and moves outputs generated by the control logic of an Allen-Bradley programmable controller to devices that map those outputs to real world physical outputs.

EtherNet/IP is based on the Control and Information Protocol (CIP) used in DeviceNet, CompoNet™, and ControlNet™. CIP provides a common, standardized mechanism for representing data, sending messages, and defining common device types for the component technologies that use the CIP core protocol. CIP is a media-independent protocol, which means that CIP messages can be sent over any communication media including CAN, Ethernet, and even something like FireWire. Sending CIP messages over CAN forms the basis for the DeviceNet protocol. Sending CIP messages over the ControlNet communication bus is the basis for ControlNet. Sending CIP messages over Ethernet TCP and UDP is the basis for EtherNet/IP. CIP provides the core technology used in each of these application layer protocols.

CIP defines two kinds of messages: explicit and implicit. Explicit messages are asynchronous, request/response type messages. A sender builds a request and sends it to a receiver. The receiver receives the request, opens it, decodes it, and sends a response. It is the traditional mechanism for communication between two devices. Implicit messages are synchronous messages that are continuously passed back and forth between the sender and receiver. Unlike explicit messages, the contents of implicit messages are simply raw data. Both the sender and the receiver have to have prior knowledge of how to construct and decode that raw data. How the sender and receiver map that implicit data is described later in this section.

The CIP protocols—EtherNet/IP, ControlNet, and DeviceNet—all define a type of controller device and some type of end device. Unlike other CIP protocols that use the terms master and slaves, the "master" device in EtherNet/IP is labeled a *scanner* and end devices, instead of slaves, are labeled as *adapters*. Scanners, typically programmable controllers, open connections with adapters, configure the timing of the asyn-

chronous implicit messaging with the adapters, and send explicit messages to adapters when needed. Adapter devices are typically industrial I/O devices, such as valves, I/O blocks, drives, scales, meters, and other end devices you might find in an automation system. An adapter has one job: send the scanner an implicit message with the status of its real world inputs and set its real world outputs as directed in the implicit output message received from the scanner.

EtherNet/IP uses TCP/IP for explicit messaging. Explicit messages (messages that are sent asynchronously) are sent over TCP. Examples of explicit messages include: changing the ramp time on a drive, setting a tare weight on a scale, and reading a barcode using TCP as the initiator of the message. By using TCP, the initiator automatically gets delivery acknowledgement for these important messages. On the other hand, implicit messages (messages that are delivered synchronously) are sent over UDP because they do not require delivery notification. By definition, a lost synchronous message is going to be replaced quickly by the next message in the sequence.

One of the most important features of EtherNet/IP (and CIP in general) is how it models device data in adapter devices. EtherNet/IP devices—in fact all CIP devices—are modeled as a collection of objects, each containing related data (a model of an EtherNet/IP device is illustrated in Figure 8-3). Objects are composed of data values or *attributes* in CIP terminology. Attributes values can be assigned a type with any one of a large number of EtherNet/IP types to model the specific data in the device.

The object nature of EtherNet/IP does not imply that the device implements the object structure internally, only that the device looks to the EtherNet/IP network as a collection of objects each with one or more attributes. These attributes form

the available data that an EtherNet/IP device exposes to the outside world. Scanners can access these attributes using explicit or implicit messaging.

There are two kinds of objects in every EtherNet/IP device: required objects and application objects (see Figure 8-3). Required objects must be present in every EtherNet/IP device while application objects are particular to the function of the end device. For example, every EtherNet/IP device must have an identity object, an Ethernet object, a TCP object, a router object, and a connection object. Each object provides attributes that describe the specific functionality of the device. The identity object, for example, presents identity information to the network by making available attributes like the vendor ID, the product code, the software revision, and other information that specifically identifies that device and its application. The TCP object provides information on the TCP connection like the TCP/IP address of the device. The connection object provides information on the current connections to a controller.

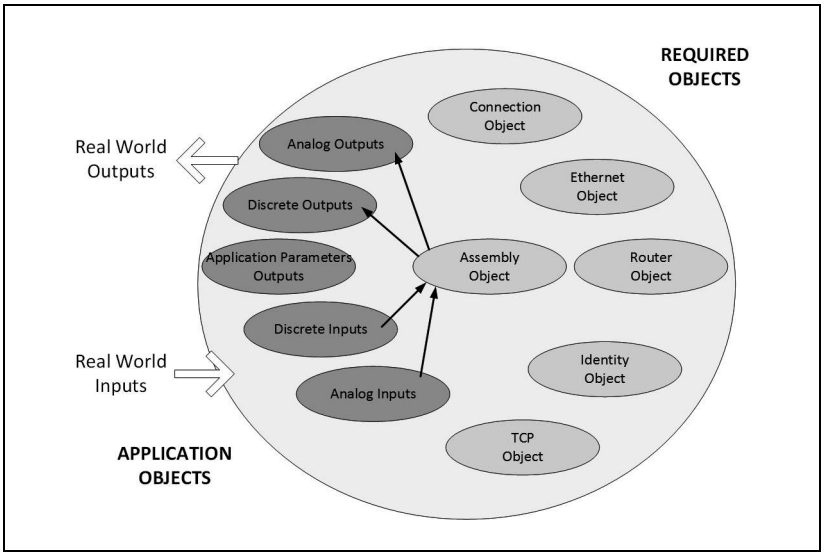


Figure 8-3. EtherNet/IP Object Representation

The object number and attribute numbers of required objects are predefined and identical in every EtherNet/IP device. Object 1 is always the identity object, Object 2 is defined to be the router object and so on. Attributes for the required objects are also predefined. Attribute 1 of the identity object is always the vendor ID, Attribute 2 is the device type and so on. By predefining the object numbers and attribute numbers for all the required objects, a controller or a PC tool always knows exactly how to get specific information about an EtherNet/IP device or, in actuality, any CIP device.

Application objects are the set of objects that model the I/O data of the adapter device. The set of application objects can be simple or complex. The object model for a simple device like an 8-channel valve might simply be one application object with one 8-bit attribute containing the current status of the valve states and one 8-bit attribute containing the commanded state of each valve as currently specified by the scanner. For a more sophisticated device, like a motor drive, there might be tens or even hundreds of objects to provide access to all the functionality of that device. The complexity of the object model in an EtherNet/IP device is directly related to the complexity of the data being exposed to the network through the object interface.

These application layer objects are predefined for a large number of common device types. All CIP devices with the same device type (drive system, motion control, valve transducer, etc.) must contain the identical series of application objects. The series of application objects for a particular device type is known as the *device profile*. A large number of profiles for many device types have been defined. Supporting a device profile allows a user to easily understand and switch from a vendor of one device type to another vendor with that same device type.

A device vendor can also group application layer objects into assembly objects (Figure 8-4). These super objects contain attributes of one or more application layer objects. Assembly objects form a convenient package for transporting implicit messages between devices. For example, a vendor of a temperature controller with multiple temperature loops may define an assembly for each temperature loop and an assembly with the data for all temperature loops. The user can then pick the assembly that is most suited to the application.

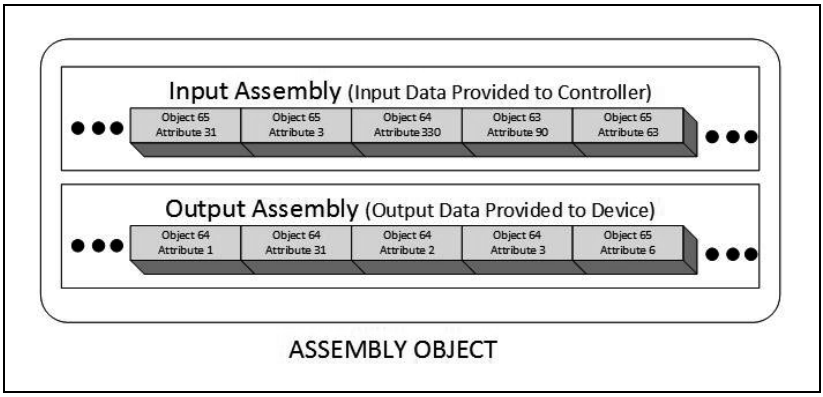


Figure 8-4. Assembly Object Structure

Assemblies are what is transferred in the implicit message. The input assembly is the set of attributes that are delivered to the scanner each time the implicit message is triggered. The output assembly is the set of attributes that are received from the scanner on each implicit output message. The contents of these assemblies are specified in an EDS or Electronic Data Sheet. The EDS can be used by the engineer configuring the controller to assemble the data to deliver in the output assembly and decode the data received in the input assembly. Another mechanism to decode the implicit message assemblies is the Add-On Profile (AOP). The AOP is a way of electronically configuring a

Rockwell Controller to know how to encode and decode messages for a specific device.

The Open Device Vendor Association (ODVA), headquartered in Ann Arbor, Michigan, is the vendor trade association that manages all CIP technologies, including EtherNet/IP. ODVA members, some of the world's leading automation companies, work to advance the development of CIP technologies and promote interoperability among vendor devices. One of the most important jobs of the association is conformance testing. Vendors manufacturing EtherNet/IP devices must submit each new device for conformance testing at the ODVA test lab. In the test lab, each device is exercised independently and in a rack containing a multitude of other vendor devices. The long sequence of tests verifies not only that the device adheres to the ODVA specification, but that it interoperates with other EtherNet/IP devices from other manufacturers. Once certified, the manufacturer can exhibit the conformance logo (Figure 8-5) indicating to users that the device is certified.

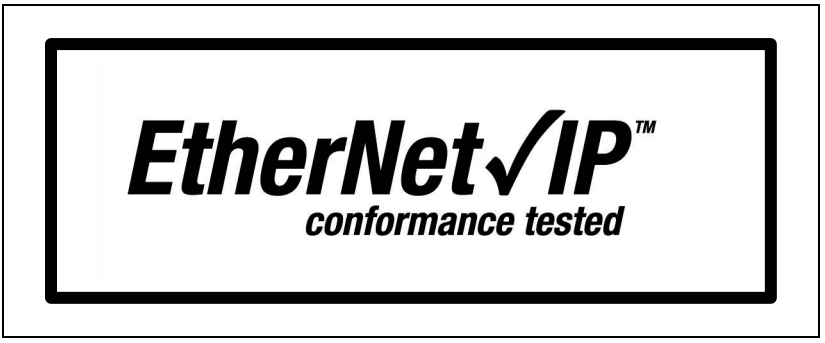


Figure 8-5. EtherNet/IP Conformance Tested Logo

EtherNet/IP is a widely implemented protocol with numerous advantages. First, Ethernet/IP uses the tools and technologies of traditional Ethernet. It uses all the transport and control protocols of standard Ethernet including the Transport Control

Protocol (TCP), the User Datagram Protocol (UDP), and the media access and signaling technologies found in off-the-shelf Ethernet. Building on these standard IP technologies means that EtherNet/IP works transparently with all standard off-the-shelf Ethernet devices (switches, routers, diagnostic tools, etc.) found in today's marketplace. It also means that EtherNet/IP is easily supported on standard PCs and all their derivatives. But even more importantly, because EtherNet/IP is based on a standard technology platform, EtherNet/IP will move forward as the base technologies evolve in the future. Secondly, as discussed above, Ethernet/IP is a certifiable standard. Devices are tested in a lab to verify that they meet the EtherNet/IP standard, which ensures interoperability between devices from multiple vendors and the consistency and quality of field devices. This ensures the consistency and quality of field devices. Third, EtherNet/IP is built on the widely accepted CIP protocol layer. Finally, and most importantly, EtherNet/IP is the industrial application layer protocol that is used by Rockwell Logix programmable controllers to communicate with Ethernet-enabled field devices. With Rockwell programmable controllers having a significant share of the programmable controller market in North America, EtherNet/IP will continue to dominate the industrial application landscape for years to come.

8.4 PROFINET

This is the PROFIBUS Trade Organization's answer to the need for interoperability between automation devices and subsystems that are linked together via Ethernet.

To understand what PROFINET is, you must understand what it is not. PROFINET is not the PROFIBUS protocol on Ethernet in the same way that Modbus/TCP is the old familiar Modbus

on Ethernet. PROFINET is not really a "fieldbus" as the term is normally understood, either.

PROFINET is not even Ethernet-specific; it links via TCP/IP and occupies layers 3 and above in the ISO/OSI model. Other physical layers, such as modems, WANs, VPNs, or the Internet may be employed so long as a PROFINET device is linked to the network via TCP/IP. An analogy to the office environment may help you understand what it is intended to do.

The PC in your office at work is networked with a dozen other PCs and a file server. Your office LAN (Ethernet 100BASE-T) is also linked to a T1 Internet line. You open Microsoft Word and create a complex document. You write some text and create some tables. Your coworker Jeff has a PowerPoint presentation on his PC; you open it via the network and copy and paste two graphics images into your Word document—the images are transferred intact as objects. Your other coworker Leslie has an Excel spreadsheet that you also open remotely and embed in your document—it is as simple as cutting and pasting. In this case, the Excel data is not static, it is live. Leslie updates this spreadsheet every Tuesday, and every time you open your document it will retrieve the latest data from her document on her PC. Finally, you access the Internet, copy and paste text and graphics from one website to your document, and then insert hyperlinks to other websites.

Behind this transparency among applications is a very complex object model created by Microsoft. Savvy PC users are accustomed to this level of sophistication and its benefits. This expectation naturally extends to the integration of business applications throughout an entire company and, of course, to devices in an automation system. This is the expectation that

PROFINET was engineered to satisfy. The OLE[1] for Process Control (OPC) software standard (www.opcfoundation.org) was developed to create transparency between hardware devices (e.g., network and I/O cards) and software applications (operator interface and programming tools). PROFINET uses components of OPC (COM and DCOM) and extends this transparency to all devices on a TCP/IP network, further defining object models for many kinds of device and programming parameters.

Rather than being specific to only one manufacturer's hardware or software (as is often the case with Microsoft), PROFINET is an industry standard available to all PROFIBUS members. PROFINET is an open communications and multivendor engineering model. This means that a preconfigured, preprogrammed, and pretested machine such as a transport conveyor can be set up using the vendor-specific electrical devices and applications as it has been in the past.

With PROFINET, the entire vendor-specific module (machine, electrical, and software) is represented as a vendor-independent PROFINET component. This PROFINET component is described within a standardized XML file that can be loaded into any PROFINET engineering tool, and interconnections between the PROFINET objects can be established by connecting lines from object interface to object interface.

In regards to communication and physical topology, established protocols such as TCP/IP, RPC, and DCOM are used. Data access to the PROFINET objects is standardized via OPC. As for physical device connections, not only can devices be connected via an integrated PROFINET interface, but existing

1. OLE stands for Object Linking and Embedding, a standard developed by Microsoft.

intelligent devices that are currently used with fieldbus networks, such as PROFIBUS, can be connected to Ethernet through a gateway device called a PROFINET *proxy server*.

Every PROFINET object is described by an XML file that defines these parameters so that every defined data type in the system is accessible by name throughout the PROFINET network. Integrators do not have to link devices at the bit level. It is expected that PROFINET proxies for each different fieldbus system (PROFIBUS, DeviceNet, Modbus, ControlNet, and others) will be developed over time, extending the transparency of large systems.

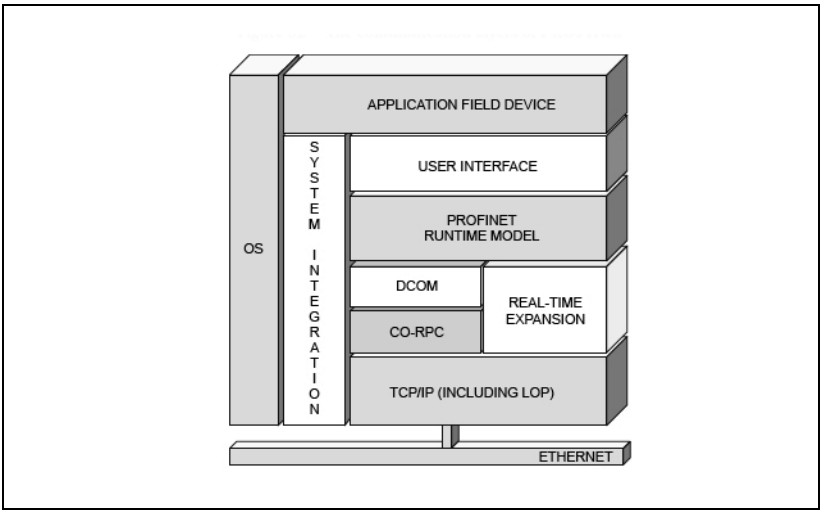


Figure 8-6. The Communication Layers of PROFINET

To delve into the internals of PROFINET as described in Figure 8-6 is beyond the scope of this book. However, more information is available at www.PROFIBUS.com, and PROFIBUS organization members can download the specification and source code at the site.

8.5 FOUNDATION Fieldbus High-Speed Ethernet

This protocol uses the FOUNDATION Fieldbus H1 process control protocol on TCP/IP. FOUNDATION Fieldbus H1 is a sophisticated, object-oriented protocol that operates at 31.25 Kbps on standard 4–20 mA circuits. It uses multiple messaging formats and allows a controller to recognize a rich set of configuration and parameter information (device description) from devices that have been plugged into the bus. FOUNDATION Fieldbus even allows a device to transmit parameters relating to the estimated reliability of a particular piece of data. FOUNDATION Fieldbus uses a scheduler to guarantee the delivery of messages, so issues of determinism and repeatability are solidly addressed. Each segment of the network contains one scheduler.

FOUNDATION Fieldbus high speed Ethernet (HSE) is the same as the H1 protocol, but instead of 31.25 Kbps, it runs on TCP/IP at 100 Mbps. It provides the same services and transparency of network objects but operates at a higher level.

FOUNDATION Fieldbus is specifically focused on the process control industry and will likely be the dominant Ethernet I/O standard there.

Installations in this segment of the world typically have the following characteristics:

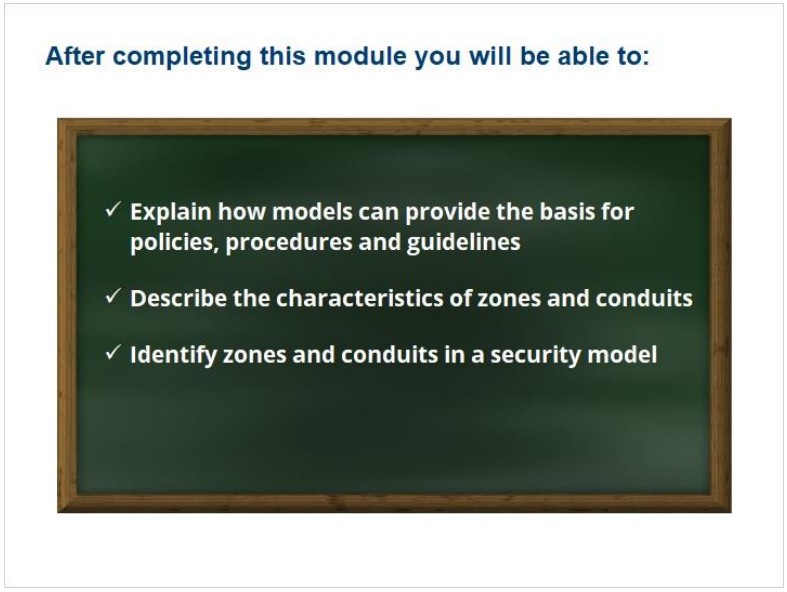
- Very large campuses (e.g., chemical refineries) with many nodes
- Data does not have to move quickly, but there is a lot of it to move (large packets)
- Large quantities of analog data
- Hazardous area classifications such as Class I, Division 2

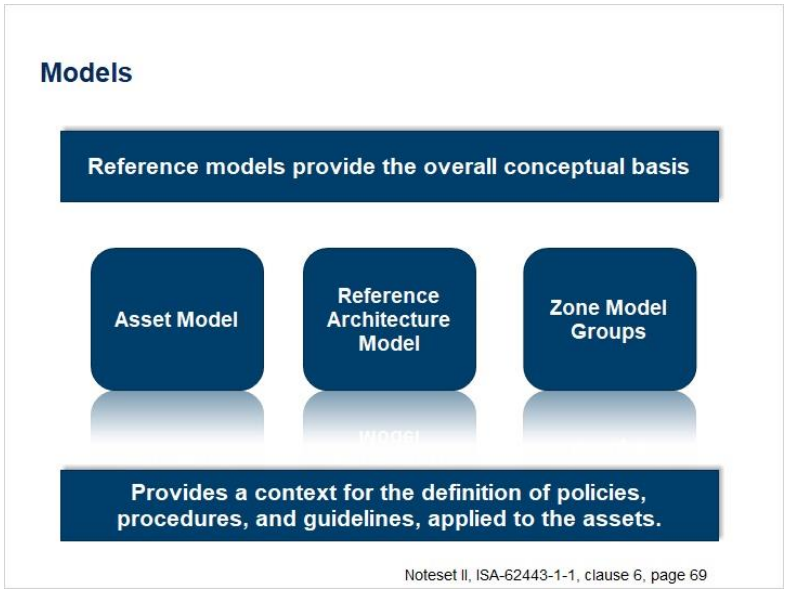
Week 6

Week 6
Week 6
Week 6
Week 6
Week 6

Setting the Standard for Automation™

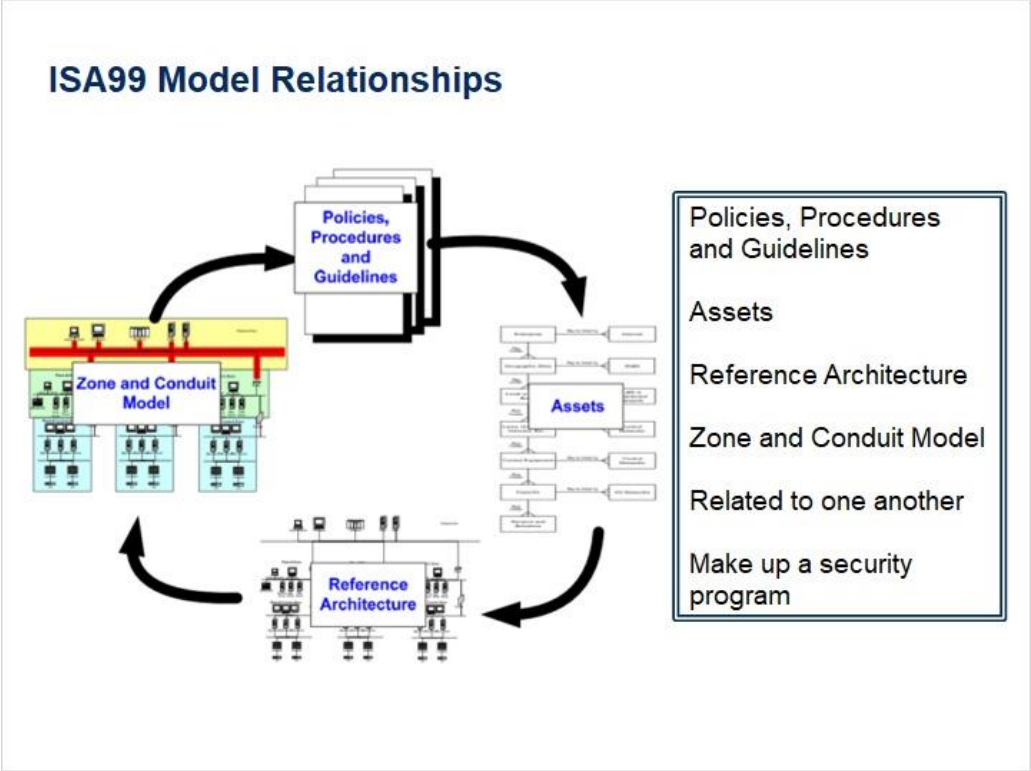
IC329 Module 9





Notes:

- The objective is to identify the security needs and important characteristics of the environment at a level of detail necessary to address security issues with a common understanding of the framework and vocabulary
- These models come in various forms
- All of this information is used to develop a detailed program for managing the security of an industrial automation and control system.
- Noteset Volume II, ISA-62443-1-1, clause 6, page 69



Notes:

- Assets, Reference Architecture, Zone and Conduit Model described are related to one another and to the policies, procedures, and guidelines that make up a security program
- Do not get into details at this point, you will cover them in the next set of slides
- Recall that the objective is to identify the security needs and important characteristics of the environment at a level of detail necessary to address security issues with a common understanding of the framework and vocabulary
- You can find this figure in Noteset Volume II, ISA-62443-1-1, clause 6.6, Figure 23, page 89

Reference Model Levels

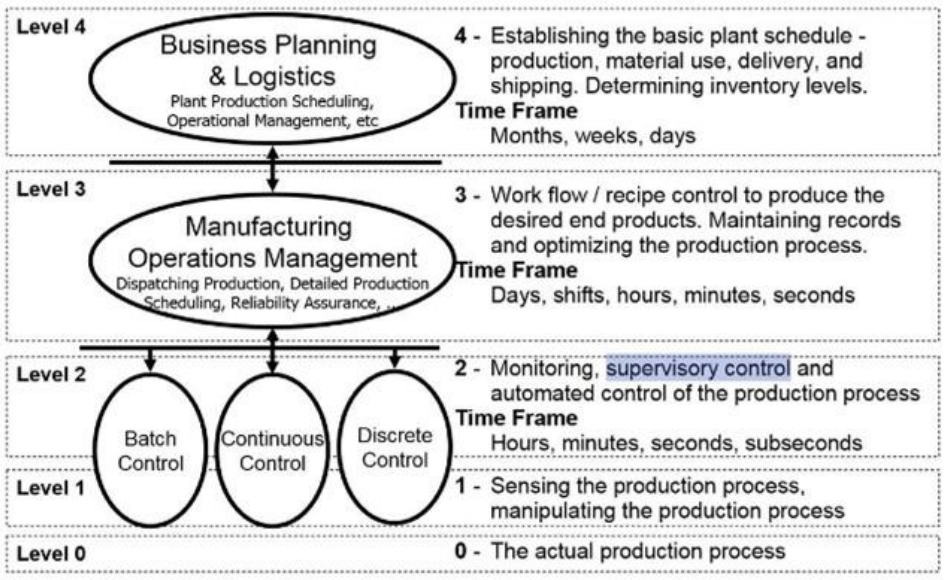


Figure 3 – Functional hierarchy

ANSI/ISA-95

Notes:

- Next few slides will show some models depicted to help clarify the level concept
- Level 4 Enterprise Systems defined as including the functions involved in the business-related activities needed to manage a manufacturing organization. Functions include enterprise or regional financial systems, production scheduling, operational management, and maintenance management for an individual plant or site in an enterprise Engineering systems are also considered to be in this level
- Level 3 includes the functions involved in managing the work flows to produce the desired end products such as dispatching production, detailed production scheduling, reliability assurance, and site-wide control optimization
- Level 2 includes the functions involved in monitoring and controlling the physical process. There are typically multiple production areas in a plant such as distillation, conversion and blending in a refinery or the turbine deck and coal processing facilities in a utility power plant
- Level 1 includes the functions involved in sensing and manipulating the physical process, maintaining process history
- Level 0 is the actual physical process. It includes the sensors and actuators directly connected to the process and process equipment
- Noteset Volume II, ISA-62443-1-1, clause 6.2, page 71
- Note that U.S. Nuclear Generation plants use a similar model with the levels numbered in reverse-Process =Level 4 versus Level 0
    - Reference NRC REGULATORY GUIDE 5.71, section C.3.2.1 Security Defensive Architecture, January 2010
- Do not mix up the term Reference Model “Level” with the OSI/RM 7 “layer” model. You will have the IT guys all confused.

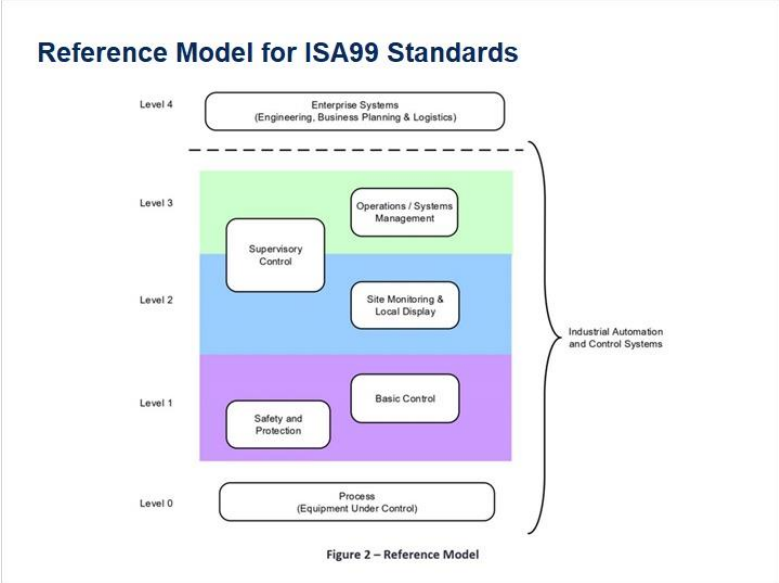
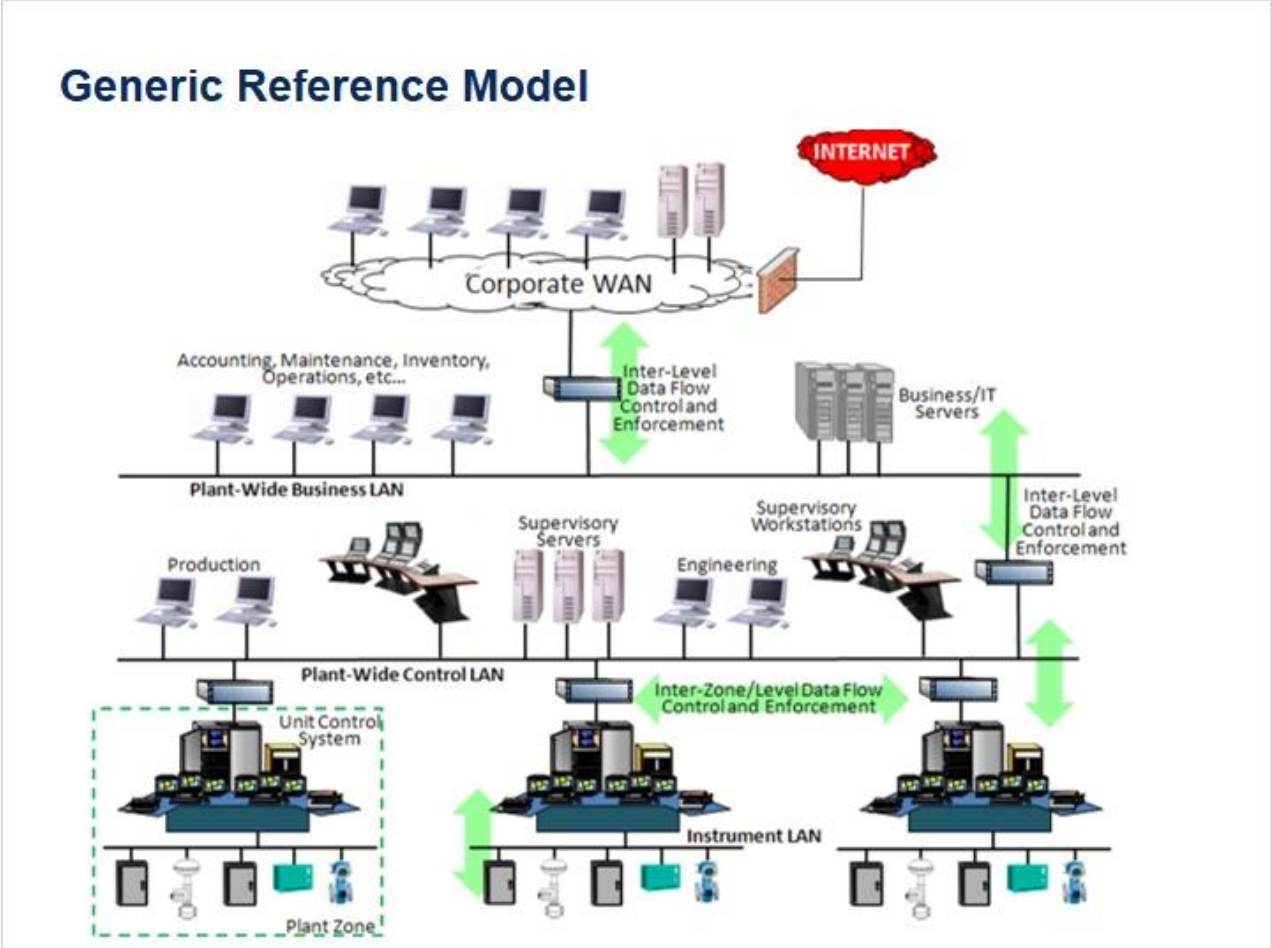


Figure 2 – Reference Model

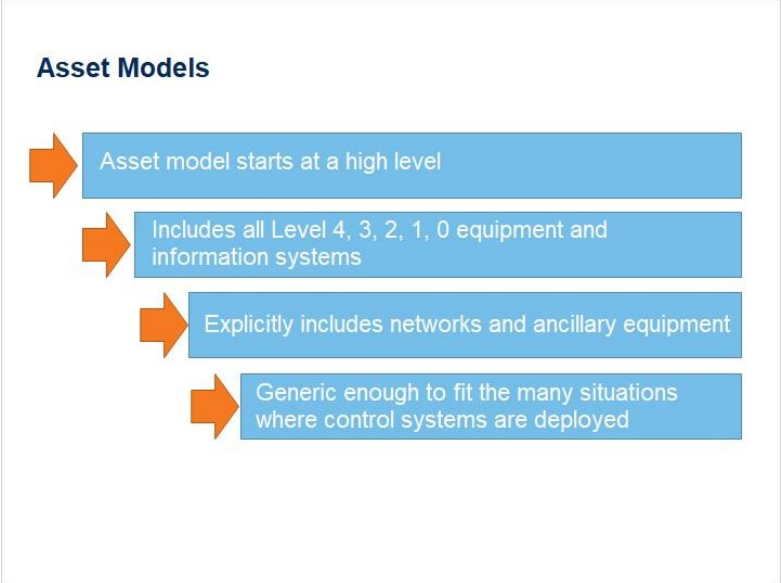
Notes:

- The objective is to identify the security needs and important characteristics of the environment at a level of detail necessary to address security issues with a common understanding of the framework and vocabulary
- A reference model describes a generic view of an integrated manufacturing or production system, expressed as a series of logical levels
- The term “reference model” became popular with the success of the ISO “Seven Layer” model for Open Systems Interconnection (OSI)
- Both of the models in this and the next couple of slides consist of the same basic levels, each representing a particular class of functionality which we will discuss
- The reference model shown is used by the ISA99 series of standards and appears in Noteset Volume II, ISA-62443-1-1, clause 6.2, page 69
- This model is derived from the general model used in ANSI/ISA-95.00.01-2000, Enterprise-Control System Integration Part 1: Models and Terminology
- Functional Hierarchy (Purdue Model)



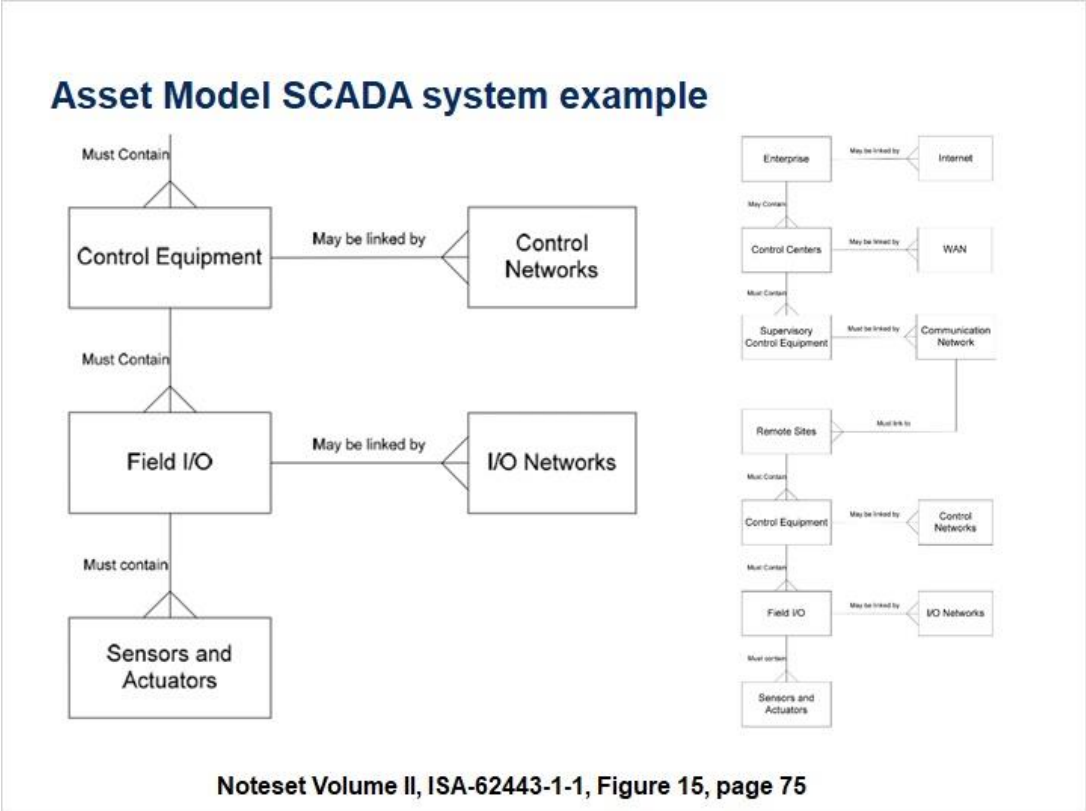
Notes:

- A slightly different view of the reference model
- Copied from TS06 v2.1 course
- There is no one right way, these are all examples
- It is beneficial to adopt a consistent model across your enterprise if at all possible.



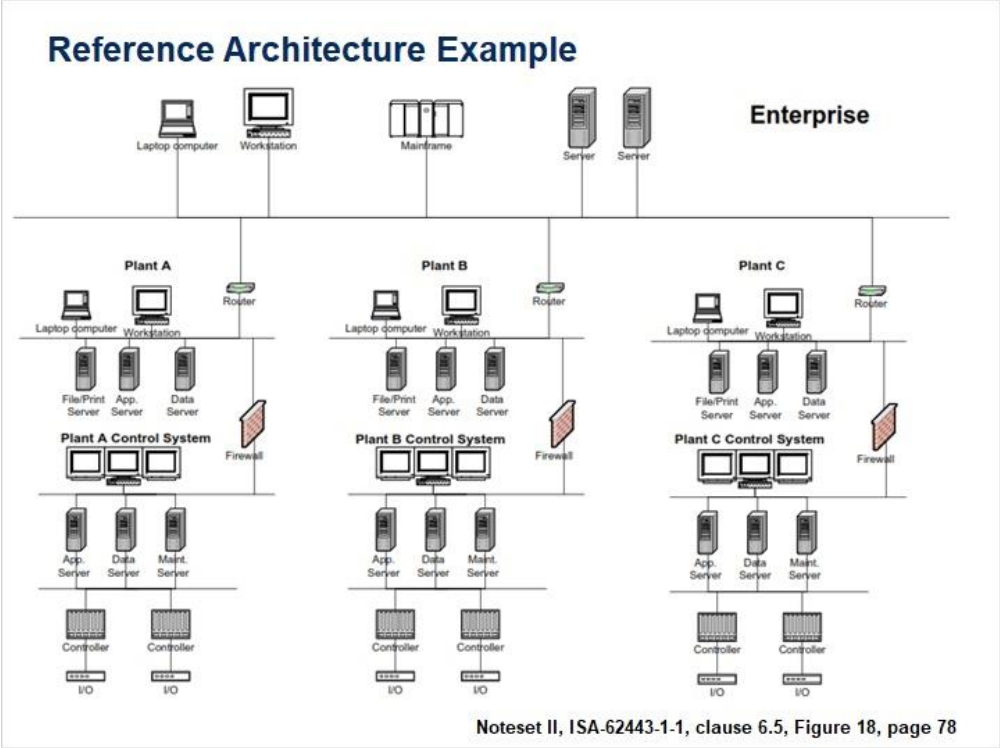
Notes:

- At one time these systems were isolated from other computers in the enterprise and used proprietary hardware, software, and networking protocols.
- This is no longer the case as control system vendors have adapted COTS information technology because of its cost advantages
- Business needs have driven integration of control systems with business information systems.
- From a security perspective the concern is with the control equipment itself, the users of that equipment, the connections between control system components, and the interconnections with business systems and other networks
- Excerpt from a sample asset model depicted on next slide
- Noteset Volume II, ISA-62443-1-1, clause 6.3, page 73



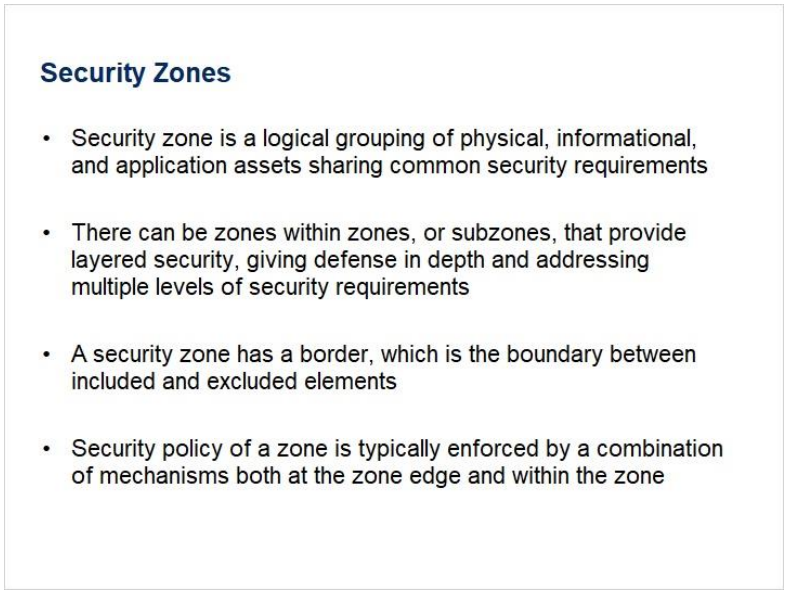
Notes:

- Excerpt from SCADA asset model sample depicted
- For the full image refer to Noteset Volume II, ISA-62443-1-1, Figure 15, page 75
- Figure 14 has a process manufacturing asset model example that can be reviewed if time allows



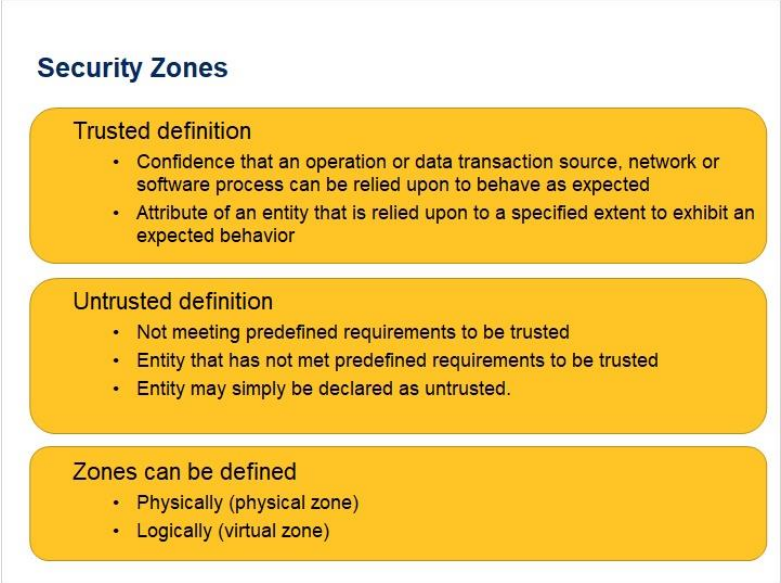
Notes:

- A reference architecture is specific to each situation under review and will be specific for that analysis
- It would be common for an organization to have a single reference architecture for the corporation that has been generalized to cover all operating facilities
- Each facility or type of facility may also have a more detailed reference network architecture diagram that expands on the enterprise model
- A zone and conduit model is then developed from the reference architecture
    - It is used to describe the logical groupings of assets within an enterprise or a subset of the enterprise.
- There is a distinct advantage to aligning security zones with physical areas or zones in a facility - for example, aligning a control center with a control security zone
- All unqualified uses of the word "zone" in this standard should be assumed to refer to a security zone
- Manufacturing function is shown
- Noteset Volume II, ISA-62443-1-1, clause 6.4, Figure 16 page 78
- In draft version of 62443-1-1 D6E2 referred to as a Physical Architecture Model Example, …. single generic model that has been generalized to cover all operating facilities and thus level of detail is not there.



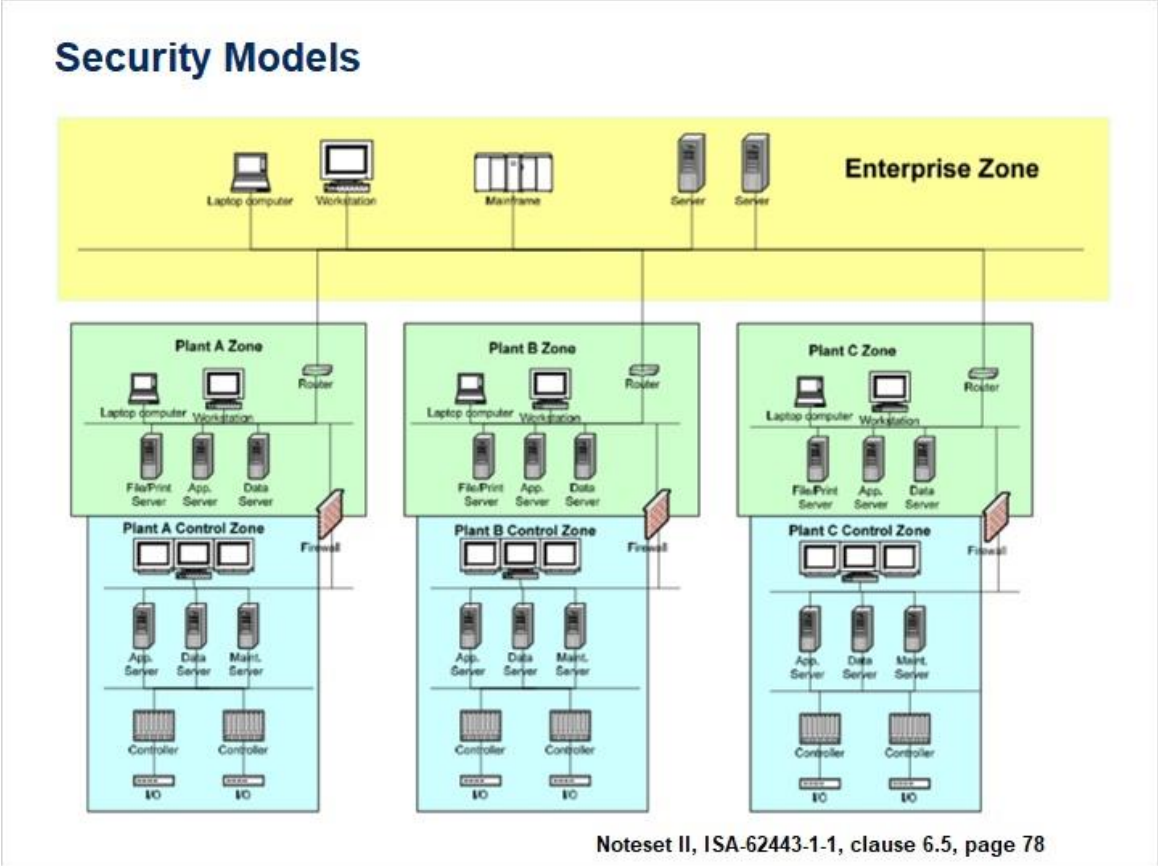
Notes:

- Every situation has a different acceptable level of security
- For large or complex systems it may not be practical or necessary to apply the same level of security to all components.
- Differences can be addressed by using the concept of a security "zone," or area under protection.
- A security zone is a logical grouping of physical, informational, and application assets sharing common security requirements
- This concept applies to the electronic environment where some systems are included in the security zone and all others are outside the zone
- ISA-62443-3-3
- confidence that an operation or data transaction source, network or software process can be relied upon to behave as expected
- Note 1 to entry: Generally, an entity can be said to 'trust' a second entity when it (the first entity) makes the assumption that the second entity will behave as the first entity expects.
- Note 2 to entry: This trust may apply only for some specific function.



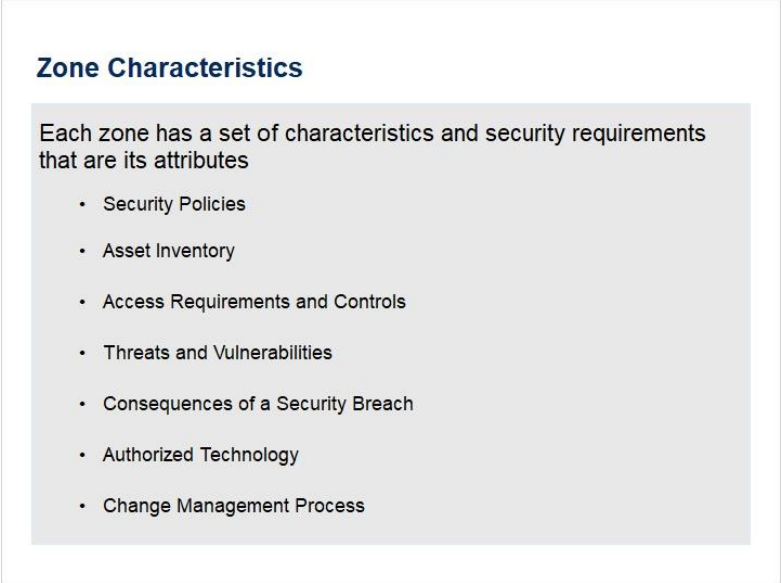
Notes:

- Every situation has a different acceptable level of security
- For large or complex systems it may not be practical or necessary to apply the same level of security to all components.
- Differences can be addressed by using the concept of a security “zone,” or area under protection.
- A security zone is a logical grouping of physical, informational, and application assets sharing common security requirements
- This concept applies to the electronic environment where some systems are included in the security zone and all others are outside the zone
- ISA-62443-3-3
- confidence that an operation or data transaction source, network or software process can be relied upon to behave as expected
- Note 1 to entry: Generally, an entity can be said to 'trust' a second entity when it (the first entity) makes the assumption that the second entity will behave as the first entity expects.
- Note 2 to entry: This trust may apply only for some specific function.



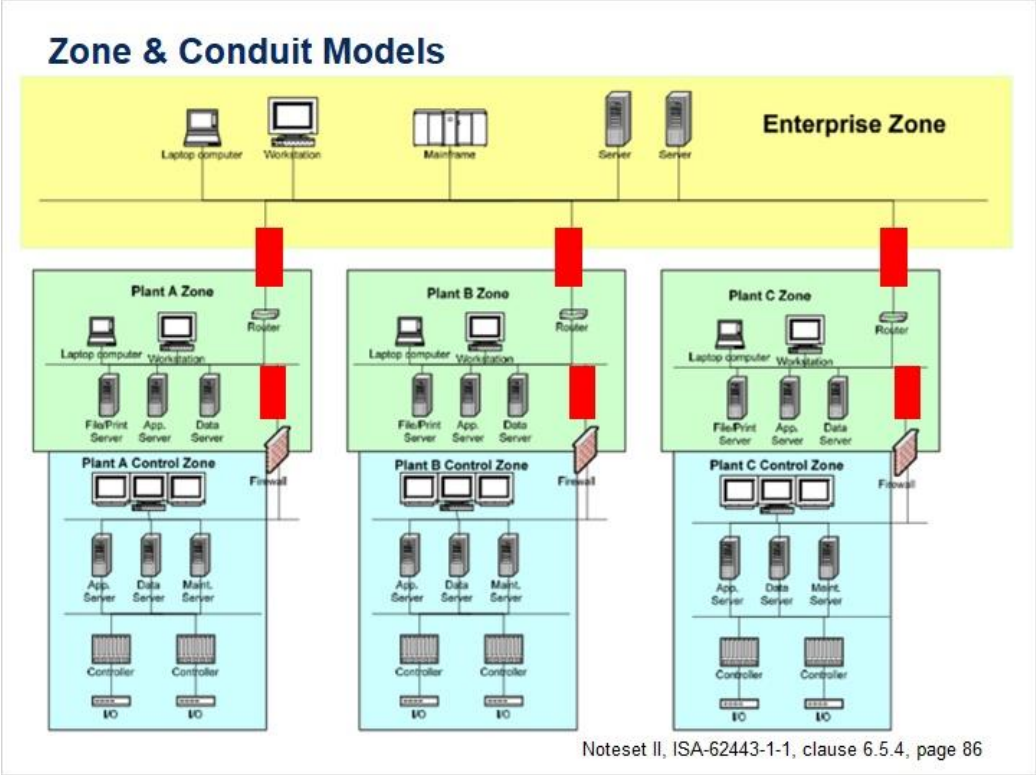
Notes:

- Security model is developed from the reference architecture
    - It is used to describe the logical groupings of assets within an enterprise or a subset of the enterprise
- The assets are grouped into entities (e.g., business, facility, site, or IACS) that can then be analyzed for security policies and hence requirements
- The model helps to assess common threats, vulnerabilities, and the corresponding countermeasures needed to attain the level of security (Target Security Level) required
- Target Security Level will be discussed later in the course
- By grouping assets in this manner, a security policy can be defined for all assets that are members of the zone
- This analysis can then be used to determine the appropriate protection required based on the activities performed in the zone
- Noteset Volume II, ISA-62443-1-1, clause 6.5, page 78
- Shown here is a separate zones example
- Zone policies would be independent, and each zone could have totally different security policies
- Noteset Volume II, ISA-62443-1-1, clause 6.5, Figure 18, page 78



Notes:

- Security Policies - controlling document that describes the overall security goals and how to ensure the Target Security Level is met
- Target Security Level discussed later in the course
- Asset Inventory - maintain a list of all of the assets (physical and logical)
- Access Requirements and Controls - articulate the access required for the zone to meet its business objectives, and how this access is controlled
- Threats and Vulnerabilities - documenting the threats and vulnerabilities happens in the threat and vulnerability assessment that is part of the zone security policy
- Consequences of a Security Breach - security policy should outline what types of countermeasures are appropriate to meet the Target Security Level for the zone, within the cost versus risk trade-off
- Authorized Technology - dynamic list of technologies allowed in the zone, as well as those not allowed
- Change Management Process - maintain the accuracy of a given zone's asset inventory and how changes to the zone security policy are made
    - A formal process ensures that changes and additions to the zone do not compromise the security goals



Notes:

- Defining Conduits - Conduits are security zones that apply to specific communications processes
- Security zones that apply to specific communications processes
- "pipes" that connect zones or that are used for communication within a zone
    - Wired or wireless
- Conduit is the wiring, patch panels, black boxes, hubs, media converters, routers, switches, and network management devices that make up the communications under study
- Noteset Volume II, ISA-62443-1-1, clause 6.5.4, page 86

Conduits

Conduit is a logical grouping of communication assets that protects the security of the channels it contains.

(Similar to how physical conduit protects cables from physical damage)

Stated another way

- logical grouping of communication channels, connecting two or more zones, that share common security requirements

Trusted conduits crossing zone boundaries must use an end-to-end secure process

Physical devices and applications that use the channels contained in a conduit define the conduit end points

Can be defined physically or logically

Notes:

- See definition Noteset Volume II, ISA-62443-1-1, subclause 3.2.27, page 21
- See definition Noteset Volume II, ISA-62443-3-3, subclause 3.1.12, page 17

Conduit Characteristics

- ✓ Physically a conduit can be cable or wireless that connects zones for communication purposes
- ✓ A conduit is a type of zone that cannot have subzones
  - Conduit is not made up of subconduits
  - Conduit is allowed to traverse a zone as long as the security of the channels contained within the conduit is not impacted by the zone
  - Can be trusted or untrusted
- ✓ Conduits are defined by the list of all zones that share the given communication channels
- ✓ It can be a single service (i.e., a single Ethernet network) or can be made up of multiple data carriers

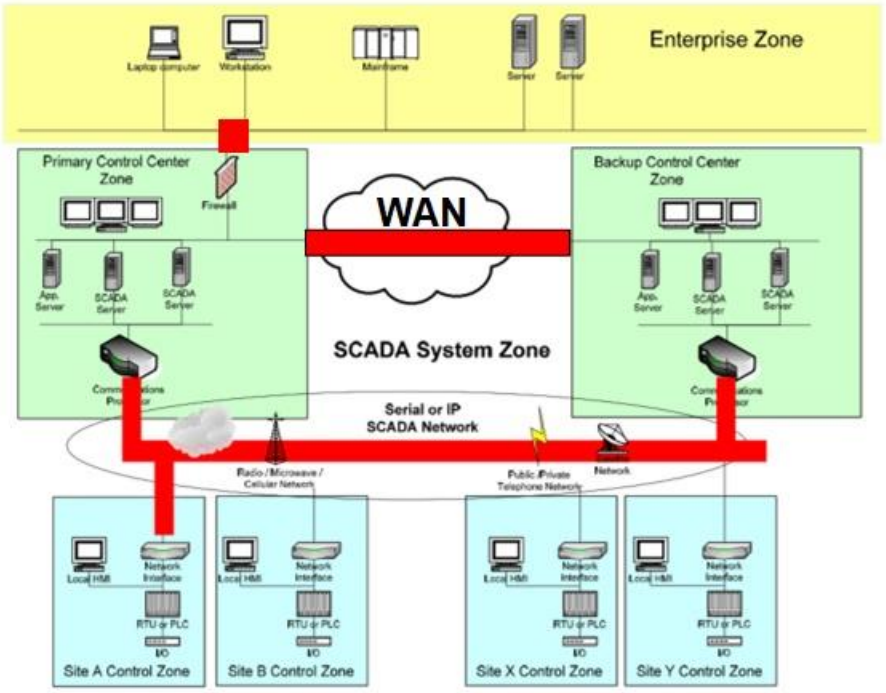
Notes:

- Defining Conduits - Conduits are security zones that apply to specific communications processes
- Security zones that apply to specific communications processes
- “pipes” that connect zones or that are used for communication within a zone
- Conduit is the wiring, routers, switches, and network management devices that make up the communications under study

Notes:

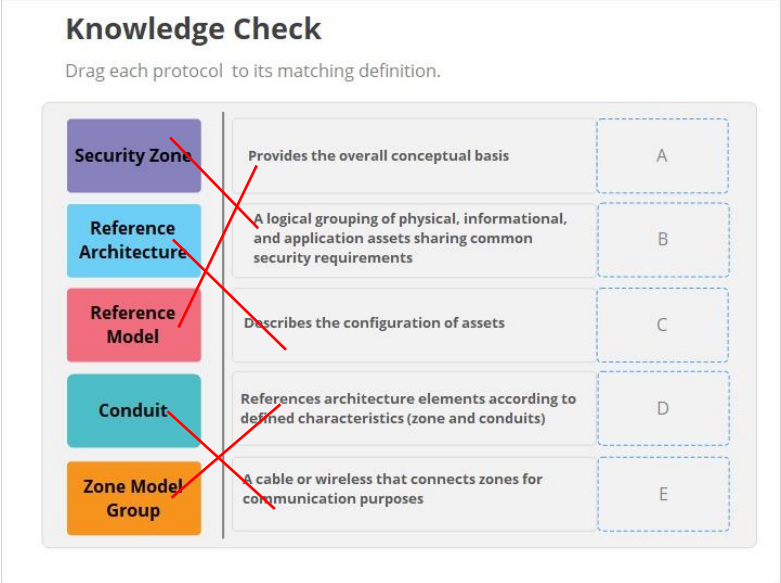
- Security Policies - controlling document that describes the overall security goals and how to ensure the Target Security Level is met
- Target Security Level discussed later in the course
- Asset Inventory - maintain a list of all of the communication assets (physical and logical)
- Access Requirements and Controls - articulate the access required for the zone to meet its business objectives, and how this access is controlled
- Threats and Vulnerabilities - documenting the threats and vulnerabilities happens in the threat and vulnerability assessment that is part of the zone security policy
- Consequences of a Security Breach - security policy should outline what types of countermeasures are appropriate to meet the Target Security Level for the zone, within the cost versus risk trade-off
- Authorized Technology - dynamic list of technologies allowed in the zone, as well as those not allowed
- Change Management Process - maintain the accuracy of a given zone's asset inventory and how changes to the zone security policy are made
    - A formal process ensures that changes and additions to the zone do not compromise the security goals
- Connected Zones - A conduit may also be described in terms of the zones to which it is connected

Zone & Conduit Models

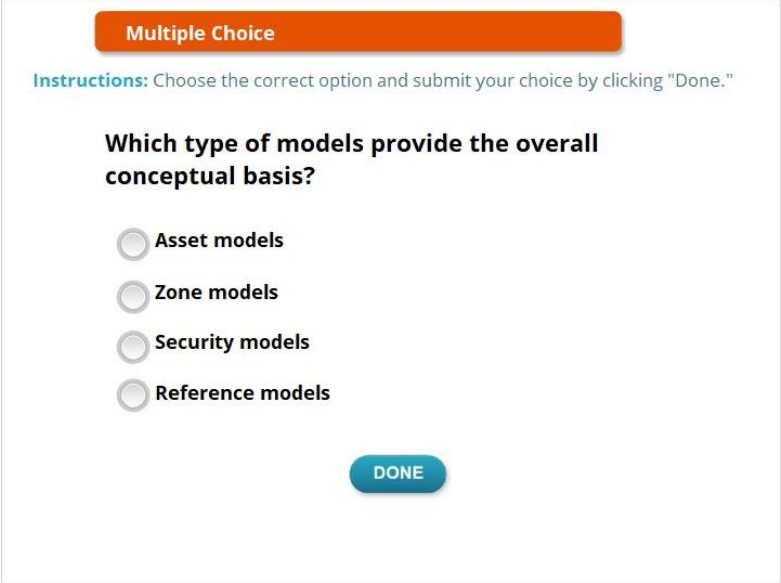


Notes:

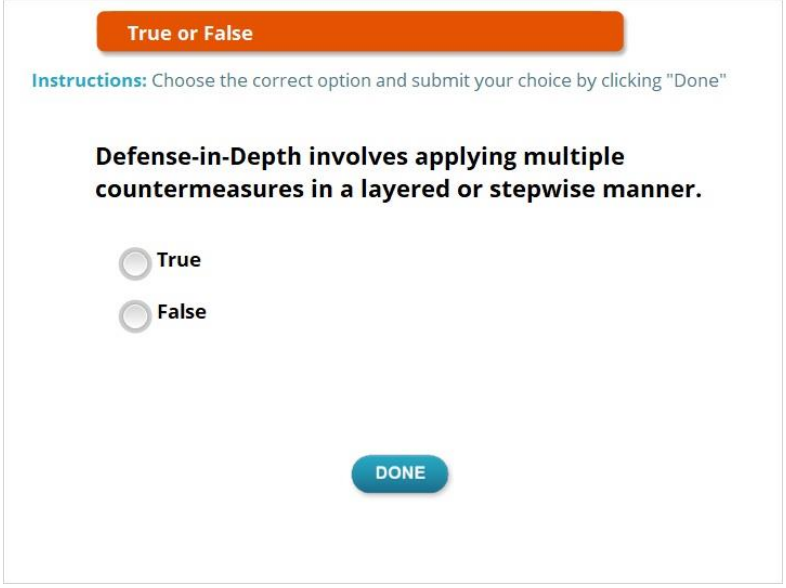
- SCADA Conduit Example
- Noteset Volume II, ISA-62443-1-1, clause 6.5.5, Figure 22, page 87



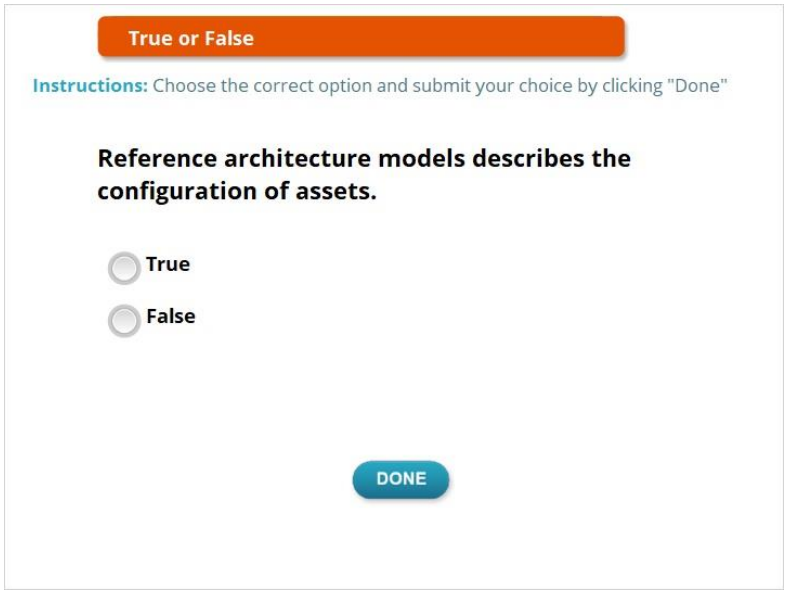
Drag Item	Drop Target
Security Zone	B
Reference Architecture	C
Reference Model	A
Conduit	E
Zone Model Group	D



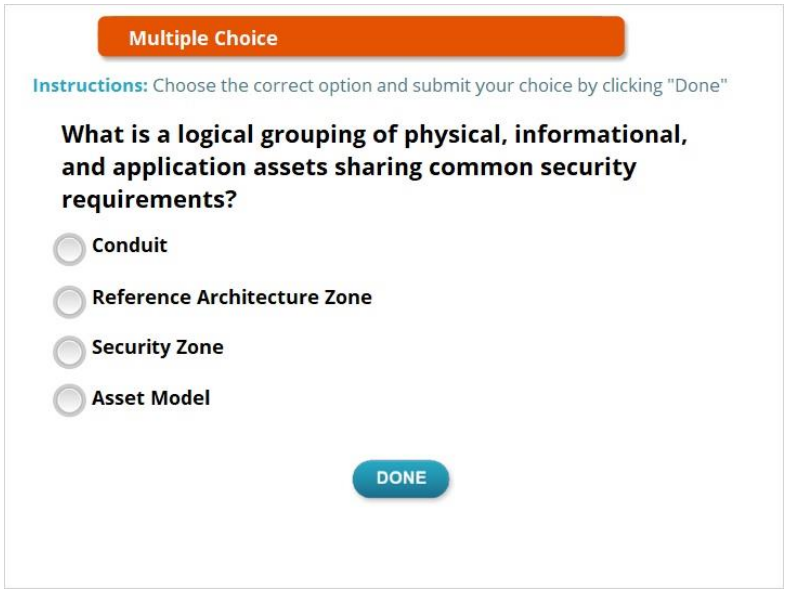
Correct	Choice
X	Radio Button 4



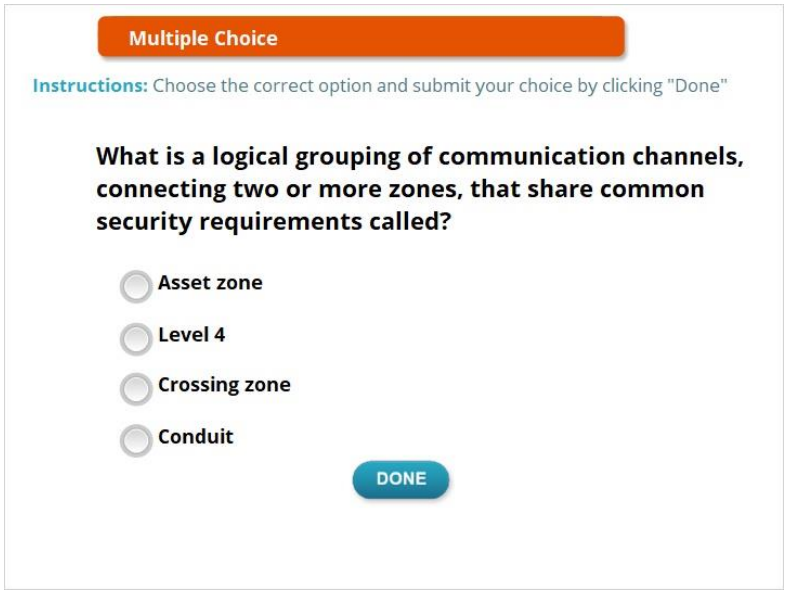
Correct	Choice
X	Radio Button 1



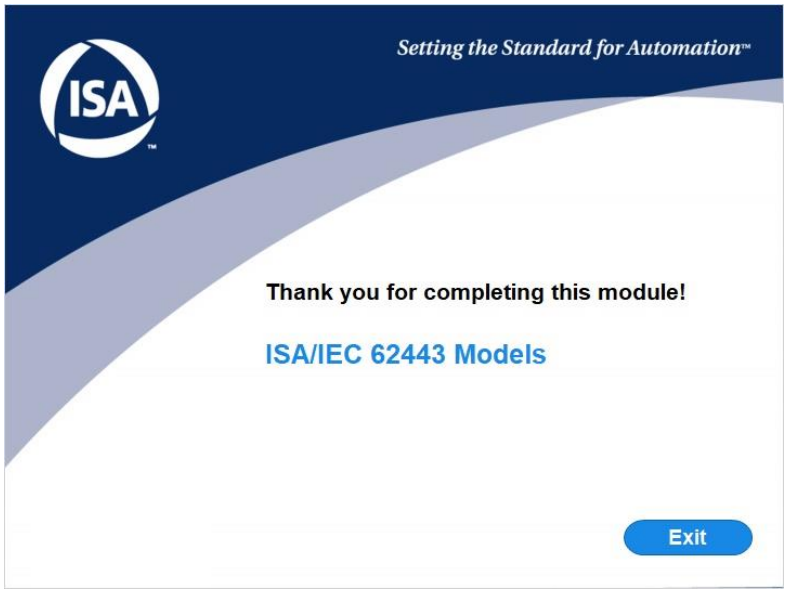
Correct	Choice
X	Radio Button 1



Correct	Choice
X	Radio Button 3



Correct	Choice
X	Radio Button 4



IC329 Module 10

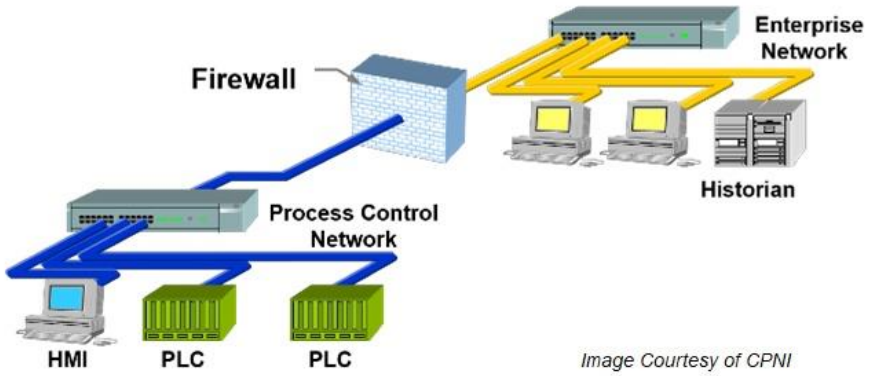
After completing this module you will be able to:

- ✓ Discuss why and how to separate business and process networks
- ✓ Explain the need for Malicious Code Protection
- ✓ Explain the need for patching IACS systems
- ✓ Identify asset owner requirements for patch management
- ✓ Identify product supplier/service provider requirements for patch management
- ✓ Explain the use of IDS and IPS
- ✓ Identify the two types of IDS
- ✓ Identify IDS/IPS best practices
- ✓ Discuss the use of cryptography and file hashing to enhance security
- ✓ Discuss best protocol and VPN choices

Network Segmentation

Business/Process Firewall Architectures

- Between plant floor and the rest of the company networks a firewall is a must
- Do not try to use a router to prevent hackers/viruses entering – it isn't good enough



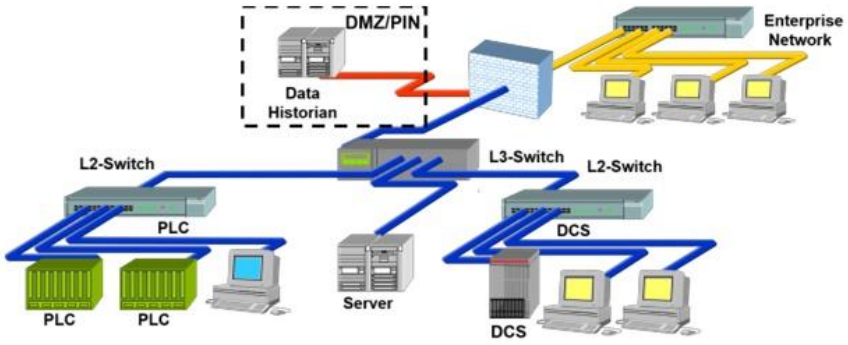
Notes:

"*By introducing a simple firewall between the enterprise and process control networks, a significant security improvement can be achieved. Most firewalls on the market today offer stateful inspection for all TCP packets and application proxy services for common Internet application layer protocols such as FTP, HTTP and SMTP. Aggressively configured, the chance of a successful external attack on the PCN is significantly reduced. Many of the companies interviewed for this study used this as their standard design for PCN/SCADA security*."

From "The NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks", National Infrastructure Security Co-ordination Centre (NISCC), 8th July 2004

Business/Process Firewall Architectures (Cont'd)

- Much better is the use of Demilitarized Zones (DMZ) between the enterprise and process control networks
- This three-tier design allows secure data transfer between systems



NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control
http://www.cpni.gov.uk/docs/re-20050223-00157.pdf

Notes:

Point out how commonly shared devices such as a data historian can be placed in a Demilitarized Zones (DMZ) between the enterprise and process control networks. See below…

> *"A further improvement is the use of firewalls with the ability to establish a number of Demilitarized Zones (DMZ) between the enterprise and process control networks. Each DMZ holds a separate "critical" component, such as the data historian, the wireless access point or remote and third party access systems. In effect, the use of a DMZ-capable firewall allows the creation of an intermediate network often referred to as a Process Information Network (PIN).*
>
> *To create a DMZ requires that the firewall offer three or more interfaces, rather than the typical public and private interfaces. One of the interfaces is connected to the enterprise, the second is connected to the PCN/SCADA network and the remaining interfaces to the shared or insecure assets such as the data historian server or wireless access points*." Alternatively, multiple firewalls can be used to establish a DMZ.

From "The NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks", National Infrastructure Security Co-ordination Centre (NISCC), 8th July 2004

Defense-in-depth Firewall Architectures

Distributing security appliances provide defense-in-depth to key assets like controllers

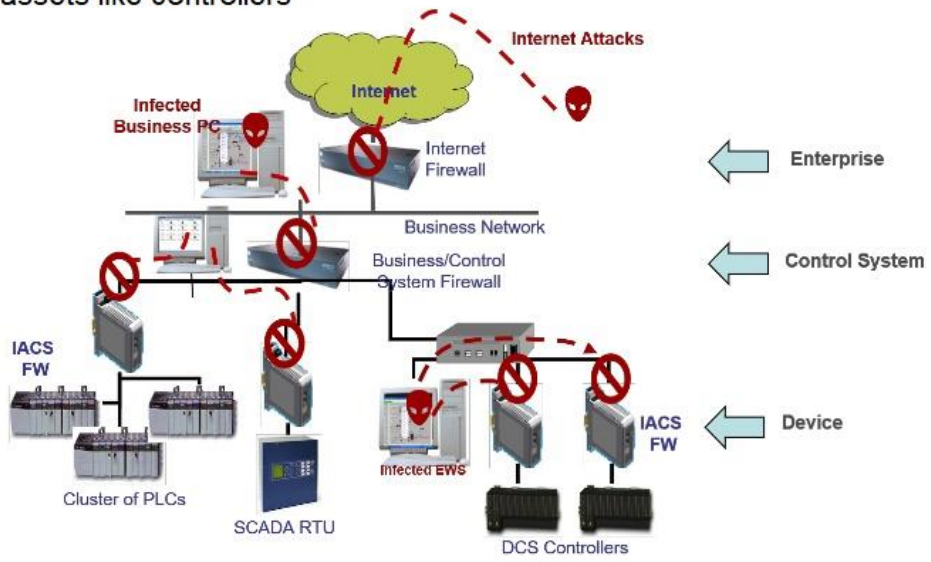
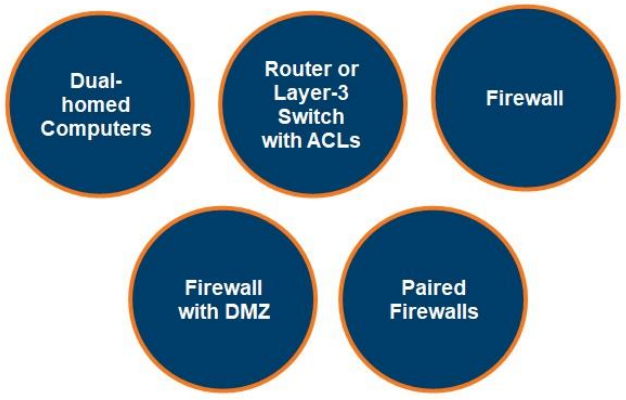


Image Courtesy of MTL Instruments

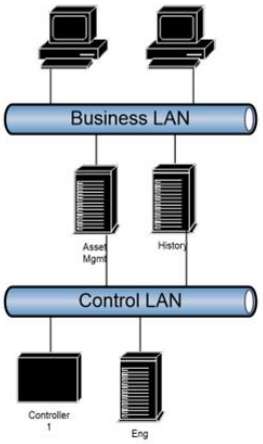
Notes:

- This allows a "Defence- in-depth" strategy to be used, so that even if a hacker or virus manages to get through the main corporate firewall, they will still be faced with an army of SCADA-focused security devices that need to be breached before any damage can be done.

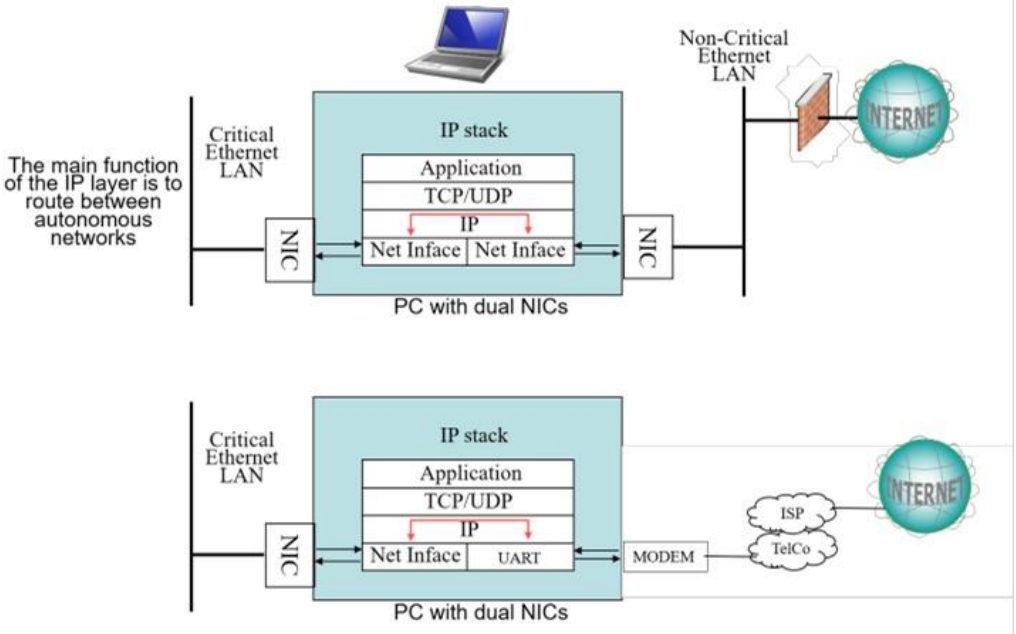
Comparing Various Architectures



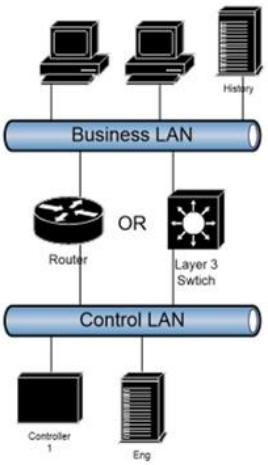
Dual-homed Computers



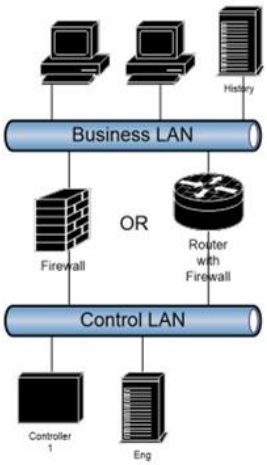
Access Vulnerabilities – Bridged LANs



Routers / Firewalls

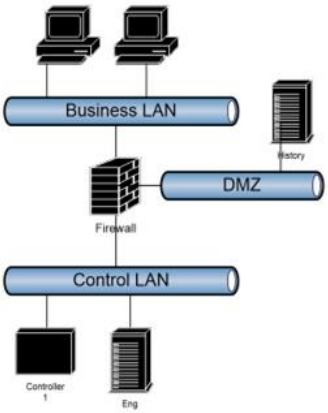


Routers or Layer-3 Switches with ACL Filters

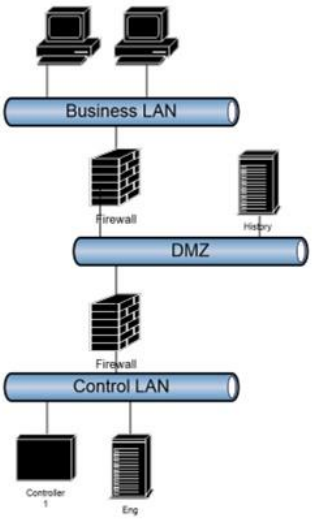


Firewall

Firewalls / DMZs



Firewall with DMZ



Paired Firewalls


~~Short~~ Diversion
to
Patch
Management

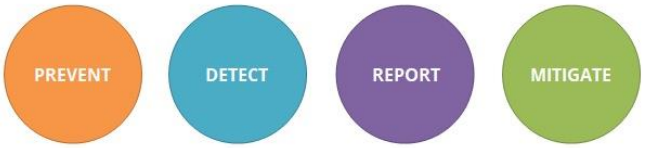
Topics


• Malicious Code Protection
• IACS Patching
• Asset Owner Requirements
• Product Supplier/Service Provider Requirements

Malicious Code Protection

Malware-related incidents are among the top cause of cyber-related production losses and upsets in process control systems

Protection mechanisms protect against malicious code to:



How do you verify that your prevention or detection mechanisms are functioning as expected?

Malicious Code Protection

Use mixed deployment systems:

- ✓ Scanning at the control system firewall
- ✓ Ingress and egress traffic
- ✓ Application whitelisting (AWL)
- ✓ Automatic updating for non-critical systems
- ✓ Systems with vendor-approved update schemes
- ✓ Manual scheduled updates for more difficult systems

Focus on anti-virus signatures in all computers located in the DMZ

A dedicated anti-virus server can be located in the DMZ

Patching is an important tool for mitigation

Patch Management in the IACS Environment

Patching is not a spectator sport. It requires all actors to play.

Asset owners **Integrators**

Maintainers **Product suppliers**

IACS Patching

IMPORTANCE

- ✓ IACS and the software it relies on is highly vulnerable
- ✓ New vulnerabilities are discovered and published almost daily
- ✓ Malware authors take advantage of these vulnerabilities to exploit systems
- ✓ Old malware still works on unpatched systems

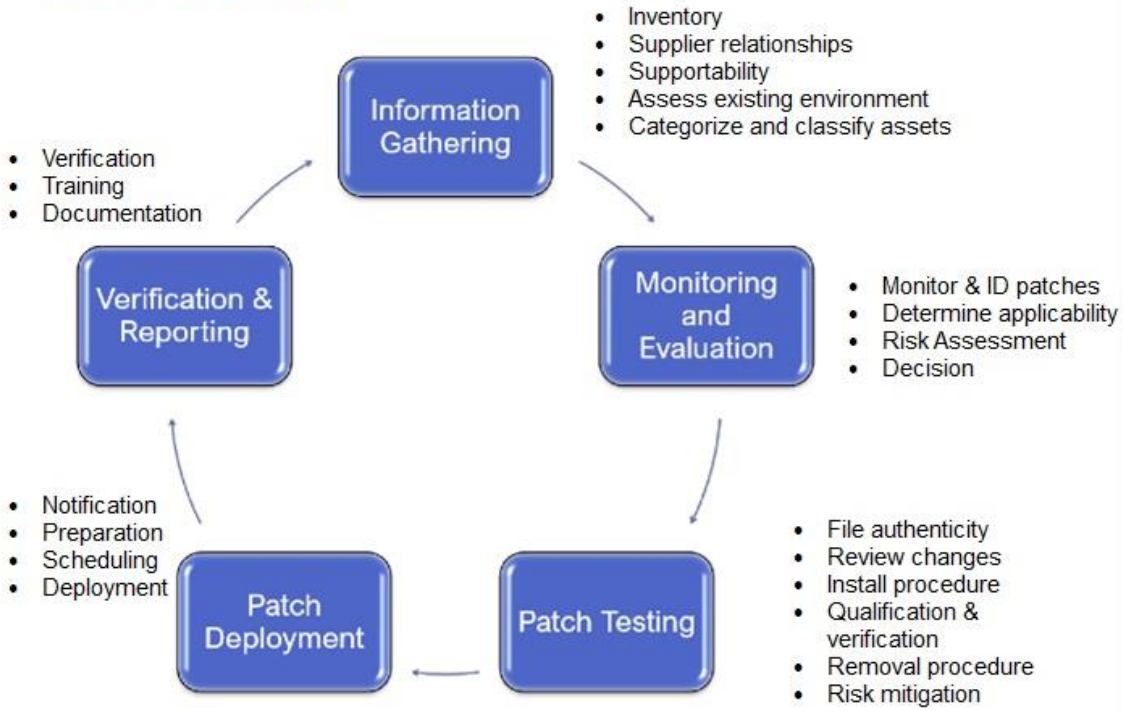
CHALLENGES

- ✓ **Patches are changes!!!**
  - Changes may impact safety, reliability, certification and performance
  - Must be part of change and configuration management process
- ✓ Patching is very resource intensive
- ✓ Infrequent maintenance outages

IACS Patching

Develop the business case

IACS Patching



Source: ISA-TR62443-2-3 "Patch management in the IACS environment"

Notes:

- IACS patch management workflow
- See ISA-TR62443-2-3, Annex B & C

Asset Owner Requirements

Priority Level	Target installation timeframe after approval of the patch by the IACS vendor
High	Within 1 week
Medium (default)	Within 3 months
Low	Within 2 years or next available outage
None	Never

Sample severity based patch management timeframes

Notes:

- IACS patch management workflow
- See ISA-TR62443-2-3, Annex B & C
- Discussion items
    - Change management process will affect timeframes
    - Available outage preferred to be a scheduled outage
    - Not a good practice to start applying patches during unscheduled outage

Product Supplier/Service Provider Requirements

Discovery of Vulnerabilities
- Procedures in place
- Frequency defined

Development, Verification and Validation
- Validate mitigation
- Compensating controls to reduce attack surface

Product Supplier/Service Provider Requirements

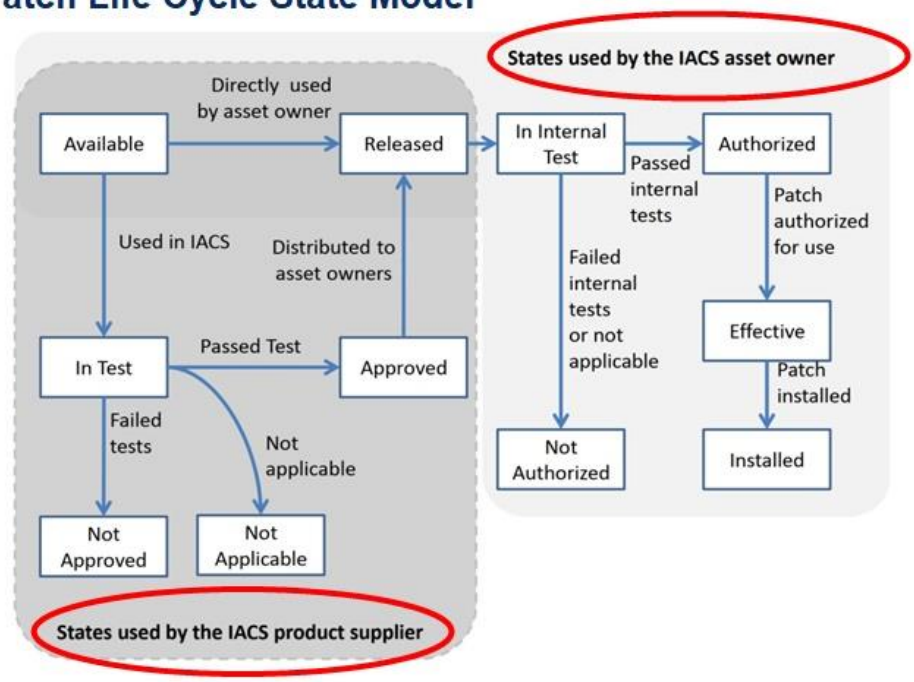
Distribution of Cybersecurity Updates

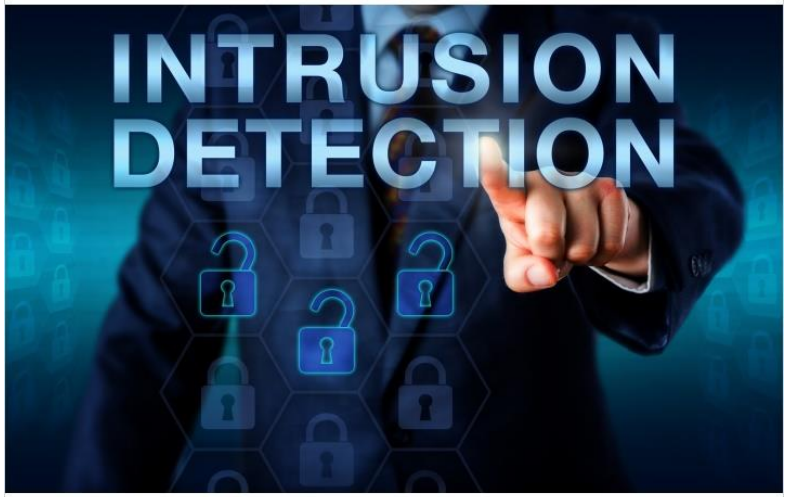
- Available via a secure channel
- Provide patch sources for third-party software used in product
- Windows Server Update Services (WSUS)
- Traditional Microsoft second Tuesday of the month release day
  - Microsoft patch release process is evolving
  - Out-of-band patching

Communication and Outreach

- Address asset owner communications
- Where and how to report a suspected attack or vulnerability
- Communicate to asset owners and system integrators
- Life cycle support

Patch Life Cycle State Model





Intrusion Detection Systems (IDS)

- Tools to detect attempts to break into or misuse a computer system
- Security service monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warnings of, attempts to access system resources in an unauthorized manner
- Allow system admins to respond to potential security issues
- If firewalls and access control systems are the lock on the door
  - IDS is the burglar alarm

Notes:

- IPS generally not used in IACS

Intrusion Prevention Systems (IPS)

Intrusion Prevention Systems (IPS) add the ability to act on intrusion detection by automatically blocking malicious activity

IPS generally not used within IACS zones

As attacks become more sophisticated, tools and techniques will need to become more sophisticated as well

Behavior-based IPS

Types of IDS

Types of IDS

Network Intrusion Detection (NIDS)

- Monitor network traffic
- Pre-defined rules (signature-based)
- Behaviors (heuristics-based)
- Passive Sniffing
- Inline Deployment (bump in the wire)

Host Intrusion Detection (HIDS)

- Monitor host
- Pre-defined rules (signature-based)
- Behaviors (heuristics-based)
- Passive Sniffing

IDS Issues

IDS Issues

- False positives
- Deployment and operational costs
- Only effective against known vulnerabilities
- Limited signatures for control system protocols
- Requires continuous care and feeding

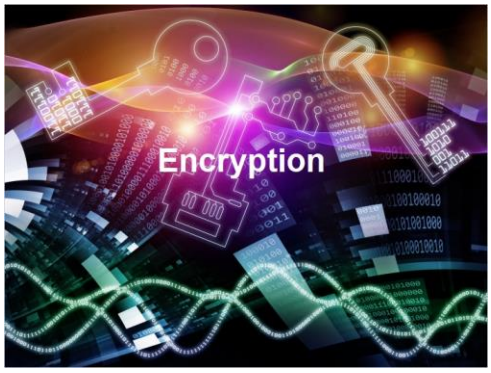
IDS/IPS Best Practices

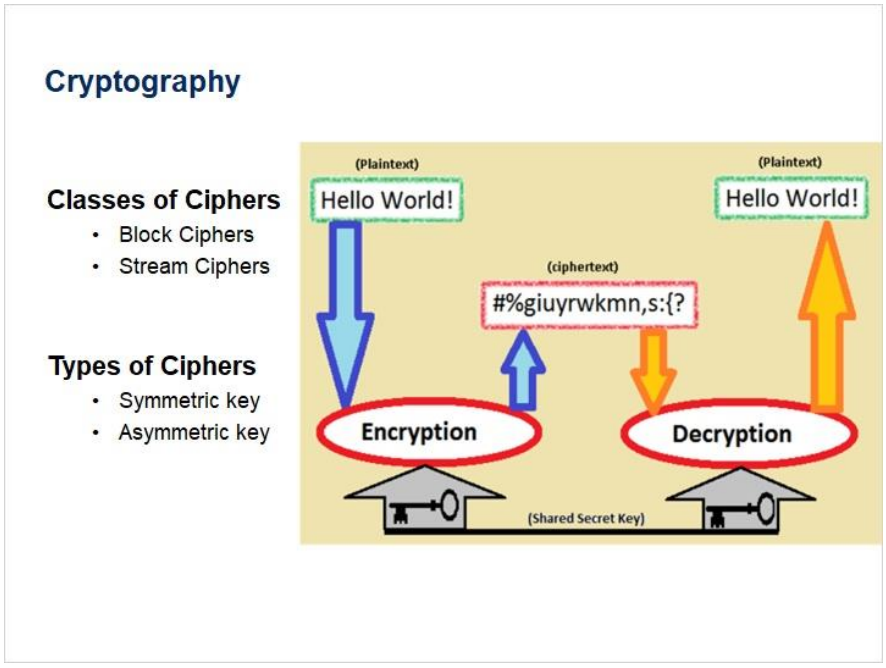
- Distributed deployment – install NIDS at zone entry points
- Enhance IT IDS signatures with SCADA IDS signatures
  - Industrial protocols such as Modbus, DNP3
- Rules written in Snort syntax cover
  - Unauthorized requests
  - Malformed protocol requests and responses
  - Dangerous commands
  - Malicious network behavior
- Intrusion Prevention System (IPS) should be implemented with extreme care to avoid inadvertently blocking necessary traffic

Unified Threat Management (UTM)

Unified Threat Management (UTM)

- Single appliance
- Network firewalling
- Network intrusion prevention
- Gateway antivirus (AV)
- Gateway anti-spam
- VPN
- Content filtering
- Load balancing
- Data leak prevention

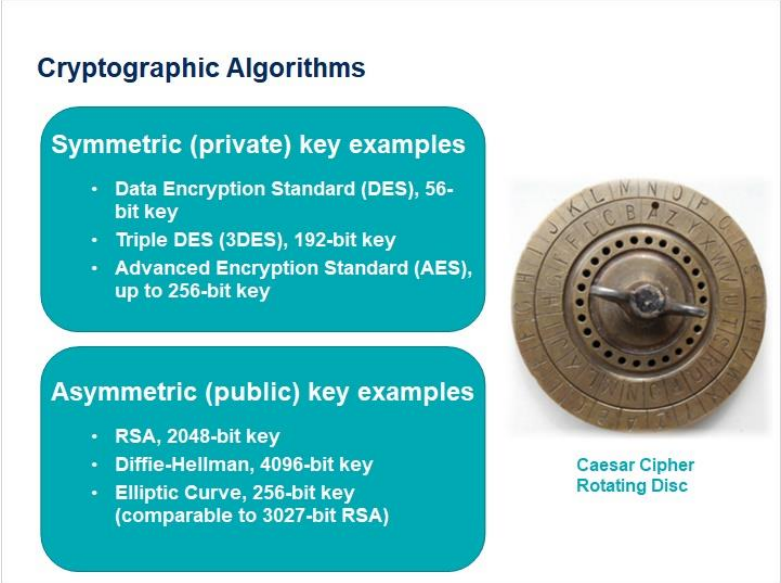




Notes:

Time to break out your secret decoder ring. Another countermeasure to network attacks is by using cryptography.

- The role of cryptography is to secure communication in the presence of a 3rd party, where a plaintext message is encrypted and sent and the decrypted at the receiving end. Cryptography uses ciphers or algorithms for encrypting and decrypting messages.
- Most modern ciphers can be categorized in several ways
- By whether they work on blocks of symbols usually of a fixed size (**block ciphers**), or on a continuous stream of symbols **(stream ciphers**).
- By whether the same key is used for both encryption and decryption (**symmetric key algorithms**), or if a different key is used for each (**asymmetric key algorithms**).



Notes:

- **Symmetric-key algorithms**[1] are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link.[2] This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption
- **Asymmetric or Public-key cryptography** refers to a cryptographic system requiring two separate keys, one of which is secret and one of which is public. Although different, the two parts of the key pair are mathematically linked. One key locks or encrypts the plaintext, and the other unlocks or decrypts the ciphertext. Neither key can perform both functions. One of these keys is published or public, while the other is kept private.
- Public key cryptography uses asymmetric key algorithms (such as RSA), and can also be referred to by the more generic term "asymmetric key cryptography." The algorithms used for public key cryptography are based on mathematical relationships (the most notable ones being the integer factorization and discrete logarithm problems) that have no efficient solution. Although it is computationally easy for the intended recipient to generate the public and private keys, to decrypt the message using the private key, and easy for the sender to encrypt the message using the public key, it is extremely difficult (or effectively impossible) for anyone to derive the private key, based only on their knowledge of the public key. This is why, unlike symmetric key algorithms, a public key algorithm does *not* require a secure initial exchange of one (or more) secret keys between the sender and receiver. The use of these algorithms also allows the authenticity of a message to be checked by creating a digital signature of the message using the private key, which can then be verified by using the public key. In practice, only a hash of the message is typically encrypted for signature verification purposes
- **Data Encryption Standard** (**DES**) is a previously predominant algorithm for the encryption

of electronic data. It was highly influential in the advancement of modern cryptography in the academic world

- **Some Symmetric algorythms are:**
- ***3DES*** is a mode of the DES encryption algorithm that encrypts data three times. Three 64-bit keys are used, instead of one, for an overall key length of 192 bits (the first encryption is encrypted with second key, and the resulting cipher text is again encrypted with a third key).
- **Advanced Encryption Standard** (**AES**) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2002. Originally called **Rijndael**, the cipher was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted to the AES selection process.
- **Blowfish** is a keyed, symmetric block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. However, the Advanced Encryption Standard now receives more attention
- **Twofish** is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. It was one of the five finalists of the Advanced Encryption Standard contest, but was not selected for standardization. Twofish is related to the earlier block cipher Blowfish.

- **Some Asymmetric Algorythms are:**
- **RSA** is an Internet encryptionand authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Microsoft and Netscape
- Jump to: navigation, search
- **Diffie-Hellman key exchange** is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie-Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.
- **ElGamal encryption system** is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie-Hellman key exchange.

File Hashing

What is hashing?

- Creating a unique identifier of some chunk of data

What are cryptographic hashing algorithms?

- One-directional math formula used to generate a unique hex signature

What are some common algorithms?

- Message Digest (MD5)
- Secure Hash Algorithm (SHA-1, SHA-256, SHA-512)

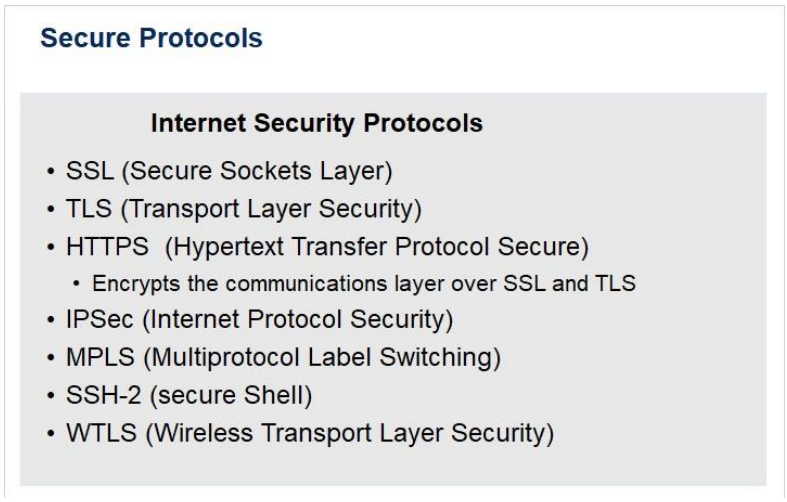
Why should I care about hashing?

- Verify that data is legitimate and has not been tampered with

Where can I learn how to hash my data?

- See Additional Resources tab File Hashing white paper
- Browser search on "NCCIC ICS_Factsheet_File_Hashing_S508C.pdf"

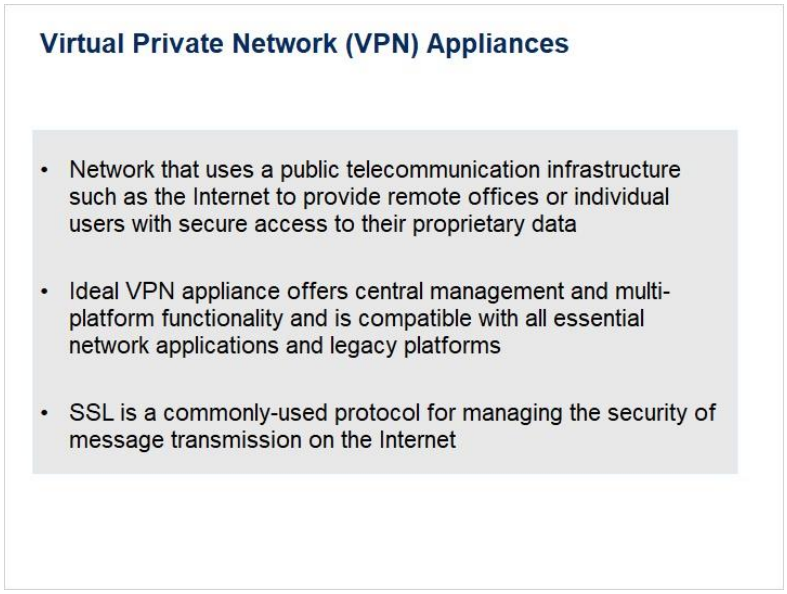
Making Wise Choices



Notes:

Some secure protocols for the internet are:

- **Transport Layer Security** (**TLS**) and its predecessor, **Secure Sockets Layer** (**SSL**), are cryptographic protocols that provide communication security over the Internet[] TLS and SSL encrypt the segments of network connections at the Application Layer for the Transport Layer, using asymmetric cryptography for key exchange, symmetric encryption for confidentiality, and message authentication codes for message integrity.
- **Secure Hypertext Transfer Protocol** (**S-HTTP**) is a little-used alternative to the HTTPS URI scheme for encrypting web communications carried over HTTP.
- **Internet Protocol Security** (**IPsec**) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.
- **Multiprotocol Label Switching** (**MPLS**) is a mechanism in high-performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table. The labels identify virtual links (*paths*) between distant nodes rather than endpoints. MPLS can encapsulate packets of various network protocols
- **Secure Shell** (**SSH**) is a cryptographic network protocol for secure data communication, remote shell services or command execution and other secure network services between two networked computers that it connects via a secure channel over an insecure network: a server and a client (running SSH server and SSH client programs, respectively). The protocol specification distinguishes two major versions that are referred to as SSH-1 and SSH-2.
- **Wireless Transport Layer Security (WTLS)** is part of the Wireless Application Protocol (WAP) stack. WTLS is derived from TLS and uses similar semantics adapted for a low bandwidth mobile device. WTLS uses modern cryptographic algorithms and in common with TLS allows negotiation of cryptographic suites between client and server.



Notes:

- **A VPN appliance** is a network device equipped with enhanced security features. Also known as an SSL (Secure Sockets Layer) VPN appliance, it is in effect a router that provides firewall protection, load balancing, authorization, authentication and encryption for VPNs.
- A VPN (virtual private network) is a network that uses a public telecommunication infrastructure such as the Internet to provide remote offices or individual users with secure access to their proprietary data. SSL is a commonly-used protocol for managing the security of message transmission on the Internet. The ideal VPN appliance offers central management and multi-platform functionality and is compatible with all essential network applications and legacy platforms.
- VPNs employ the following for security:

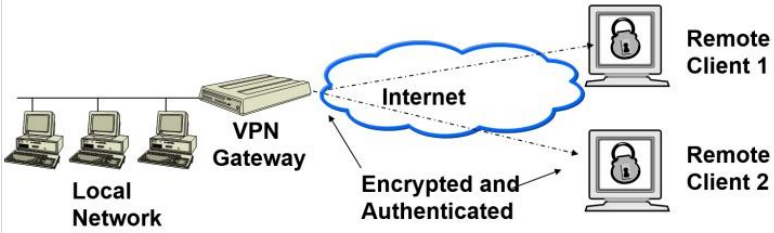
1.IPSec - Internet Protocol Security
2.SSL/TLS Transport Layer Security
3.DTLS Datagram Transport Layer Security
4.MPPE Microsoft Point to Point Encryption
5.SSTP Secure Socket Tunneling protocol
6.MPVPN Multi Path Virtual Private Network
7.SSH Secure Shell

Site-to-Site VPNs

- The two endpoints of the VPN are intermediary devices that pass traffic from a trusted network to another trusted network while relying on the VPN technology to secure the traffic on the untrusted transport network
- Commonly called site-to-site or LAN-to-LAN VPNs

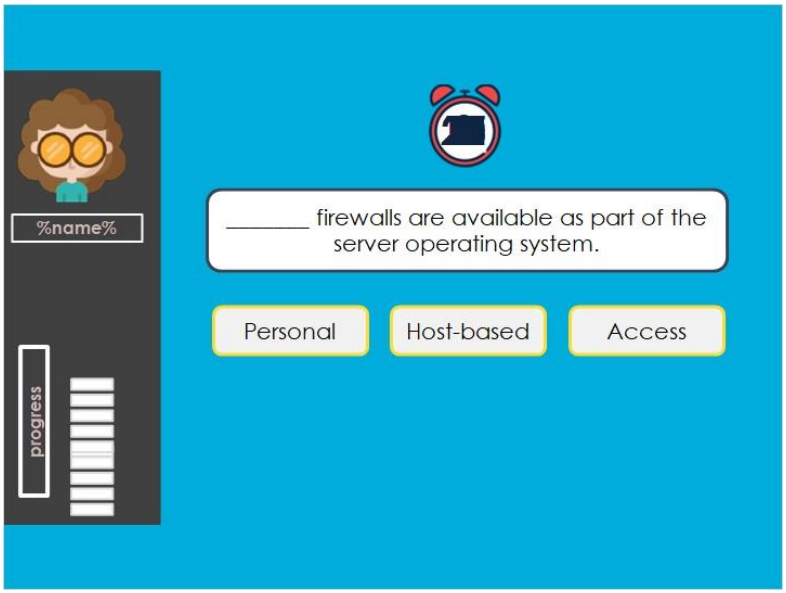
Remote Access VPNs

- One endpoint is a host computing device and the other endpoint is an intermediate device that passes traffic from the host to the trusted network behind the security gateway while relying on the VPN technology to secure the traffic on the untrusted network
- Commonly called remote access service (RAS) VPNs

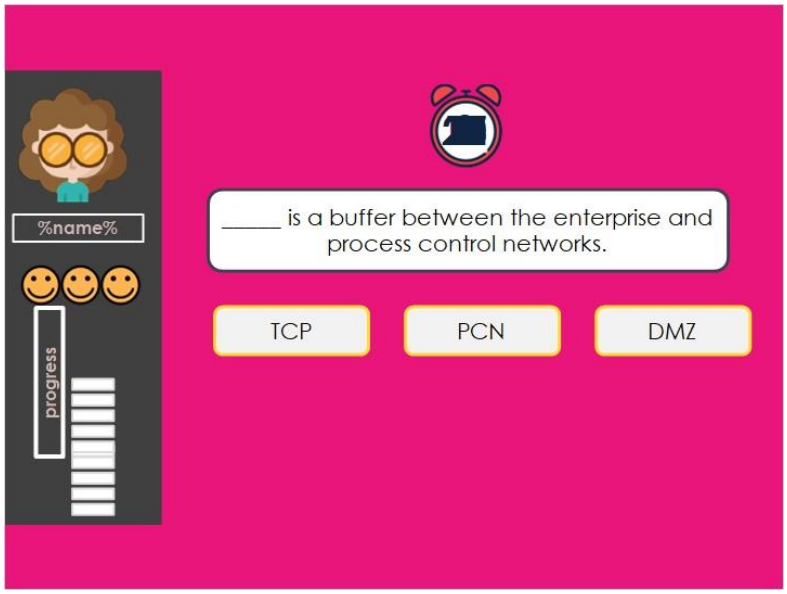


Notes:

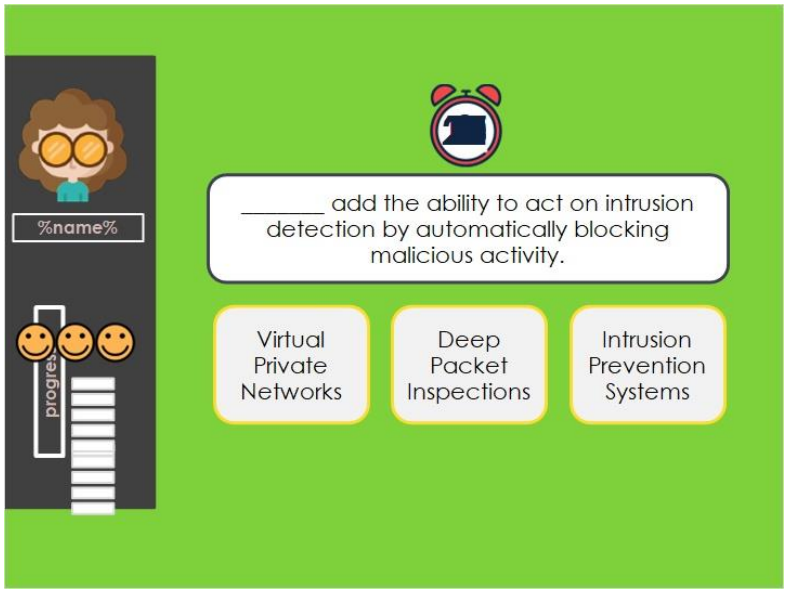
- VPN is a more secure way of connecting to a plant from home or remote office than simple modem or DSL line
- Provides encryption for authentication session and content
- Can also be firewall to firewall to interconnect two LANS



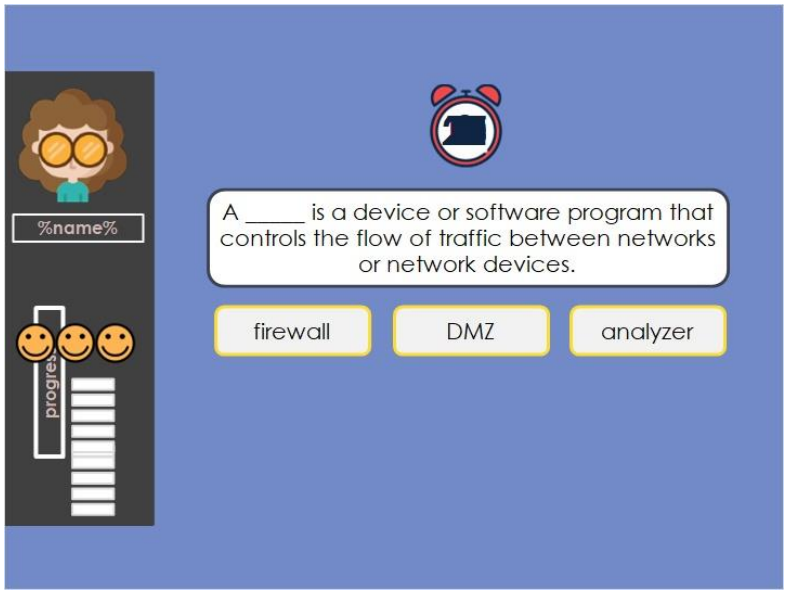
Correct	Choice
X	Host-based



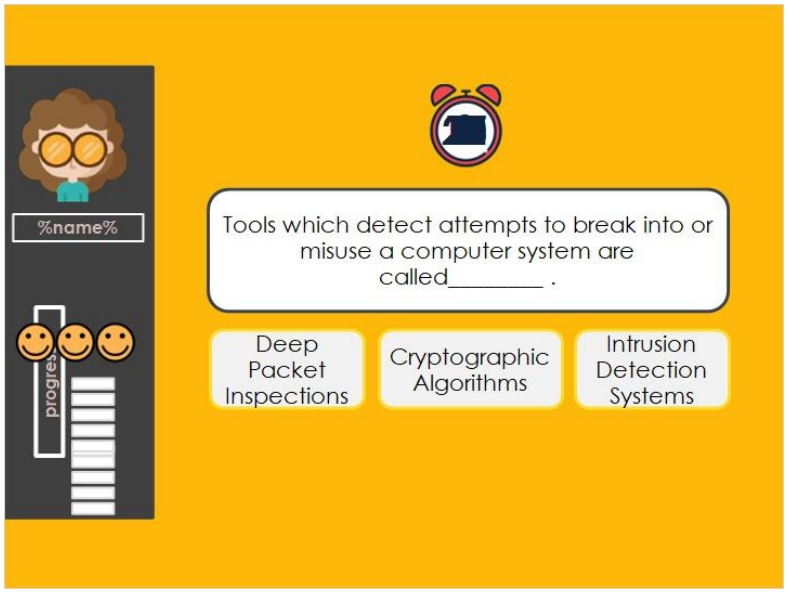
Correct	Choice
X	DMZ



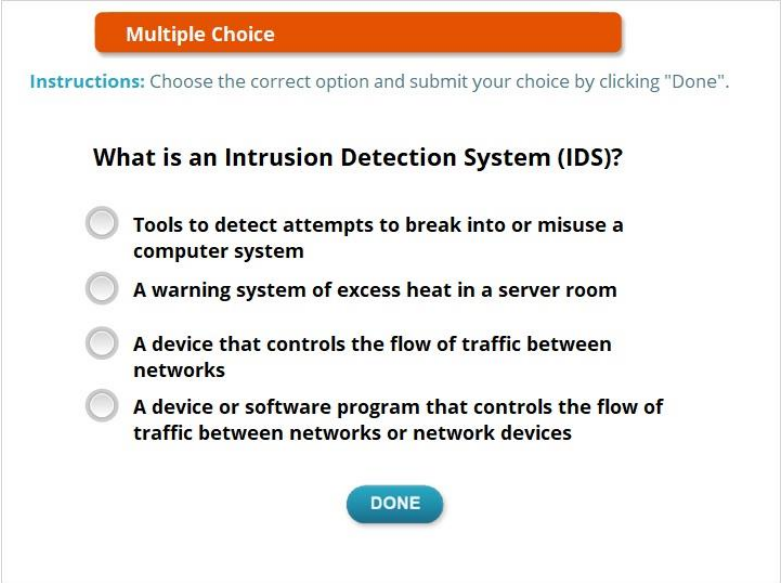
Correct	Choice
X	Deep Packet Inspections



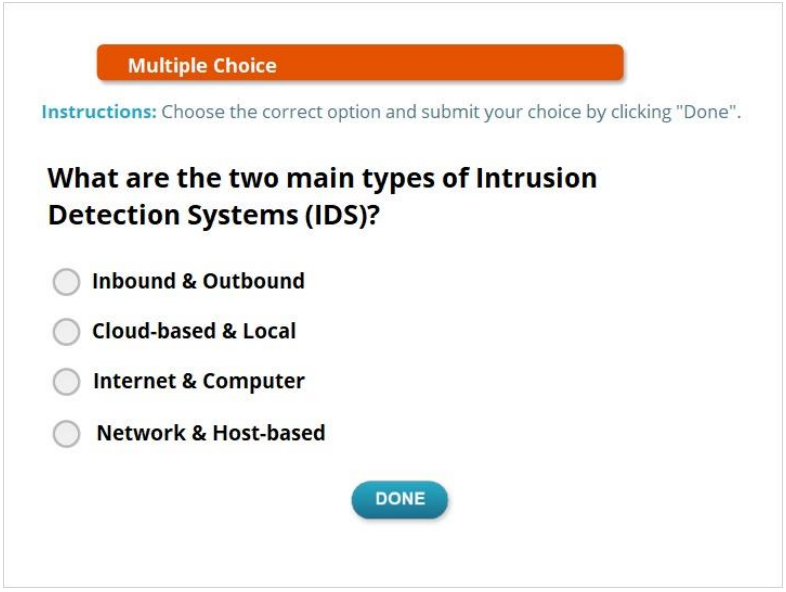
Correct	Choice
X	firewall



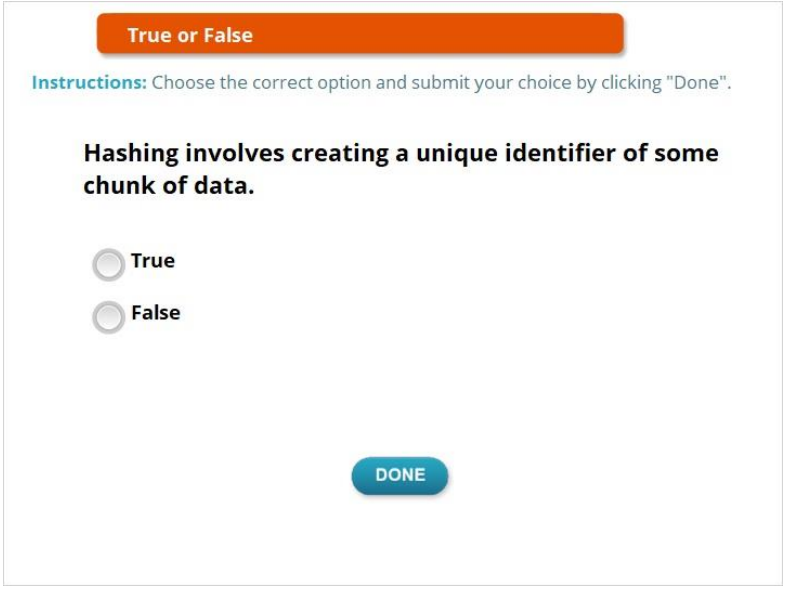
Correct	Choice
X	Cryptographic Algorithms



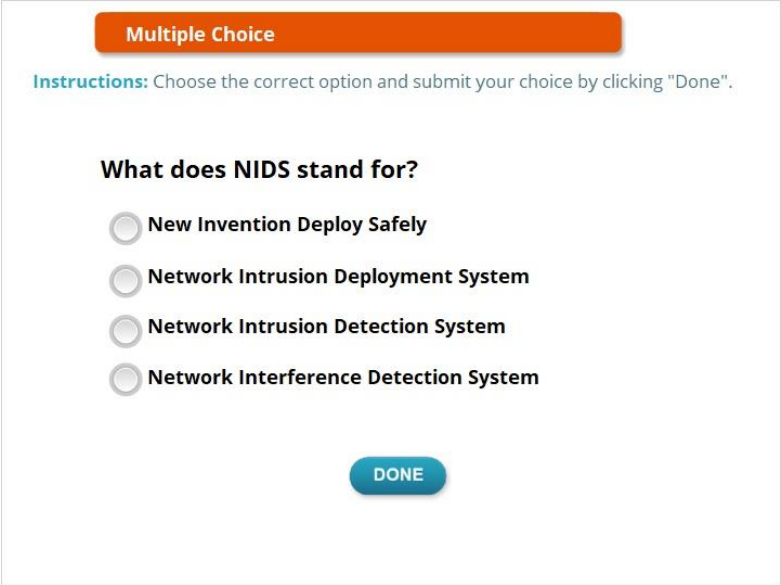
Correct	Choice
X	Radio Button 1



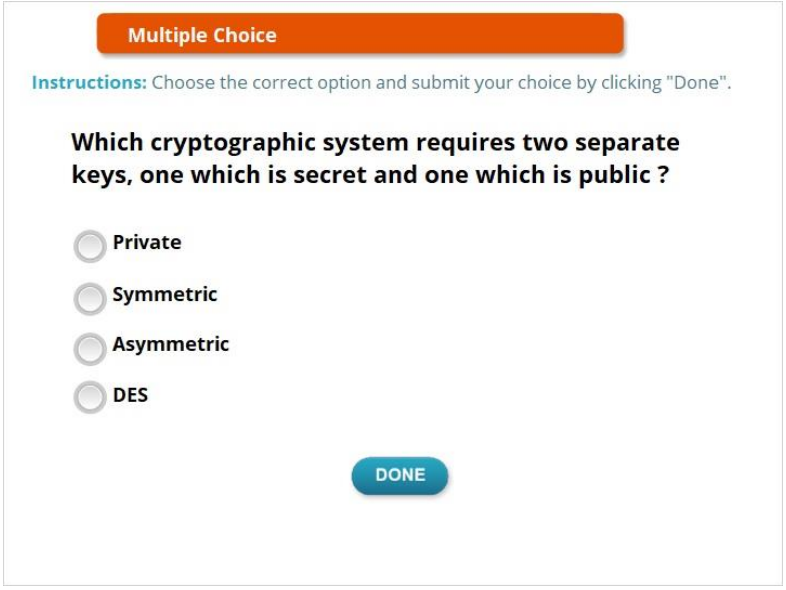
Correct	Choice
	Network & Host-based



Correct	Choice
X	Radio Button 1



Correct	Choice
X	Radio Button 3



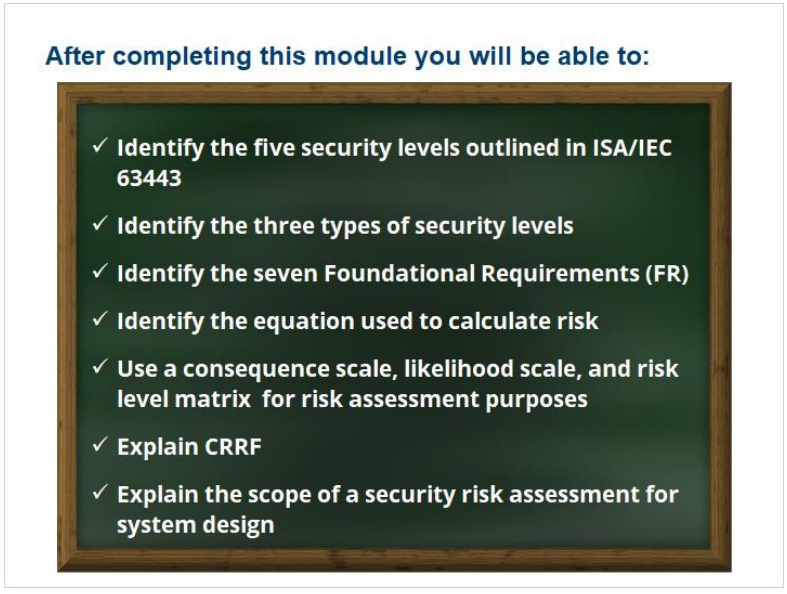
Correct	Choice
X	Radio Button 3

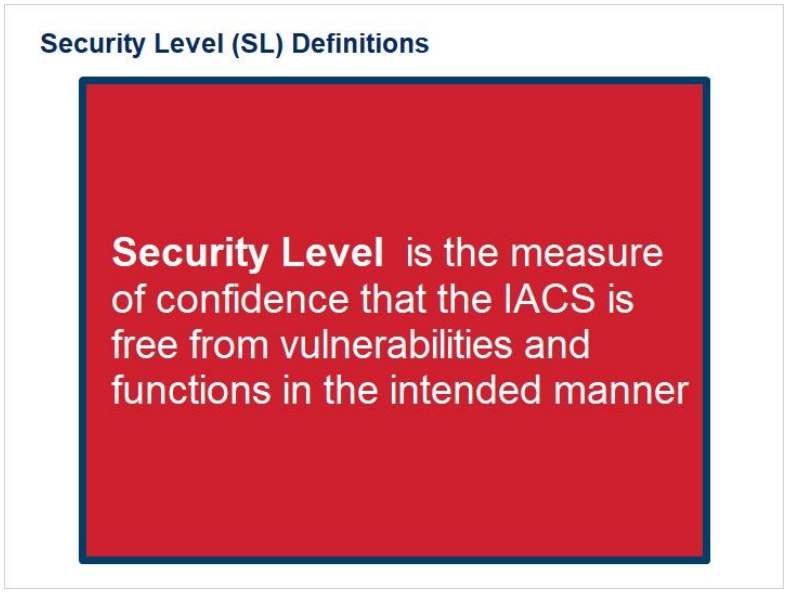
Week 7

Week 7
Week 7
Week 7
Week 7
Week 7

Setting the Standard for Automation™

IC329 Module 11





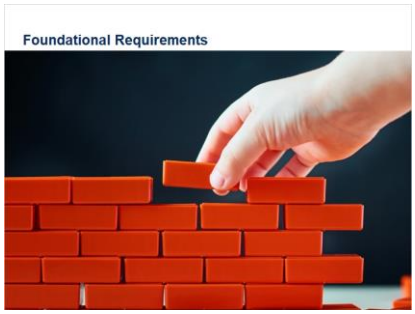
Notes:

- SL is defined in ISA 62443-3-3 (copy in Noteset Volume II), annex A, pg 67
- More detail defined in other standards

2.8 Types of Security Levels (SL)

Notes:

- Types of SL covered in Annex A of ISA 62443-3-3



Foundational Requirements

- The simple CIA model shown earlier is not adequate for a full understanding of the requirements for security in IACS

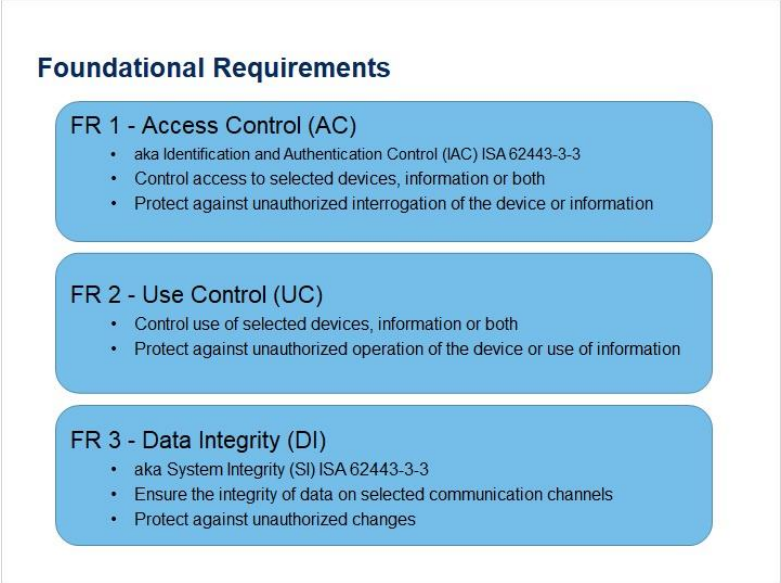
- Seven basic or Foundational Requirements (FR) have been identified for IACS that includes CIA model

- All FRs are within the scope of all standards
  - We will use FR terms/acronyms located in Part 3-3
  - In some cases more detailed normative information is provided by other standards

ANSI/ISA-62443-1-1, subclause 5.2.1, pg 37
ANSI/ISA-62443-3-3, Annex A, subclause A.3.1, pg 72

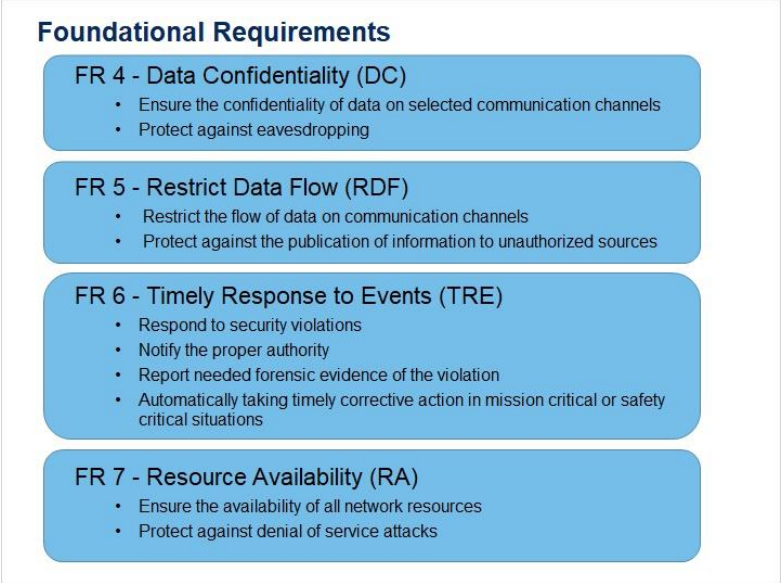
Notes:

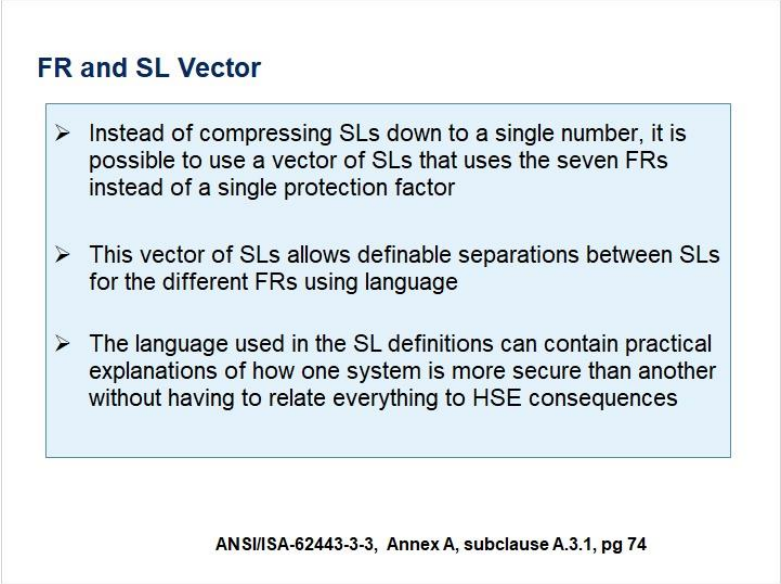
- CIA = Confidentiality, Integrity, Availability
- ISA 62443-1-1 and ISA 62443-3-3 refer to the foundational requirements
- There are 7 Foundational Requirements (FR) in the ISA 62443 series.
- Note that there are some terminology differences in the FR's due to ISA 62443 series changes since 2007



Notes:

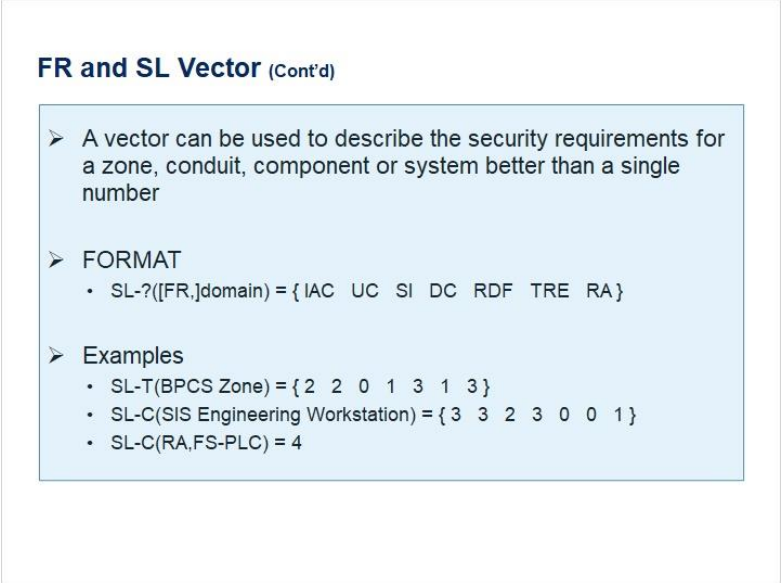
- There are 7 Foundational Requirements (FR) in the ISA 62443 series.
- Note that there are some terminology differences in the FR's due to ISA 62443 series changes since 2007
    - The definitions and concepts have not changed
    - FR IAC versus AC
    - FR SI versus DI
    - FR RA versus NRA
- There are a number of ISA/IEC 62443 Foundational Requirements (FR) and/or Component Requirements (CR) that have been updated and are out for final comment/vote.
    - Thus terms may not align across the 62443's
    - As the related ISA/IEC 62443 standards are approved the terms will be aligned.
- The original ANNSI/ISA-99.00.01-2007, clause 5.2.1 uses AC, DI and RA.
    - Work group 3 is currently working on a second edition of the ISA-62443-1-1 standard which will reflect changes to common material that has been developed since 2007. A draft of the working document is available for review and comment .
        - http://isa99.isa.org/ISA99%20Wiki/WP-1-1.aspx (retrieved 29 June 2016)





Notes:

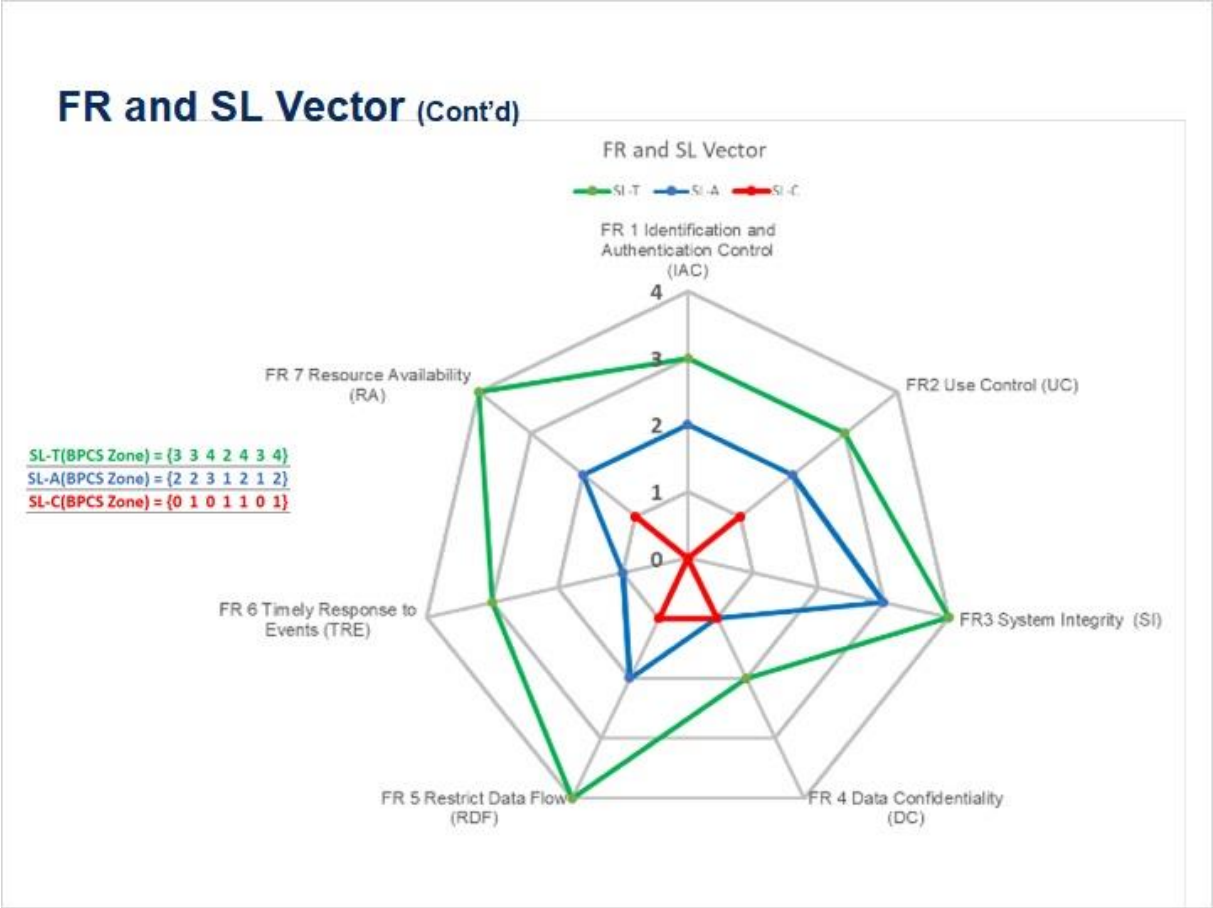
- ISA-62443-3-3, Annex A, A.3.1, page 74
- FR = Foundational Requirements
- SL = Security Levels



Notes:

- ISA-62443-3-3, Annex A, A.3.1, page 72
- FR = Foundational Requirements
- SL = Security Levels

FR and SL Vector (Cont'd)



Notes:

- Depicting FR and SL as radar/spider chart quickly shows where resources may need to be leveraged to cover a shortfall
- ISA-62443-3-3, Annex A, A.3.3.3, page 74
- FR = Foundational Requirements
- SL-A = Achieved Security Level
- SL-T = Target Security Level
- SL-C = Capability Security Level (not shown)
- Comparison of CIA = FR4 DC, FR3 DI, FR7 RA

Notes:

- We have discussed Foundational Requirements and Security Levels
- We can move on to Risk Assessment

Risk Assessment Overview
Risk Equation

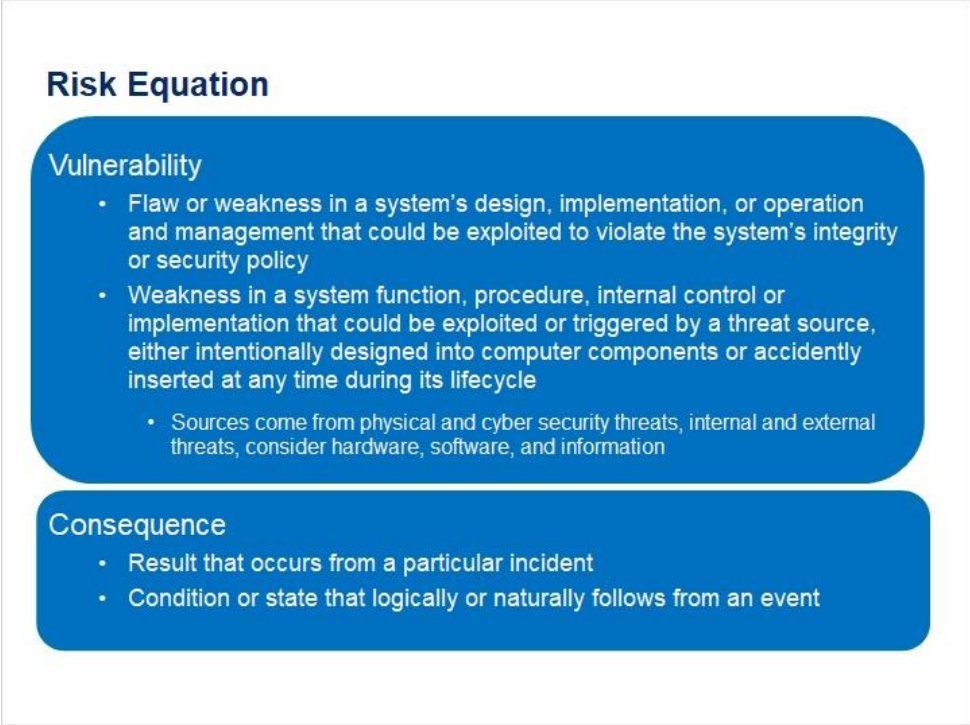
Risk = Threat x Vulnerability x Consequence

Threat

- Potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm
- Circumstance or event with the potential to adversely affect operations (including mission, functions, image or reputation), assets, control systems or individuals via unauthorized access, destruction, disclosure, modification of data and/or denial of service

Notes:

- ISA-62443-2-1, Risk equation, pg 61
- Definitions as used in ISA-62443 series in next few bullets and slides
- Sets a common baseline so that we are all on the same page
- Definitions are broad.
- Threat definition ISA-62443-1-1 pg 30 and ISA-62443-3 pg 20
- All of the following examples are typical approaches
    - Good start
    - In the real world examples are just that; examples, not mandated
- Each organization needs to determine its approach



Notes:

- Vulnerability definition ISA-62443-1-1 pg 31
- No magic table or list for Vulnerability exists, many sources that vary based on your IACS
- Consequence definition ISA-62443-2-1 and ISA-62443-3-3

Notes:

- Based loosely on a real world scenario that recently made the headlines
- First Simplify Risk equation to Risk = Likelihood x Consequence

Use Case – Financial Impact

What is the likelihood for a virus to cripple the IACS?

First it needs to be a viable virus that can affect the IACS

- Windows virus on a Unix system not a big concern
- Windows virus on unpatched Windows operating system a big concern
- What do you mean we still have an XP SP2 machine running!!!

Second it needs to reach the IACS

- Many vectors available for that, including sneaker net

Third it needs to defeat antivirus controls on the IACS

- The virus signatures are up to date, aren't they?

What does the Reasonable Person On the Street say?

- Chances are good IACS could get hit by virus in the next year

Notes:

- Based loosely on a real world scenario that recently made the headlines
- Manage your time. Risk assessment can be fun, but there is no intention or time to get into the intricate details in IC32. This is a fundamental course.

Likelihood Scale

We have determined that the likelihood of a virus to cripple the IACS is possible

- ✓ Establish a category of high, medium, low
- ✓ Use existing Scale matrix
- ✓ In the case of the virus, chances are good network could get hit by one in the next year

Likelihood	
Category	**Description**
High	A threat/vulnerability whose occurrence is likely in the next year.
Medium	A threat/vulnerability whose occurrence is likely in the next 10 years.
Low	A threat/vulnerability for which there is no history of occurrence and for which the likelihood of occurrence is deemed unlikely.

Likelihood Category = High

Notes:

- Point out that this is a typical likelihood scale found in part 2-1, pg 61.
- It is not prescriptive
- Each organization may have their own already created on the business side of the house
- You will have an increased chance of getting buyoff if you can use something that matches up with existing risk process on business side.
- We now have likelihood category high
- ISA-62443-2-1, Table A.1, pg 61

Consequence Scale

Determine consequence for each risk area

Consequence

	Risk area								
	Business continuity planning		Information security			Industrial operation safety		Environmental safety	National impact
Category	Manufacturing outage at one site	Manufacturing outage at multiple sites	Cost (million USD)	Legal	Public confidence	People – on-site	People – off-site	Environment	Infrastructure and services
A (high)	> 7 days	> 1 day	> 500	Felony criminal offense	Loss of brand image	Fatality	Fatality or major community incident	Citation by regional or national agency or long-term significant damage over large area	Impacts multiple business sectors or disrupts community services in a major way
B (medium)	> 2 days	> 1 hour	>5	Misdemeanor criminal offense	Loss of customer confidence	Loss of workday or major injury	Complaints or local community impact	Citation by local agency	Potential to impact a business sector at a level beyond that of a single company. Potential to
C (low)	< 1 day	< 1 hour	< 5	None					

Use financial COST (million USD) impact for this walk through (USD = United States Dollars)

Virus resulting in operations upset of 8 days of off-specification product that cannot be sold

Financial loss is 41 million USD = Cost >5
Consequence Category = B (medium)

Notes:

- Could have very high financial impact to the company but medium/low impacts in other areas
- Off specification product could be aluminum
- Use financial impact for this walk through
- Cost of first week has been 41 million USD which is >5 million USD = Category B (Medium)
- ISA-62443-2-1, Table A.2, pg 63
- **Stress that this is a typical likelihood scale found in part 2-1. It is not prescriptive**
- Each organization may have their own already created on the business side of the house

Risk Level Matrix

Matrix is tool for establishing first go around on assessing risk
- Provides starting point for financial COST example

Risk = Likelihood x Consequence

Proceed using organization's matrix to determine Risk Response to a Risk that has been categorized High-Risk

Likelihood of virus = High **Consequence Category = B (Medium)**

		Consequence category		
		A	B	C
Likelihood	High	High-risk	High-risk	Medium-risk
	Medium	High-risk	Medium-risk	Low-risk
	Low	Medium-risk	Low-risk	Low-risk

Notes:

- ISA-62443-2-1, Risk equation, pg 61
- Risk level matrix ISA-62443-2-1, pg 64
- Stress that this is a typical likelihood scale found in part 2-1. It is not prescriptive
- Each organization may have their own already created on the business side of the house
- The organizational matrixes can get very complex and detail down to 25 categories.

Risk Assessment

Likelihood

Likelihood = Threat x Vulnerability

Quantitative chance that an action, event or incident may occur

Likelihood	
Category	**Description**
High	A threat/vulnerability whose occurrence is likely in the next year.
Medium	A threat/vulnerability whose occurrence is likely in the next 10 years.
Low	A threat/vulnerability for which there is no history of occurrence and for which the likelihood of occurrence is deemed unlikely.

Notes:

- ISA-62443-2-1, Risk equation, pg 61
- (Eq. A.1) Likelihood (Event_Occurring)= Likelihood (Threat_Realized) × Likelihood (Vulnerability_Exploited)
- (Eq. A.2) Risk = Likelihood (Event_Occurring) × Consequence
    - Risk = **Threat x Vulnerability** x Consequence
- ISA-62443-2-1 Likelihood definition, pg 17
- Typical Likelihood scale, pg 61

Example Consequence Scale

Consequence									
	Risk area								
	Business continuity planning		Information security			Industrial operation safety		Environmental safety	National impact
Category	Manufacturing outage at one site	Manufacturing outage at multiple sites	Cost (million USD)	Legal	Public confidence	People – on-site	People – off-site	Environment	Infrastructure and services
A (high)	> 7 days	> 1 day	> 500	Felony criminal offense	Loss of brand image	Fatality	Fatality or major community incident	Citation by regional or national agency or long-term significant damage over large area	Impacts multiple business sectors or disrupts community services in a major way
B (medium)	> 2 days	> 1 hour	> 5	Misdemeanor criminal offense	Loss of customer confidence	Loss of workday or major injury	Complaints or local community impact	Citation by local agency	Potential to impact a business sector at a level beyond that of a single company. Potential to impact services of a community
C (low)	< 1 day	< 1 hour	< 5	None	None	First aid or recordable injury	No complaints	Small, contained release below reportable limits	Little to no impact to business sectors beyond the individual company. Little to no impact on community services

ISA-62443-2-1, Table A.2, pg 63

Risk Assessment

Risk equation

Risk = **Threat x Vulnerability** x Consequence

Threat x Vulnerability = **Likelihood**

		Consequence category		
		A	B	C
Likelihood	High	High-risk	High-risk	Medium-risk
	Medium	High-risk	Medium-risk	Low-risk
	Low	Medium-risk	Low-risk	Low-risk

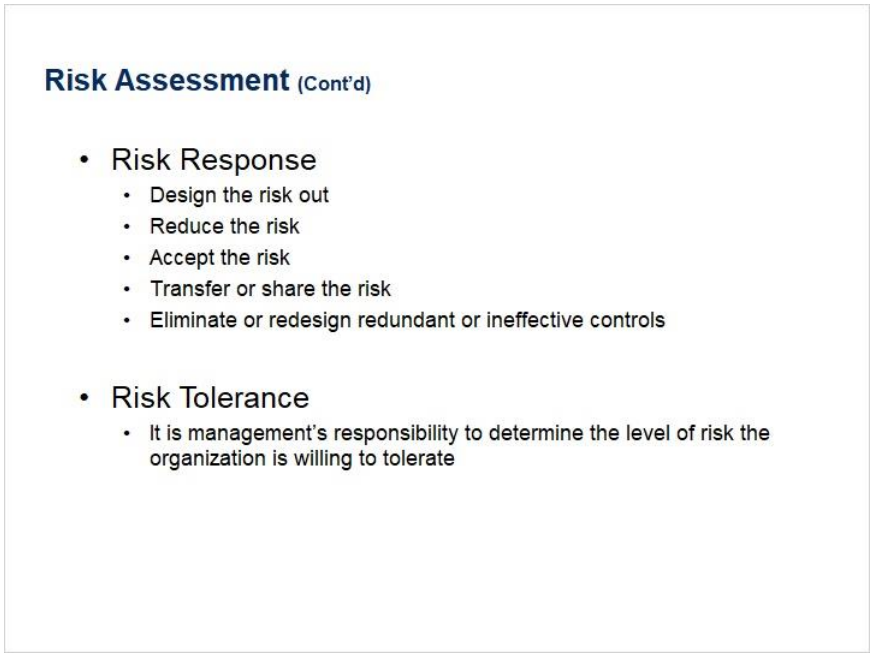
Notes:

- ISA-62443-2-1, Risk equation, pg 61
- Typical likelihood scale, ISA-62443-2-1, pg 61

Risk Assessment (Cont'd)

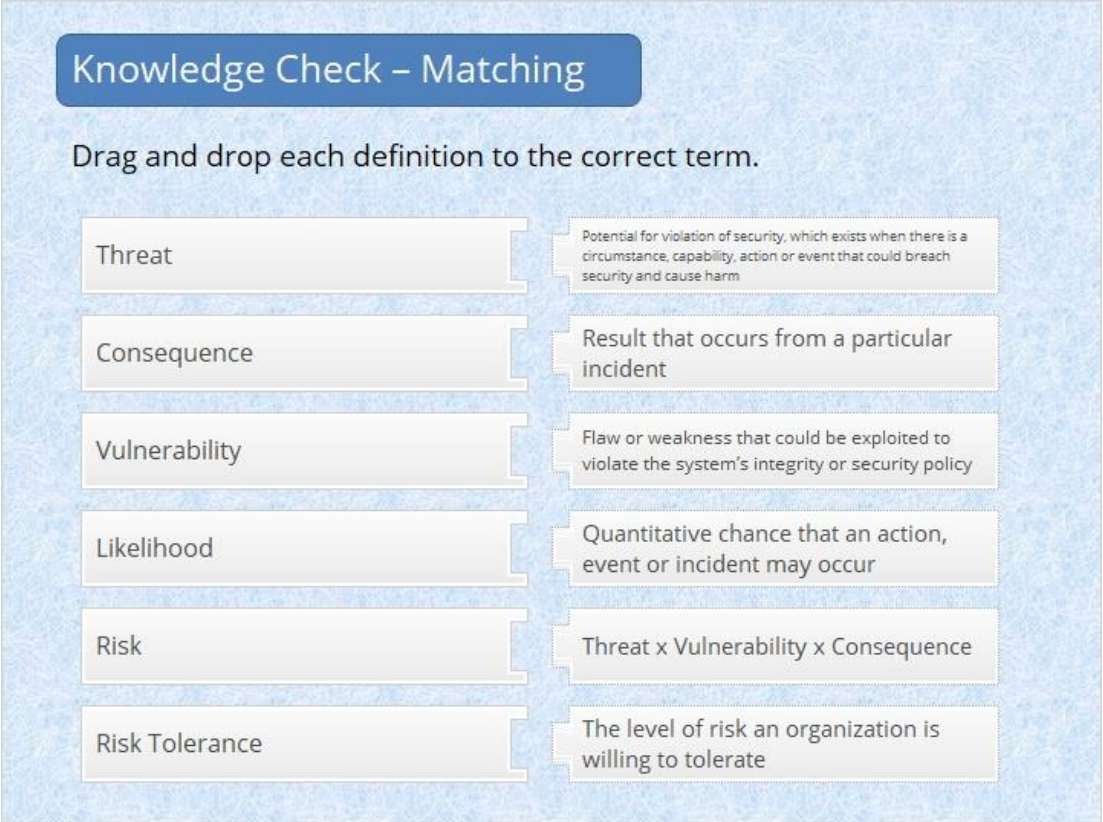
A good risk assessment should provide the following information for the entire system as well as for each zone and conduit:

- Risk profile
- Highest severity consequences
- Threats and vulnerabilities leading to the highest risks
- Target Security Levels
- Recommendations



Notes:

- a) **Design the risk out - One form of mitigation is to change the design of the system so the risk is**
- removed. Some risks exist simply because access is available to something to which no access
- is ever needed. Completely disabling the unnecessary function or "welding" the function from
- access can mitigate the risk. Organizations can make the appropriate business decisions so the
- risk is not taken. This response may involve saying no to something, whether a new vendor
- product, system, or relationship.
- b) **Reduce the risk - Risks can be decreased to an acceptable level through the implementation of**
- countermeasures that reduce the likelihood or consequence of an attack. The key here is to
- achieve a level of "good enough" security, not to eliminate the risk.
- c) **Accept the risk - There is always an option to accept the risk, to see it as the cost of doing**
- business. Organizations must take some risks, and they cannot always be cost effectively
- mitigated or transferred.
- d) **Transfer or share the risk - It may be possible to establish some sort of insurance or**
- agreement that transfers some or all of the risk to a third entity. A typical example of this is
- outsourcing of specific functions or services. This approach cannot always be effective, because
- it may not always cover all assets completely. An electronic security policy can recover certain
- damages, but not logical assets such as loss of customer confidence.
- e) **Eliminate or redesign redundant or ineffective controls - A good risk assessment process**
- will identify these types of controls that need to be addressed so that more attention can be
- focused on controls that are effective and efficient.



Correct	Choice
Threat	Potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm
Consequence	Result that occurs from a particular incident
Vulnerability	Flaw or weakness that could be exploited to violate the system's integrity or security policy
Likelihood	Quantitative chance that an action, event or incident may occur
Risk	Threat x Vulnerability x Consequence
Risk Tolerance	The level of risk an organization is willing to tolerate

NOTE: Answers in module are shuffled so they will appear in a different order.

Risk Assessment for System Design

Notes:

- Purpose of this section is to briefly highlight the risk assessment approach ISA-62443-3-2
- Noteset does not have a copy of this standard
- **PLEASE DO NOT TRY TO COMPARE TABLES AND MATRIXES FROM PREVIOUS RISK ASSESSMENT SECTION TO THIS SECTION**
    - There is no direct relationship to the previous section
    - Both are valid risk assessments processes based on ISA-624443 series
    - Both sections are **examples** of an approach-not set in stone by the standards
    - Each organization must determine their approach and adoption of process
- This approach leans toward Safety Integrity Level (SIL) ISA 84
    - RRF (risk reduction factor) used in SILs as defined in IEC EN 61508
- IC33/IC34 have more information
- There is no intent to get into the weeds with CRRF in IC32
    - Just be aware it exists and is part of the ISA-62443's

ISA-62443-3-2

Security risk assessment for system design

- Draft 6, Edit 3 out for review and committee draft for vote (CDV)
- Check ISA99 SharePoint site for latest status

Purpose is to align risk ranked vulnerabilities

- ISA-62443-3-3 system security requirements and security levels
- Uses a risk reduction factor approach similar to Safety Integrated Levels of ISA-84

Scope

- Define System under Consideration (SuC)
- Partition SuC into zones and conduits
- Assess risk
- Establish Security Level Target (SL-Ts)
- Document requirements

Notes:

- We have covered Zones and Conduits
- We have touched on Target Security Level (SL-T)
- We have not mentioned Cyber Risk Reduction Factor (CRRF) or System under Consideration (SuC)
- Next few slides will cover a bit more about SuC, SL-T and CRRF

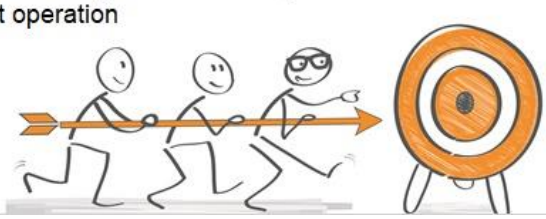
Security Risk Assessment for System Design

System under Consideration (SuC)

- Defined collection of IACS and related assets for the purpose of security risk analysis
- Consists of one or more zones and related conduits
- All assets belong to either a zone or conduit

Target Security Level (SL-T)

- Measure of confidence based on security policy and consequence analysis
- This is usually determined by performing a risk assessment on a system and determining that it needs a particular level of security to ensure its correct operation



Security Risk Assessment for System Design (Cont'd)

- Achieved Security Level (SL-A)
  - Actual level of security
  - Measured after a system design is available
  - Additional compensating countermeasures in place
  - Used to measure that the Target Security Level (SL-T) goal is met
- Capability Security Level (SL-C)
  - Built in to a device or system when properly configured
  - Capable of meeting a Target Security Level (SL-T) without additional compensating countermeasures

Security Risk Assessment for System Design (Cont'd)

- A Target Security Level (SL-T) shall be provided or established for each security zone or conduit
- SL-T is dependent upon the Cyber Risk Reduction Factor (CRRF)
- CRRF is a measure of the degree of risk reduction required to achieve tolerable risk
- CRRF is a ratio that is calculated by dividing unmitigated risk by tolerable risk
- A relationship between CRRF and SL-T will need to be established based upon the organization's
  - risk matrix
  - risk tolerance

Security Risk Assessment for System Design (Cont'd)

- **Cyber Risk Reduction Factor (CRRF)**
  Measure of the degree of risk reduction required to achieve tolerable risk

  CRRF = Unmitigated Risk / Tolerable Risk

- **Potentially hazardous process taken into account**
  - Process hazard analysis (PHA)
  - Functional safety assessments (FSA)

- **Threat intelligence**
  - Government sources
  - Sector specific intel
  - Other relevant sources

Notes:

- Cyber Risk Reduction Factor (CRRF) is analogous to Risk Reduction Factor (RRF) in S84/IEC 61511 safety instrumented system design
- It is a measure of the amount of risk reduction needed to reduce the risk to tolerable level.

Security Risk Assessment for System Design (Cont'd)

- **Establishment of zones and conduits**
  - Group IACS and related assets
  - Criticality of assets
  - Operational function
  - Physical location
  - Logical location
- **Separation of business and control system zones**
  - Logically
  - Physically
  - Impact to health, safety and environment (HSE)

Security Risk Assessment for System Design (Cont'd)

Documentation of zone and conduit characteristics (minimum)

- Name and/or unique identifier
- Logical boundary
- Physical boundary if applicable
- List of all physical and logical access points and associated boundary devices
- List of data flows associated with each access point
- Connected zones or conduits
- List of assets and their classification, criticality and business value
- Applicable security requirements
- Target Security Levels (SL-T)
- Applicable security policies
- Assumptions and external dependencies

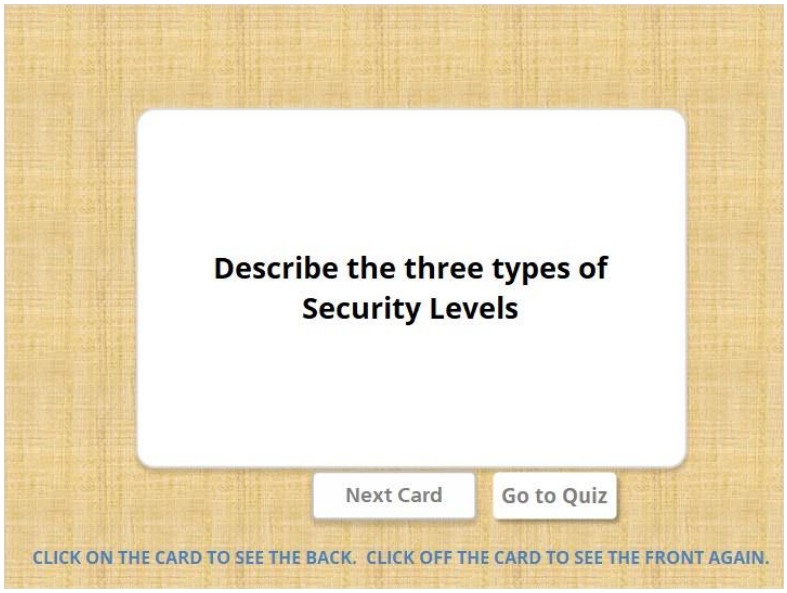
Security Risk Assessment for System Design (Cont'd)

Few more considerations

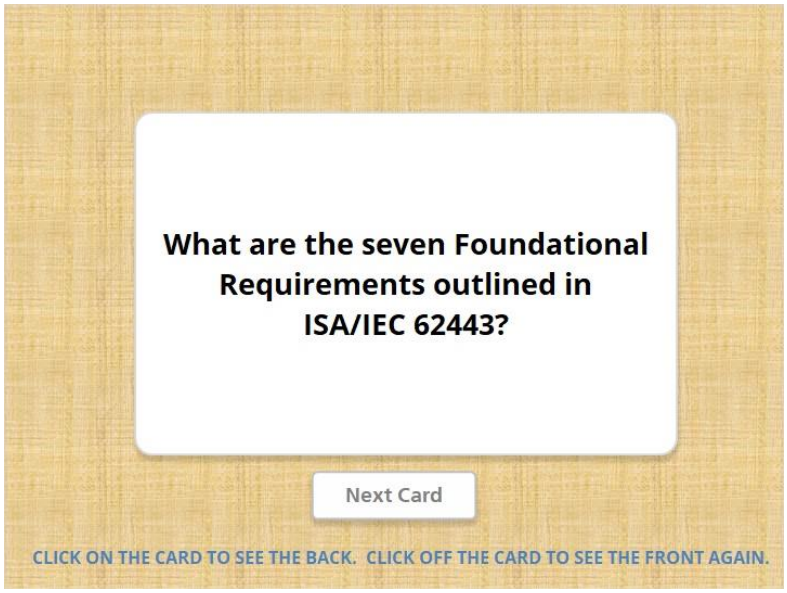
- Separation of business and control system zones
- Separation of safety-critical zones
- Separation of temporarily connected devices
- Separation of wireless communications
- Separation of devices connected via untrusted networks
  - Remote access is outside the physical boundary of the SuC
  - Model as a separate zone or zones
  - Separate security requirements identified

Practical applications

- Using what we have learned
- Review sampling of reference architectures
- See Additional Resources tab for full page drawings



- **Target SLs (SL-T)** are the desired level of security for a particular system
- **Capability SLs (SL-C)** are the security levels that components or systems can provide when properly configured
- **Achieved SLs (SL-A)** are the actual level of security for a particular system



FR 1 - Identification and Authentication Control (IAC)

FR 2 - Use Control (UC)

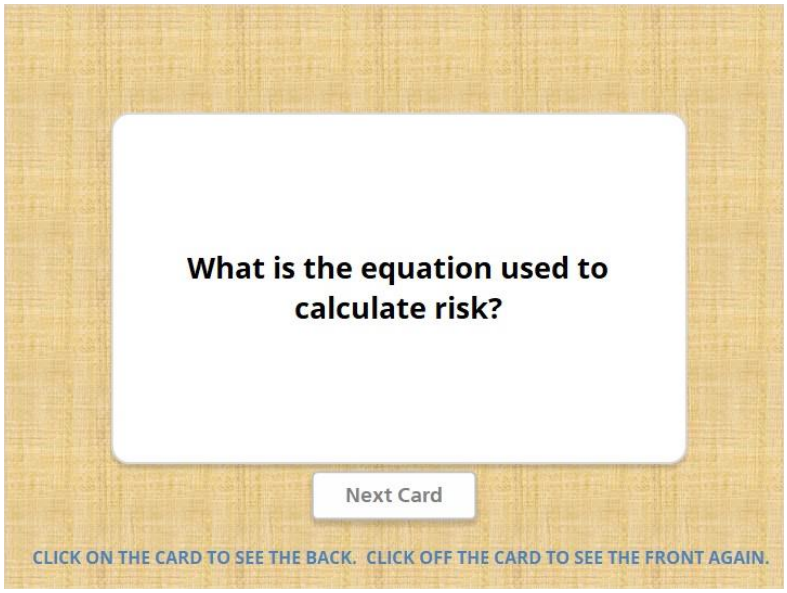
FR 3 - System Integrity (SI)

FR 4 - Data Confidentiality (DC)

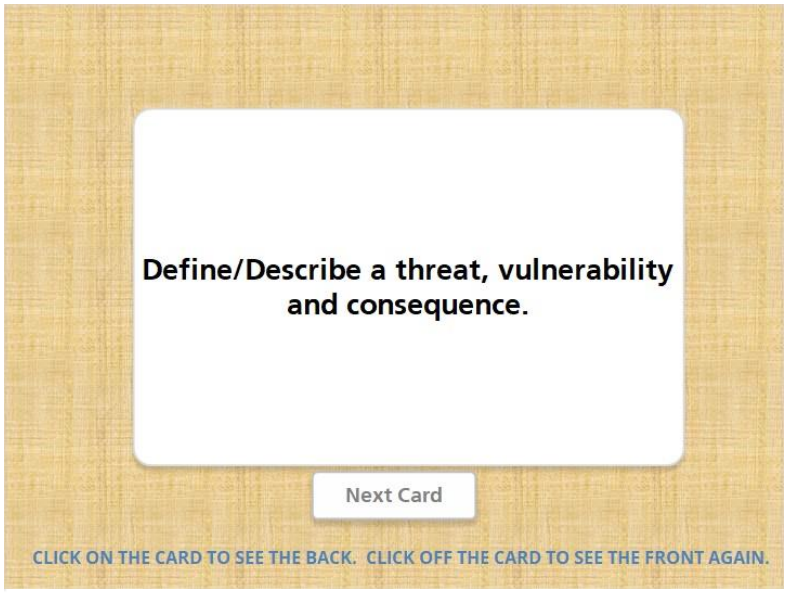
FR 5 - Restrict Data Flow (RDF)

FR 6 - Timely Response to Events (TRE)

FR 7 - Resource Availability (RA)



Risk = Threat x Vulnerability x Consequence



Threat

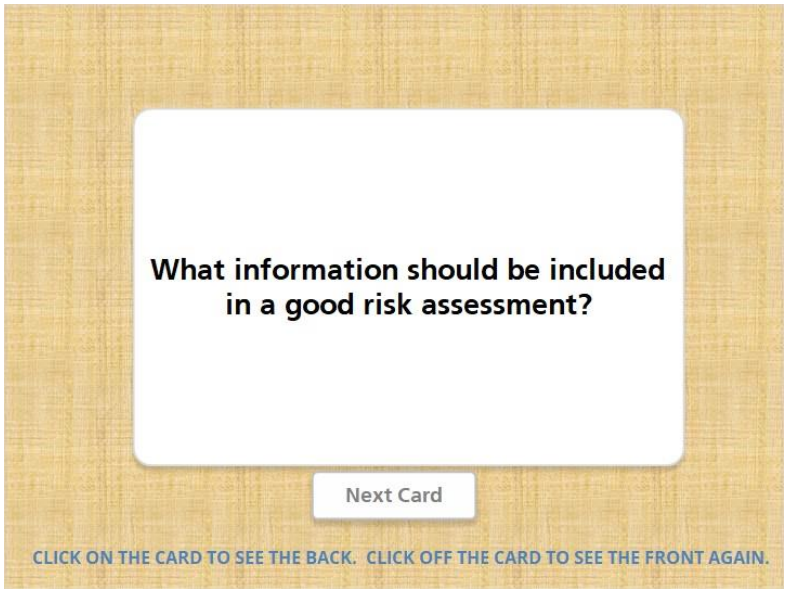
- Potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm
- Circumstance or event with the potential to adversely affect operations

Vulnerability

- Flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy

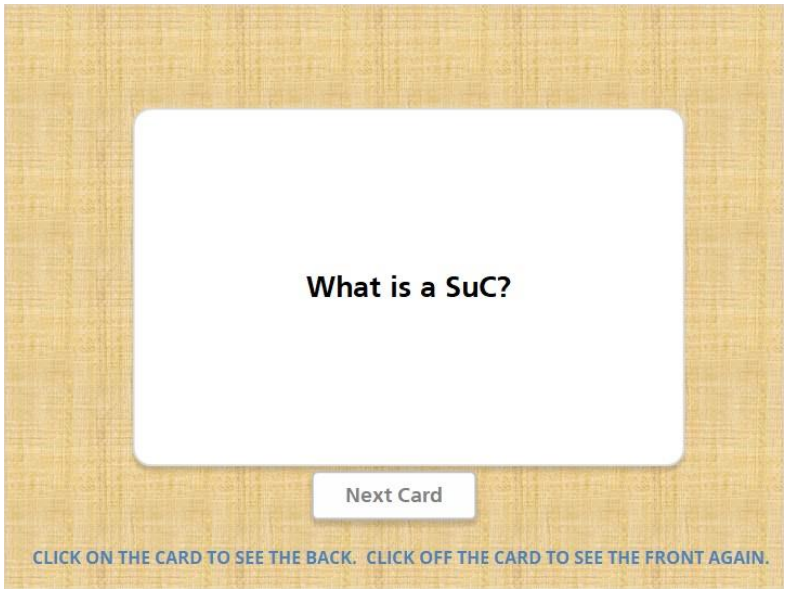
Consequence

- Result that occurs from a particular incident



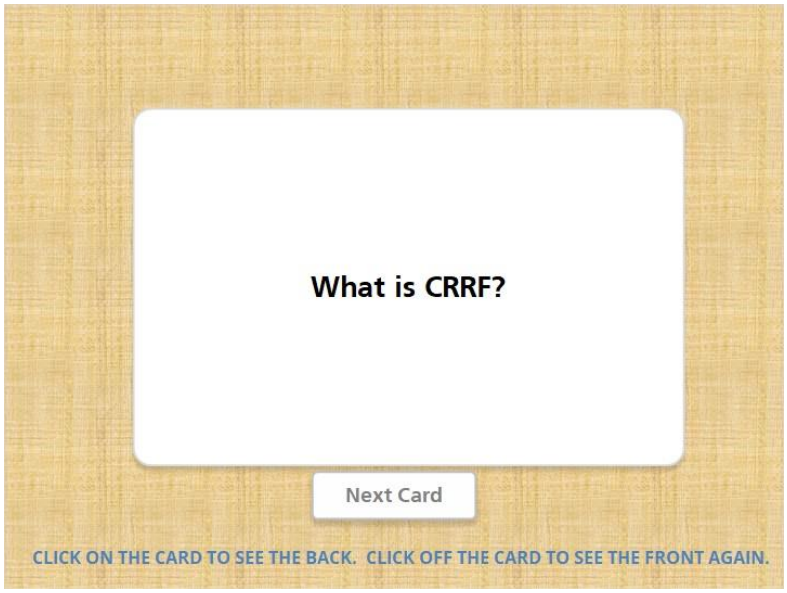
A **good risk assessment** should include the following for the entire system as well as for each zone and conduit

- ✓ **Risk profile**
- ✓ **Highest severity consequences**
- ✓ **Threats & vulnerabilities leading to the highest risks**
- ✓ **Target Security Levels**
- ✓ **Recommendations**



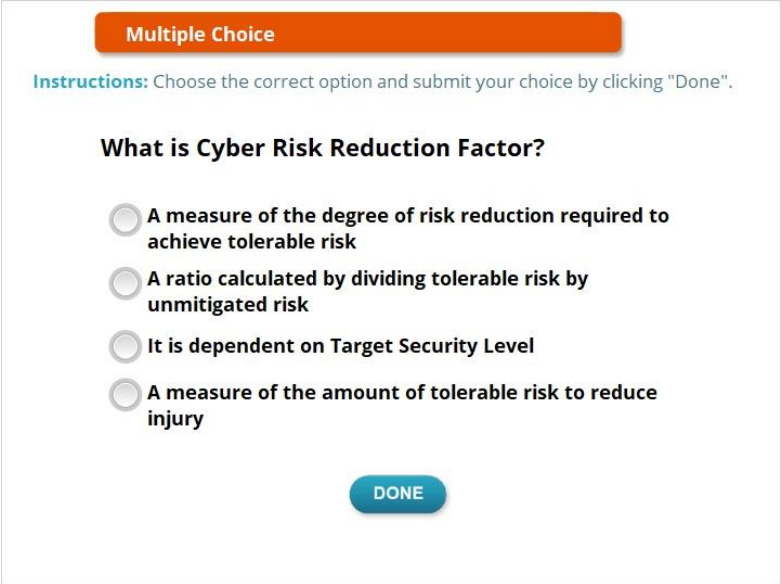
System under Consideration (SuC)

- Defined collection of IACS and related assets for the purpose of security risk analysis
- Consists of one or more zones and related conduits
- All assets belong to either a zone or conduit

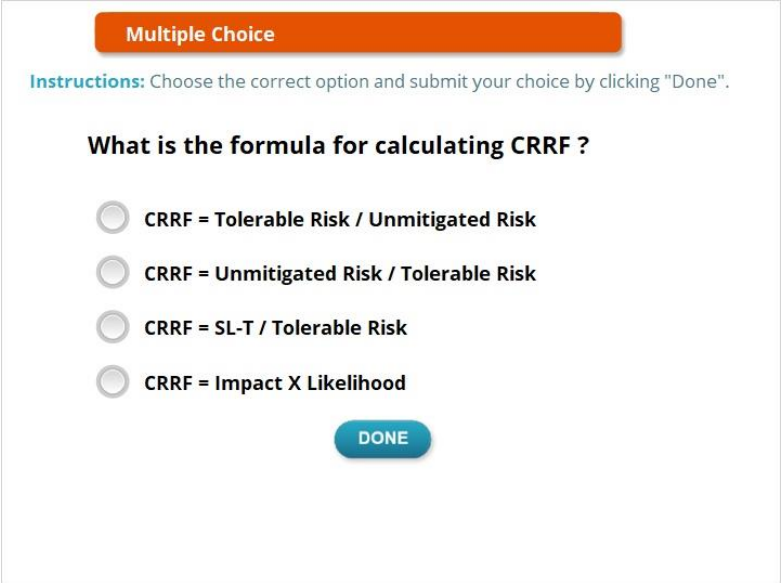


CRRF (Cyber Risk Reduction Factor)

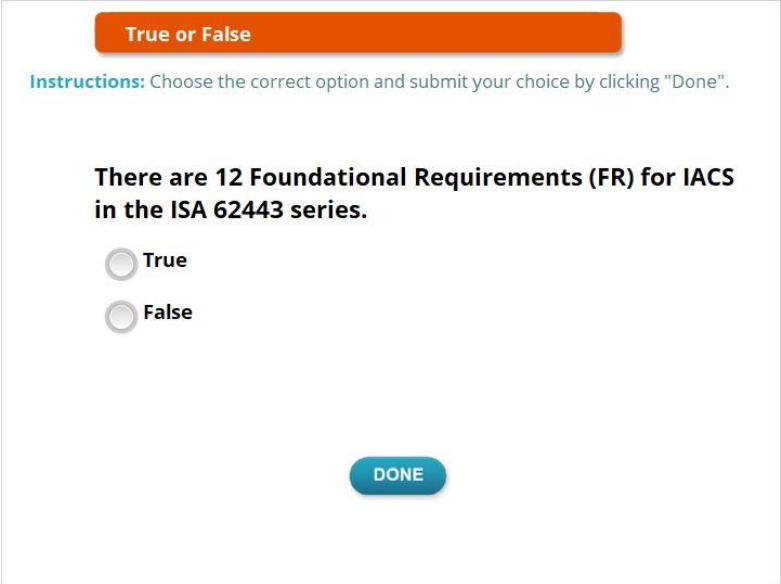
- a measure of the degree of risk reduction required to achieve tolerable risk
- a ratio that is calculated by dividing unmitigated risk by tolerable risk



Correct	Choice
X	Radio Button 1

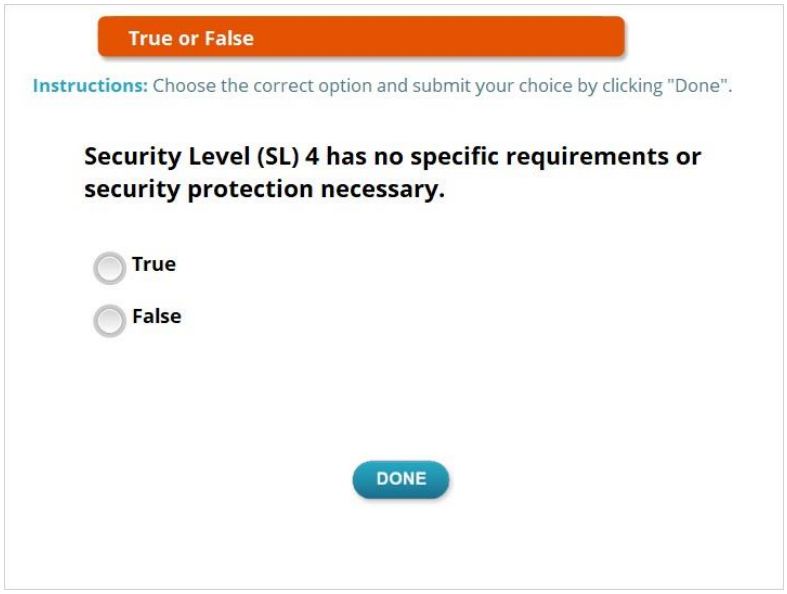


Correct	Choice
X	Radio Button 2

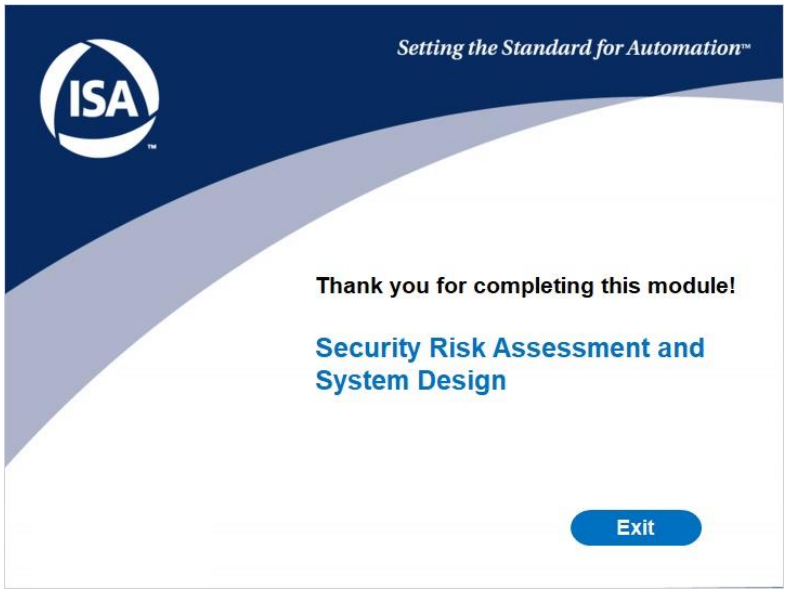


Correct	Choice
X	Radio Button 2

Correct	Choice
X	Radio Button 4



Correct	Choice
X	Radio Button 2



Week 8

Week 8
Week 8
Week 8
Week 8
Week 8

Setting the Standard for Automation™

IC329 Module 12

After completing this module you will be able to:

- ✓ Identify ISA/IEC 62443 Part 2-4 as the guide for requirements for IACS service providers activities
- ✓ Identify types of service providers including Integration Service Provider, Maintenance Service Provider and Product Suppliers
- ✓ Discuss Product Security Development Life Cycle requirements
- ✓ Explain Defense in Depth strategy as a key philosophy of secure product life cycle
- ✓ Identify ISA/IEC 62443 Part 4-2 as the guide for Technical Security Requirements for IACS components

Security Program Requirements for IACS Service Providers

Requirements for IACS Service Providers

Part 2-4 covers requirements for IACS service providers activities

- Service providers will have to use technologies considered secure
- Technologies no longer considered secure (e.g., Digital Encryption Standard (DES) or Wireless Equivalent Privacy (WEP) security would be non-conformant)

Notes:

Point out IEC 62443-2-4 Requirements for IACS service providers is “Approved”

Fairly recent in standards time. 13 July 2018 (as of 12 May 2019)

This section is designed to be a high level overview about service providers.

Part 2-4, Annex A has a list of about 130 normative requirements

The specific terms and conditions for providing these requirements are beyond the scope of this course

Service providers can be a course in itself when you add in Parts 4-1 and 4-2

Students do not get a copy of this Pat 2-4

Part 2-4 available for viewing as ISA member or purchase from ISA/IEC

Requirements for IACS Service Providers

Notes:

This part of the ISA- 62443 series defines requirements for security capabilities to be supported by security programs of integration and maintenance service providers.

Support for these capabilities means that the service provider can provide them to the asset owner upon request.

In addition, ISA- 62443-2-4 can be used by these service providers to structure and improve their security programs.

IACS Integration Service Provider

Provides capabilities to implement/deploy Automation Solutions

- According to asset owner requirements

Integration service provider activities generally occur

- Starting with the design phase
- Ending in handover of the Automation Solution to the asset owner

Typical Integration Service Provider Activities

- Analysis
- Development
- Definition
- Installation, configuration, patching, backup, and testing
- Gaining approval of the asset owner during the execution of activities

Part 2-4, clause 4.1.5, page 18

IACS Maintenance Service Provider

Performs activities that maintain and service Automation Solutions according to asset owner requirements

Maintenance activities are separate from operation activities

Maintenance activities generally start after handover of the Solution

- May continue until the asset owner no longer requires them

Typical Maintenance Service Provider Activities

- Patching and anti-virus updates
- Equipment upgrades and maintenance
- Component and system migration
- Change management
- Contingency plan management

Part 2-4, clause 4.1.6, page 18

IACS Product Supplier

Manufacturer of hardware and/or software product

Develops control system product as a combination of

- Supporting applications
- Embedded devices
- Network components
- Host devices

Independent of IACS environment

Maintenance activities may be shared by

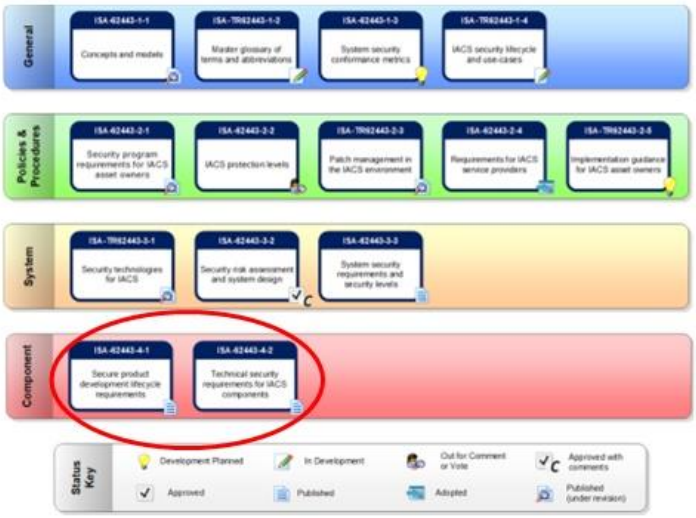
- Asset Owner
- Integrator
- Maintainer
- Product Supplier

Notes:

- Product supplier definition bullet from Part 2-4, subclause 3.1.12, pg 13
- Develops from Part 2-4, Fig 2, pg 11
- Independent from IACS part 2-4, Fig 2, pg 11
- In the real-world, Asset Owner/Integrator/Maintainer/Product Supplier may share tasks in maintenance activities.
- Lots of overlap.

Developing Secure Products and Systems

- Product security development life-cycle requirements
- Technical security requirements for IACS components



Notes:

Introduction topic slide

Parts 4-1 and 4-2 cover a lot of ground and could easily be a separate 2 day or longer course

The intent of this section is to introduce parts 4-1 & 4-2

This section provides a high level overview of the following 2 standards

62443-4-1 Secure Product Development Life-cycle

62443-4-2 Technical Security Requirements for IACS Components

Students do not get a copy of parts 4-1 & 4-2

Course objectives covered:

Describe how secure software development strategies can make systems inherently more secure

Describe what is being done to validate or verify the security of systems

Product Security Development Life-Cycle Requirements

Product suppliers are the main audience

Primary goal to provide a product framework addressing

- Secure by design
- Defense in depth approach to designing
- Building
- Maintaining
- Retiring

Support meeting product overall Capability Security Level (SL-C)

- What is the product's SL-C?
- Ensure product security capabilities implemented correctly
- Know security vulnerabilities are eliminated or mitigated
- Concept of Target and Achieved Security Levels (SL-T, SL-A) other than Capability (SL-C) not covered in Part 4-1

Notes:

- Part 4-1, Clause 4, pg 25
- Security levels (0-4) is not discussed in this standard,
- Complying with this standard will help ensure that the security capabilities implemented in the product will be implemented correctly and that any known security vulnerabilities in the product are eliminated or mitigated
- A maturity model level 1-5 used to measure the supplier's maturity. That model is not tied to the 62443 SL (0-4). We discuss maturity model in a couple slides
- Concept of security levels was covered in an earlier module

Product Security Development Life-Cycle Requirements

Secondary goal is to align

- Development process
- Needs of industrial users
  - Asset owners
  - Integrators
  - Maintenance contractors
- Security configs & patch management polices and procedures
- Communications about uncovered product security vulnerabilities

Key concept is use of threat modeling

- Impact analysis
- Resolution

Key philosophy of secure product life-cycle

- Defense in depth strategy (shown next slide)

Notes:

Part 4-1, Clause 4, pg 25

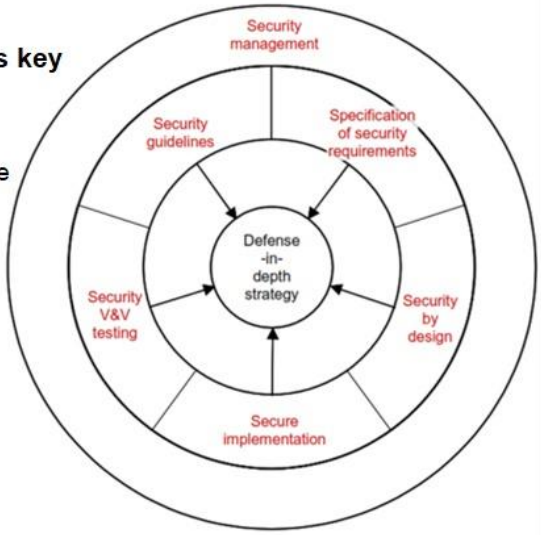
Defense in Depth Strategy Practices

Defense in depth strategy is key philosophy to

- Secure product life-cycle
- Security development life-cycle

Security Management includes

- Security Defects
- Security-related issues
- Documentation updates



Notes:

- Graphic shows how the product secure product life cycle wraps around and supports the traditional defense-in-depth approach which was shown in a previous slide.
- Part 4-1, Fig 3, pg 26 illustrates how secure by design principles in this standard contribute to a defense in depth strategy for the product
    - 6 of the 8 practices are shown in figure using red font
    - Not shown are “defect management” and “security update management” which provide verified repairs to the secure implementation
    - “defect management” and “security update management” fall under the category of overall security management
- Security management practice ensures adequate planning, documentation, and execution throughout the product’s life cycle
- See Part 4-1, Clause 5 which covers the 8 practices in detail

Notes:

- There is a range of levels used in the Capability Maturity Model Integration for Development (CMMI-DEV) model used to measure how a supplier has met requirements of part 4-1
- This is not tied to Security Levels (0-4).
- Complying with this standard will help ensure that the security capabilities implemented in the product will be implemented correctly and that any known security vulnerabilities in the product are eliminated or mitigated based on the supplier's capability maturity
- CMMI-DEV maturity model found in Part 4-1, subclause 4.2, pg 26, 27, 28
- Table 1, page 28 shows levels
    - Level 1 typically perform product development in an ad hoc and often undocumented (or not fully documented) manner. As a result, consistency across projects and repeatability of processes may not be possible
    - Level 5 quantitively managed, optimized and use suitable process metrics and demonstrate continuous improvement

Technical Security Requirements for IACS Components

Who is the audience for 62443 Part 4-2?

System Integrators

- ✓ Assist in procuring control system components
- ✓ Specify the appropriate security capability level of the individual components required
- ✓ Choose components that provide necessary security capabilities to achieve SL-T for each zone

Product suppliers

- ✓ Understand the requirements placed on control system components for specific security capability level (SL-C) of those components
- ✓ Provide documentation of how to properly integrate the component into a system to meet a specific SL-T

Types of IACS Components

Software Application
- Operator workstation
- Data historian

Embedded Device
- PLC
- IED

Host Device
- Operator workstation
- Data historian

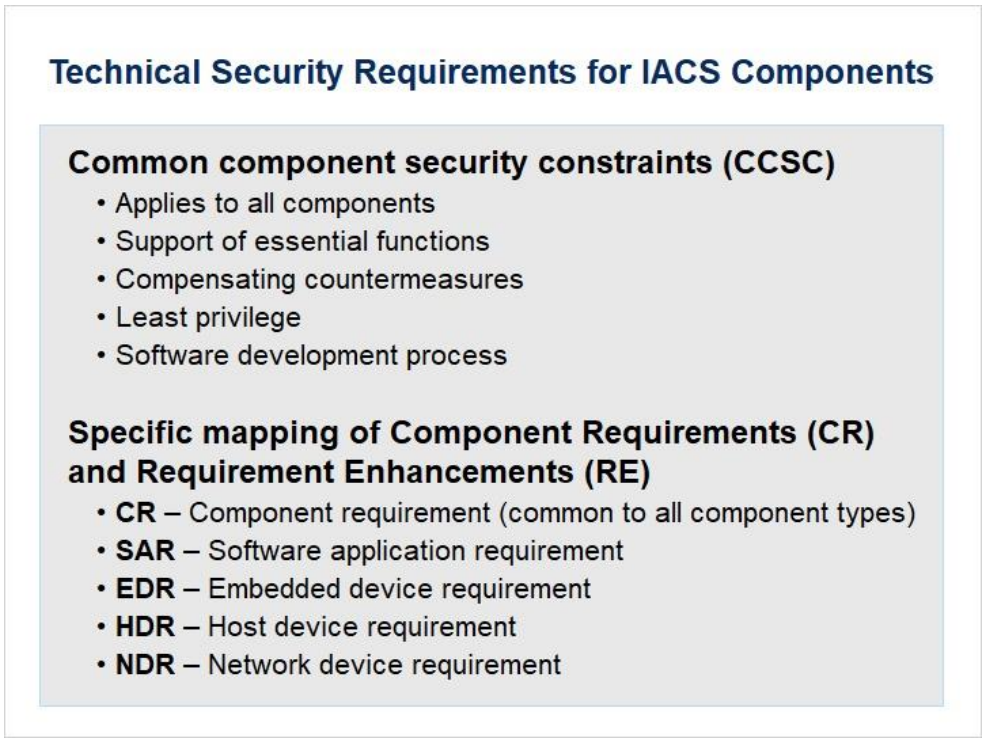
Network Device
- Switch (network)
- VPN terminator

Series of Component Requirements (CR) and Requirement Enhancements (RE) specifically for components

- Expands the System Requirements (SR) and Requirement Enhancements (RE) defined in ISA-62443-3-3
- Built upon the same Foundational Requirements (FR) 1-7 and Security Levels (SL) 0-4

Notes:

- Part 4.2, pg 14
- Part 4.2, Annex A, Device categories has definitions for types of components



Notes:

- Common component security constraints (CCSC), Part 4.2, Clause 4, pg 26
- Support of essential functions: shall adhere to specific constraints as described in Part 3-3, clause 4
- Compensating countermeasures: There will be cases where one or more requirements specified in the document cannot be met without the assistance of a compensating countermeasure that is external to the component.
    - When this is the case the documentation for that component shall describe the appropriate countermeasures applied by the system to allow the requirement to be met when the component is integrated into a system
- Least privilege: When required shall provide the capability for the system to enforce the concept of least privilege.
    - Individual system components shall provide the granularity of permissions and flexibility of mapping those permissions to roles sufficient to support it. Individual accountability shall be available when required. Dependent on the type of device and the product documentation for the device should define this in the product documentation.
- Software development process: shall be developed and supported following the secure product development processes described in Part 4-1

About 124 CR, RE, SAR, EDR, NDR listed-beyond scope of this course

ISASecure Conformance

ISA Security Compliance Institute (ISCI) bridges the gap between standards and their implementation

- Manages ISASecure conformance certification program

ISASecure

- Does not operate an internal testing lab, but instead, partners with qualified labs to perform IACS cybersecurity assessments
- Independently certifies IACS products and systems to ensure that they are robust against network attacks and free from known vulnerabilities
- Does not offer assessments for integrator site engineering practices or asset owner operations and maintenance practices
- Certifies off-the-shelf systems

Notes:

https://www.isasecure.org/en-US/

ISASecure Conformance

Accredited ISASecure Certification Bodies (as of May 2019)

Control System Security Center Certification Laboratory

- https://www.isasecure.org/en-US/Certification-Bodies/Accredited-ISASecure-Certification-Bodies

ISASecure Certified Sample (as of August 2019)

Picture	Supplier	Type	Model	Version	Level	Cert Date
	Emerson Automation Solutions	DeltaV DCS and SIS	System	14.3	SSA 2.0.0 Level 1	3/7/2019
	Honeywell Process Solutions	Experion LX/PlantCruise R500 Series 8 C300 with CF9	DCS Controller	R500	EDSA 2.0.0 Level 1	6/24/2019
	Schneider Electric	Field Device Controller 280 (FDC280)	Field Device Controller	S901032000 and 0901003000	EDSA 2.0.0 Level 1	12/21/2018

Certification includes requirements in

- Part 3-3: System security requirements and security levels
- Part 4-1: Product security development life-cycle requirements

Certifier also performs System Robustness Testing

- Fuzz testing
- Network traffic load testing
- Vulnerability scanning

Notes:

Recap slide

Parts 4-1 and 4-2 cover a lot of ground and could easily be a separate 2 day or longer course

The intent of this section is to introduce parts 4-1 & 4-2

This section provides a high level overview of the following 2 standards

62443-4-1 Secure Product Development Life-cycle

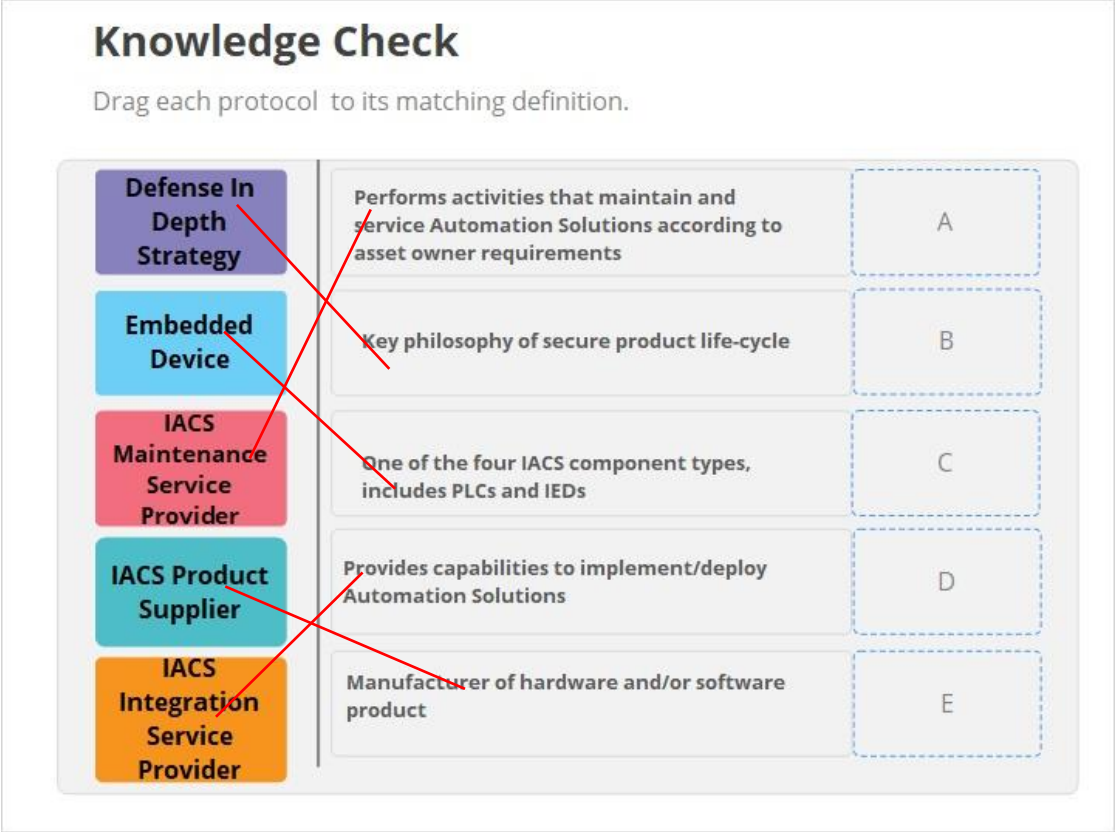
62443-4-2 Technical Security Requirements for IACS Components

Students do not get a copy of parts 4-1 & 4-2

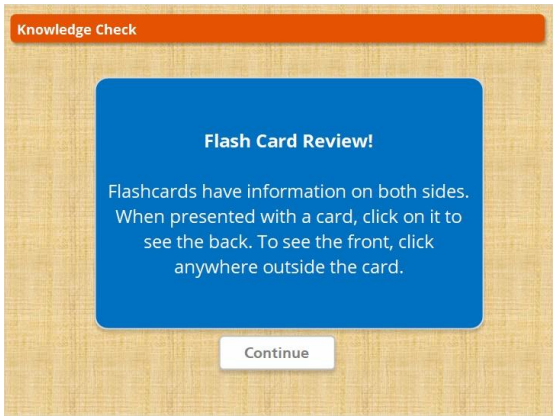
Course objectives covered:

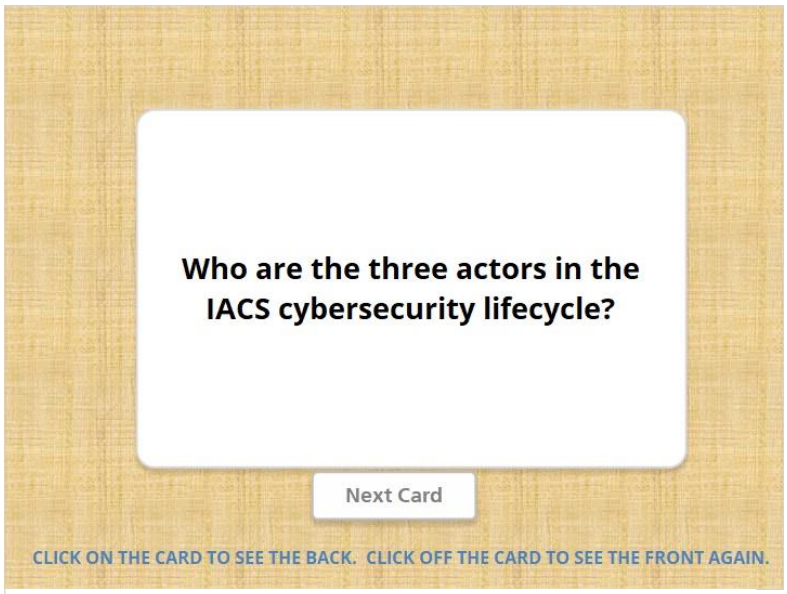
Describe how secure software development strategies can make systems inherently more secure

Describe what is being done to validate or verify the security of systems

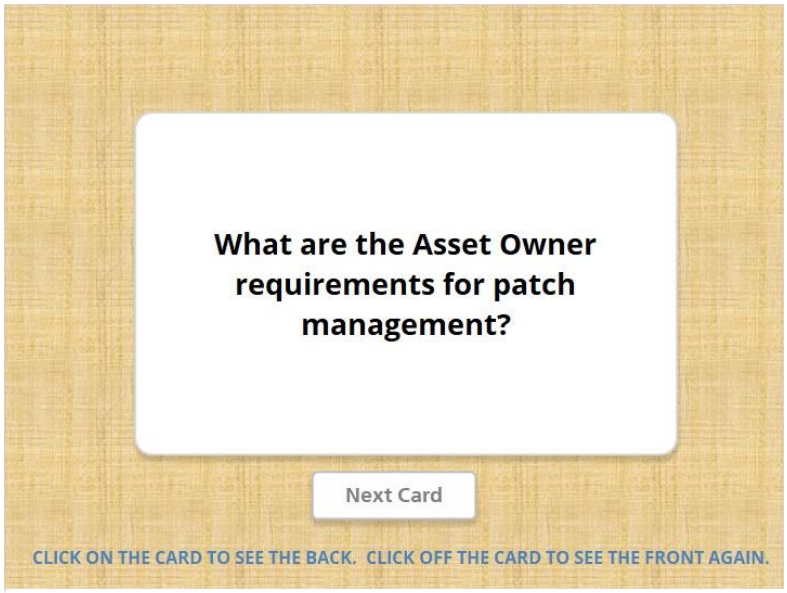


Drag Item	Drop Target
Defense In Depth Strategy	B
Embedded Device	C
IACS Maintenance Service Provider	A
IACS Product Supplier	E
IACS Integration Service Provider	D





- **Asset Owners** – Operate and maintain site specific systems
- **Integrators/Asset Owners** – Engineer and integrate COTS into site specific systems
- **Suppliers** – Design and manufacture COTS control systems



Information gathering

Inventory of existing environment

Project planning and implementation

Develop patch management process

Monitoring and evaluation

Security related patches applicability

Patch testing

Test and qualify in a lab environment

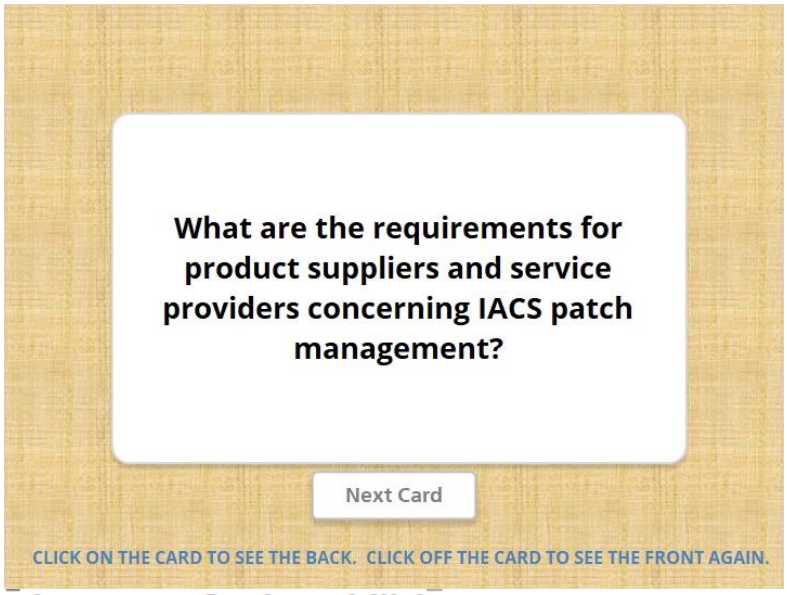
Patch deployment and installation

Notification of affected parties

Roll-back plan

Operating patch management program

Sustained and optimized



Discovery of vulnerabilities

- Procedures in place
- Frequency defined

Development, verification and validation

- Validate mitigation
- Compensating controls to reduce attack surface

Distribution of cyber security updates

- Available via a secure channel
- Provide patch sources for third-party software used in product
- Windows Server Update Services (WSUS)
- Traditional Microsoft second Tuesday of the month release day

Communication and outreach

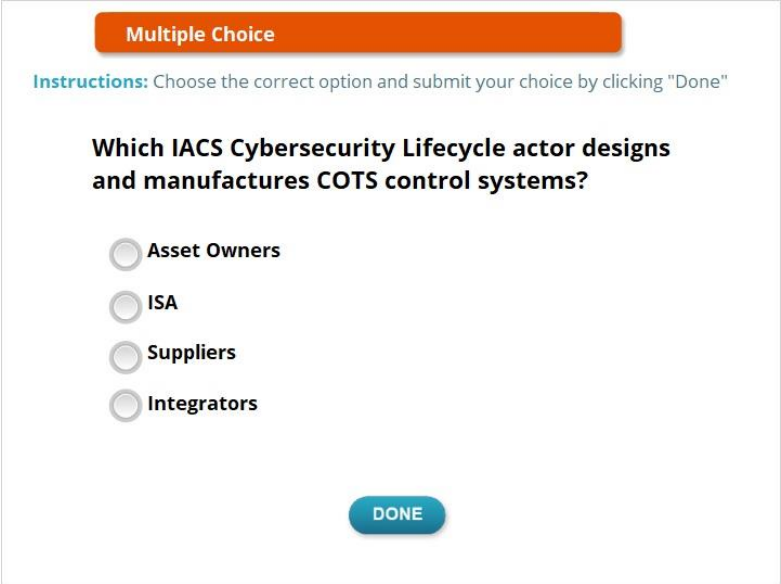
Malicious Code Protection uses protection mechanisms against malicious code to

- Prevent
- Detect
- Report
- Mitigate

Measures to protect IACS against malicious code include:

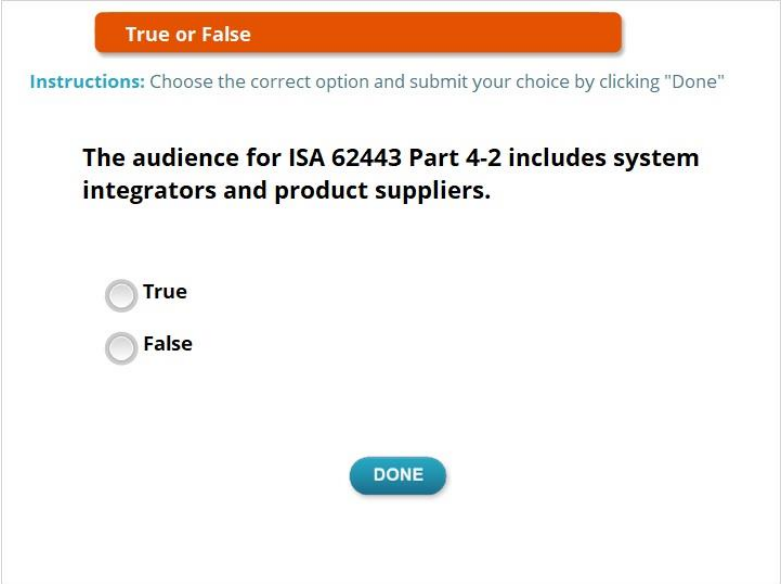
- Using mixed deployment systems
- Focus on anti-virus signatures in all computers located in the DMZ
- A dedicated anti-virus server can be located in the DMZ

Quiz Questions

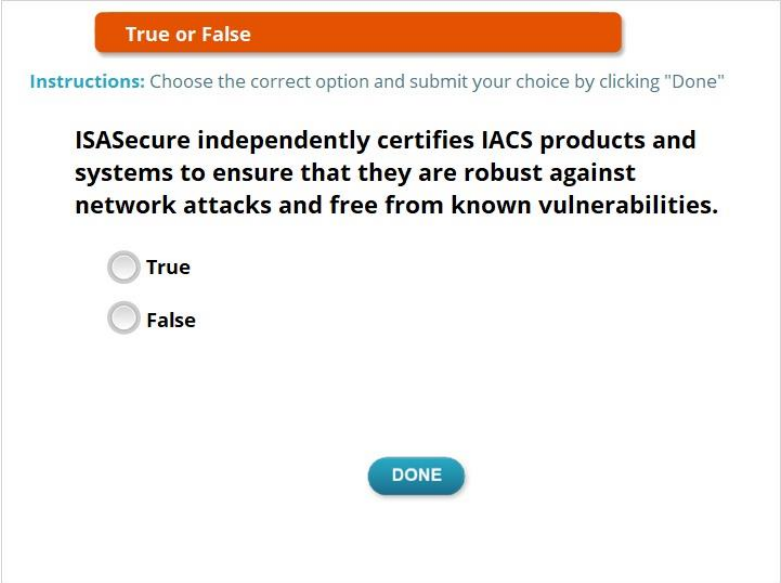


Correct	Choice
X	Radio Button 3

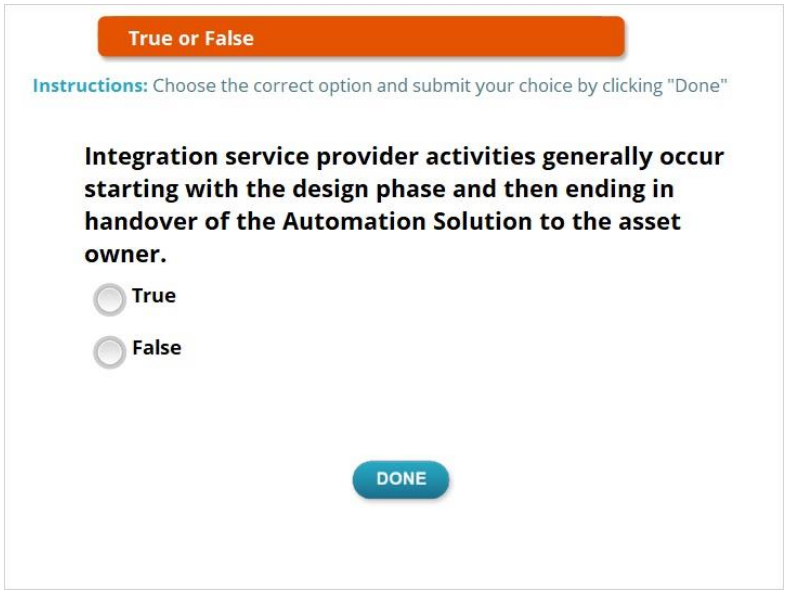
Correct	Choice
X	Radio Button 1



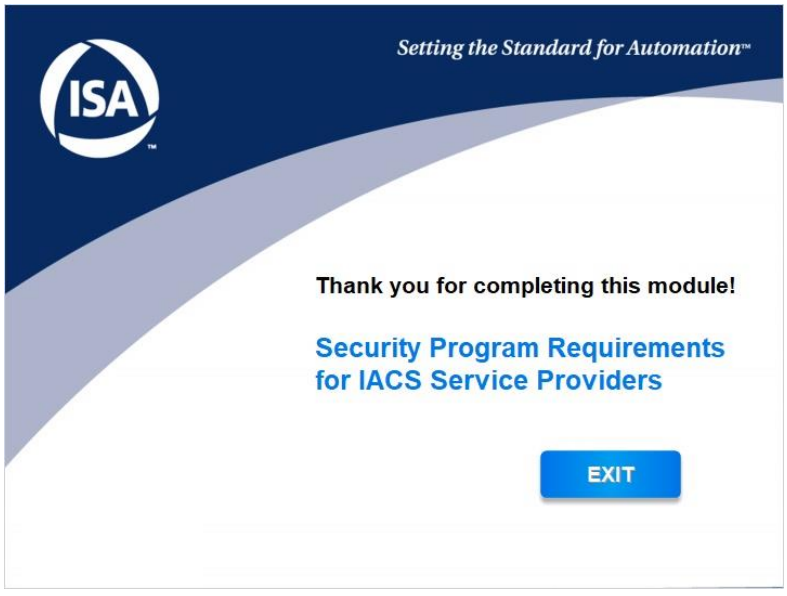
Correct	Choice
X	Radio Button 1



Correct	Choice
X	Radio Button 1



Correct	Choice
X	Radio Button 1



Certificate Exam Process

Now that you have successfully completed **IC32M**, you qualify to take the electronic exam administered by Prometrics for

Certificate 1:
ISA/IEC 62443 Cybersecurity Fundamentals Specialist

Please call ISA Customer Service at (919) 549-8411 or email info@isa.org to request your Eligibility code for Cybersecurity Certificate 1 exam. Once you receive your code, you will be able to schedule your exam with Prometrics.

Learn More

Certificate 1 Certificate 2 Certificate 3 Certificate 4 Expert

Instructional Surveys

Setting the Standard for Automation™

IC32 - Pre-Instructional Survey

1. What is the primary function of a firewall?

    a. Block all internet traffic
    b. Detect network intrusions
    c. Filters network traffic
    d. Authenticate users

2. Inter-network connection device that restricts data communication traffic between two connected networks is called a(n) _____.

    a. IDS
    b. Firewall
    c. Router
    d. Anti-virus software

3. The process of securing a system by reducing its attack surface is known as

    a. Threat Modeling
    b. System Hardening
    c. Intrusion Detection
    d. Whitelisting

4. Policies, procedures and technical controls that govern the use of system resources are known as

    a. Data Flow Controls
    b. System Integrity Controls
    c. Access Controls
    d. System Hardening Controls

5. Which of the following is an objective of cybersecurity acceptance testing?

    a. Verification of cybersecurity specifications
    b. Root cause analysis
    c. Cyber risk determination
    d. Verification of system functionality

IC32 - Pre-Instructional Survey

6. What are the three main phases of the IACS Cybersecurity Lifecycle?

   a. Assess, Develop & Mitigate, Maintain
   b. Design, Implement, Maintain
   c. Assess, Develop & Implement, Maintain
   d. Design, Mitigate, Maintain

7. Which of the following is the correct risk equation?

   a. Risk = Threat x Asset x Consequence
   b. Risk = Threat x Vulnerability x Cost
   c. Risk = Threat Agent x Threat x Vulnerability
   d. Risk = Threat x Vulnerability x Consequence

8. The desired level of security for a system is known as?

   a. Target Security Level
   b. Achieved Security Level
   c. Capability Security Level
   d. Protection Level

9. Which of the following is the correct formula for Cyber Risk Reduction Factor (CRRF)?

   a. CRRF = Unmitigated Risk / Tolerable Risk
   b. CRRF = Mitigated Risk / Tolerable Risk
   c. CRRF = Tolerable Risk / Unmitigated Risk
   d. CRRF = Tolerable Risk / Mitigated Risk

10. An Intrusion Detection System (IDS) is an example of what method of treating risk?

    a. Detect
    b. Deter
    c. Defend
    d. Defeat

IC32 - Pre-Instructional Survey

11. Security service system that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of attempts to access system resources in an unauthorized manner is called a(n) _____.

    a. IDS
    b. Firewall
    c. Router
    d. Anti-virus software

12. What is the name of the firewall feature that analyzes protocols at the application layer to identify malicious or malformed packets?

    a. Stateful inspection
    b. Deep packet inspection
    c. Packet filter
    d. Layer 3 check

13. A three-tier network segmentation design that prevents direct communication between the enterprise network and the process control network by creating a buffer is also known as a(n) _____.

    a. Zones and conduits
    b. Perimeter firewall
    c. ICS firewall
    d. DMZ

14. Which of the following represents the recommended process of firewall planning and implementation?

    a. Plan, Configure, Test, Deploy, Manage
    b. Plan, Configure, Deploy, Test, Manage
    c. Plan, Deploy, Manage, Test, Configure
    d. Design, Configure, Test, Deploy, Document

15. What are the main types of intrusion detection systems?

    a. Perimeter Intrusion Detection & Network Intrusion Detection
    b. Host Intrusion Detection & Network Intrusion Detection
    c. Host Intrusion Detection & Intrusion Prevention Systems
    d. Intrusion Prevention & Network Intrusion Detection

16. What is the desired outcome of the Initiate a CSMS program activity?
    a. Conceptual diagrams that show how an AD forest can be attacked
    b. Obtain leadership commitment, support, and funding
    c. Identify software agents used by threat agents to propagate attacks
    d. Conduct periodic IACS conformance audits

17. Which of the following is NOT a network device hardening best practice?
    a. Install latest firmware updates
    b. Shut down unused physical interfaces
    c. Enable logging, collect logs (e.g. Syslog) and review regularly
    d. Use Telnet for remote management

18. Which of the following is an example of dual-factor authentication?

    a. Username and password
    b. Digital certificate and smart card
    c. Fingerprint and retinal signature
    d. Fingerprint and smart card

19. A network that uses a public telecommunication infrastructure such as the Internet to provide remote networks or computers with secure access to another network is known as a _____.

    a. VLAN
    b. VSAT
    c. VPN
    d. VNC

20. If a virus shuts down an industrial network by overloading the Ethernet switches which basic information security property is affected?

    a. Integrity
    b. Confidentiality
    c. Availability
    d. Reliability

IC32 - Post-Instructional Survey

1) Which three basic properties are the building blocks of cyber security?

   a) Authorization, Identification, and Integrity (AII)
   b) Confidentiality, Integrity and Availability (CIA)
   c) Authorization, Reliability and Integrity (ARI)
   d) Confidentiality, Integrity and Authorization (CIA)

2) What is the biggest security problem if business networks connect directly to industrial control systems?

   a) Too many business users requesting data will slow control system operation to a crawl, endangering the security of processes.
   b) Unauthorized business users, outsiders and malware can penetrate critical industrial control systems and upset critical processes.
   c) Production workers will change data in business systems given the opportunity
   d) Cybersecurity insurance will increase in cost

3) “Countermeasures” in cyber security are measures taken to:

   a) Eliminate system penetration by outsiders
   b) Confuse perimeter intrusion detectors
   c) Reduce the system’s risk of loss from vulnerabilities and threats
   d) Eliminate the risk of an inside attacker taking over a computer network

4) Why would a company issue security policies for industrial networks?

   a) To let outside intruders know the consequences of their actions.
   b) To clearly establish which department “owns” the network
   c) To guide a company’s cybersecurity department on how to catch security violations.
   d) To communicate the responsibilities of users, management, IT staff for company security.

5) A key factor for the success of a cyber security program is:

   a) Security policy, objectives and activities that reflect business rationale and objectives.
   b) Strict rules that forbid interconnection of control system to business systems.
   c) The latest in security technologies.
   d) The latest in hardware technologies.

6) One-way safety is different from security in industrial plants is that:

a) Safety considers the effects of malicious actions, not just the causes.
b) The field of safety encompasses the field of security.
c) Safety concerns itself with human error and the natural causes of accidents, while security may involve malicious behavior.
d) Safety concerns itself with malicious behavior, while security may involve human error and the natural causes of accidents.

7) Which of the following documents are IT Security standards?

a) IEC 61850
b) ISO 27001:2013
c) ISA 95
d) ISA 84

8) Which of the following are control system security standards?

a) COBIT 5
b) ISO/IEC 15408:2009
c) ISA/IEC 62443
d) ISO 27001:2013

9) The standard ISA 62443-2-1 belongs in which tier/group of the ISA 99 committee work products?

a) Component
b) System
c) General
d) Policies & Procedures

10) Which of the following is NOT generally considerered to be a requirement of industrial control systems?

a) Real-time performance
b) High availability
c) Frequent updates
d) HSE considerations

IC32 - Post-Instructional Survey

11) Which formula is correct?

a) Risk = Threat x Asset x Consequence
b) Risk = Threat x Vulnerability x Cost
c) Risk = Threat x Likelihood x Vulnerability
d) Risk = Threat x Vulnerability x Consequence

12) Which of the following would NOT be considered a countermeasure?

a) Replay
b) Access Controls
c) Encryption
d) Intrusion Detection

13) A logical grouping of physical, informational, and application assets sharing common security requirements is called a(n) _____

a) Security model
b) Asset model
c) Conduit
d) Zone

14) Which of the following is Layer 4 in the ISO OSI/Reference Model?

a) Session
b) Network
c) Transport
d) Data

15) Which one of the following can best perform a network subnet routing function?

a) Layer 1 hub
b) Layer 2 network interface card
c) Layer 3 switch
d) Layer 4 user datagram protocol

IC32 - Post-Instructional Survey

16) TCP is a _____ protocol

a) Connection based
b) Layer 3
c) Send and forget
d) Layer 7

17) In IPv4 which protocol resolves IP addresses into MAC addresses?

a) ICMP
b) TCP
c) IP
d) ARP

18) What is Microsoft's normal scheduled release day for security patches?

a) When critical patches available
b) The first Monday of the month
c) The first Friday of the month
d) The second Tuesday of the month

19) What is the purpose of Windows Server Update Services (WSUS)?

a) Deploy the latest Microsoft Hyper-V product updates
b) Distribution of Microsoft Software Update Services
c) Deploy the latest Microsoft product updates and hotfixes
d) Distribution of Windows Software Unified Server

20) What is the primary function of a firewall?

a) Block all internet traffic
b) Detect network intrusions
c) Filters network traffic
d) Authenticate users

21) What is the first step in the High-Level Risk Assessment?

a) Identify Threats
b) Identify Critical Assets and Consequences
c) Define Methodology for Identifying Risks
d) Analyze Threats

22) What is the desired outcome of the Initiate a CSMS program activity?

a) Conceptual diagrams that show how an AD forest can be attacked
b) Obtain leadership commitment, support, and funding
c) Identify software agents used by threat agents to propagate attacks
d) Select and implement countermeasures

23) Which organization bridges the gap between 62443 standards and their implementation?

a) National Institute of Standards and Technology (NIST)
b) International Electrotechnical Commission (IEC)
c) European Union Agency for Network and Information Security (ENISA)
d) ISA Security Compliance Institute (ISCI)

24) System Robustness Testing includes which of the following?

a) Fuzz testing
b) Network traffic load testing
c) Vulnerability scanning
d) All the above

25) What are the three main phases of the ISA/IEC 62443 Cybersecurity Lifecycle?

a) Assess, Develop and Implement, Maintain
b) Assess, Integrate, Maintain
c) Analyze, Develop and Implement, Maintain
d) Analyze, Integrate, Maintain

Answer Sheets

Setting the Standard for Automation™

Answer Sheets
Answer Sheets
Answer Sheets
Answer Sheets
Answer Sheets

IC32 - Pre-Instructional Survey

Answer Key

1. c
2. b
3. b
4. c
5. a
6. c
7. d
8. a
9. a
10. a
11. a
12. b
13. d
14. a
15. b
16. b
17. d
18. d
19. c
20. c

IC32 Post-Instructional Survey
Answer Key

1) b
2) b
3) c
4) d
5) a

6) c
7) b
8) c
9) d
10) c

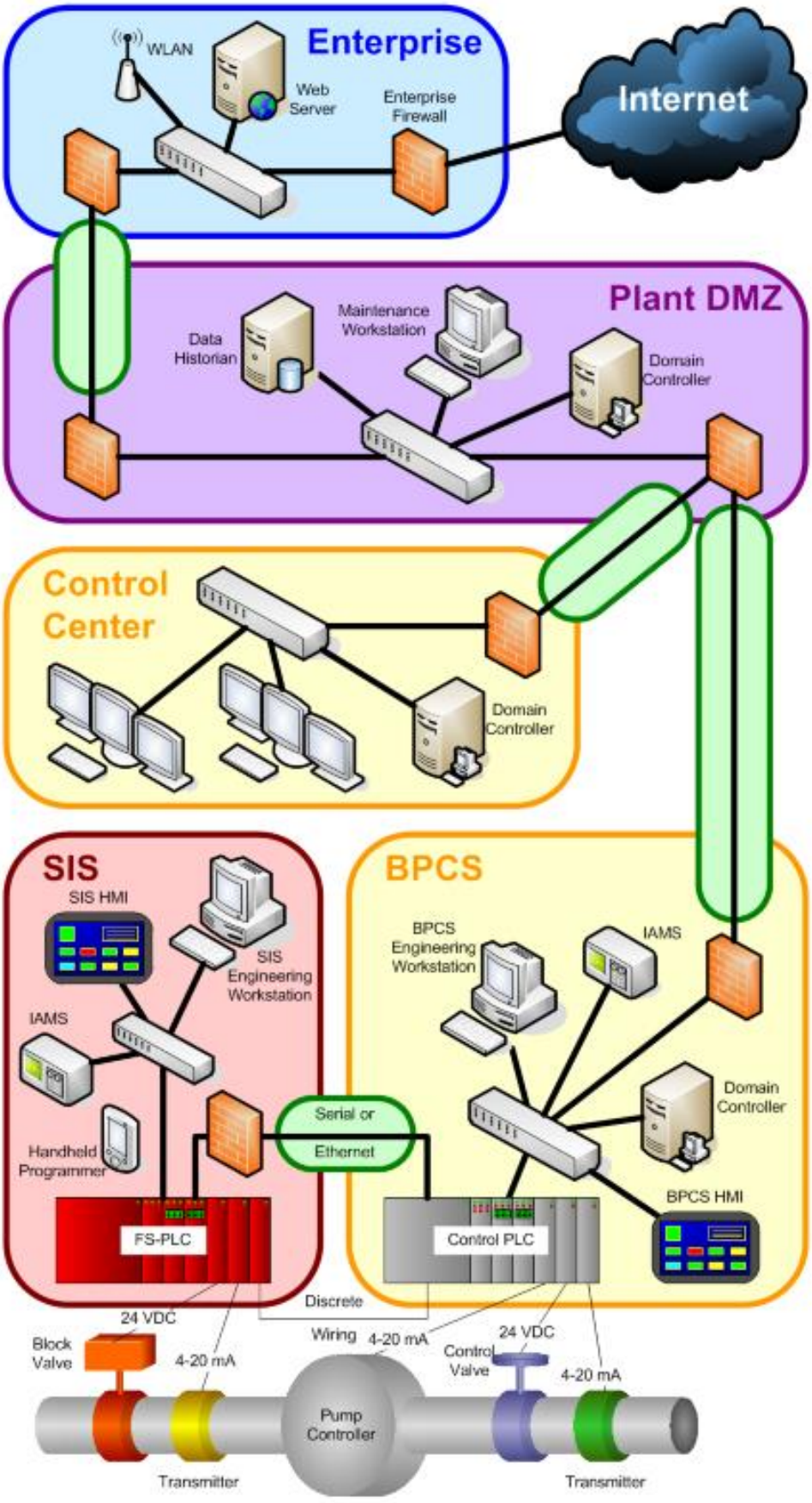
11) d
12) a
13) d
14) c
15) c

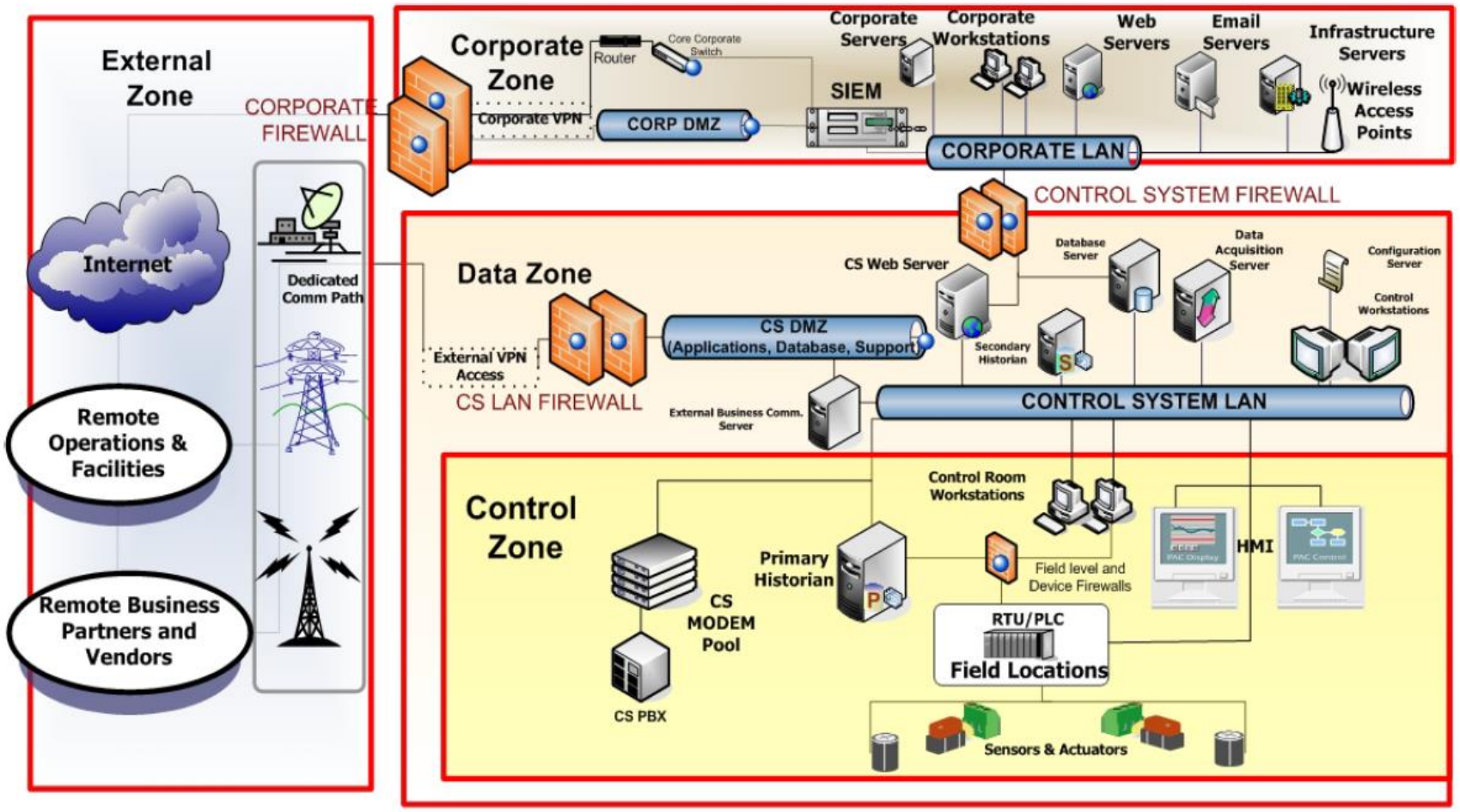
16) a
17) d
18) d
19) c
20) c

21) c
22) b
23) d
24) d
25) a

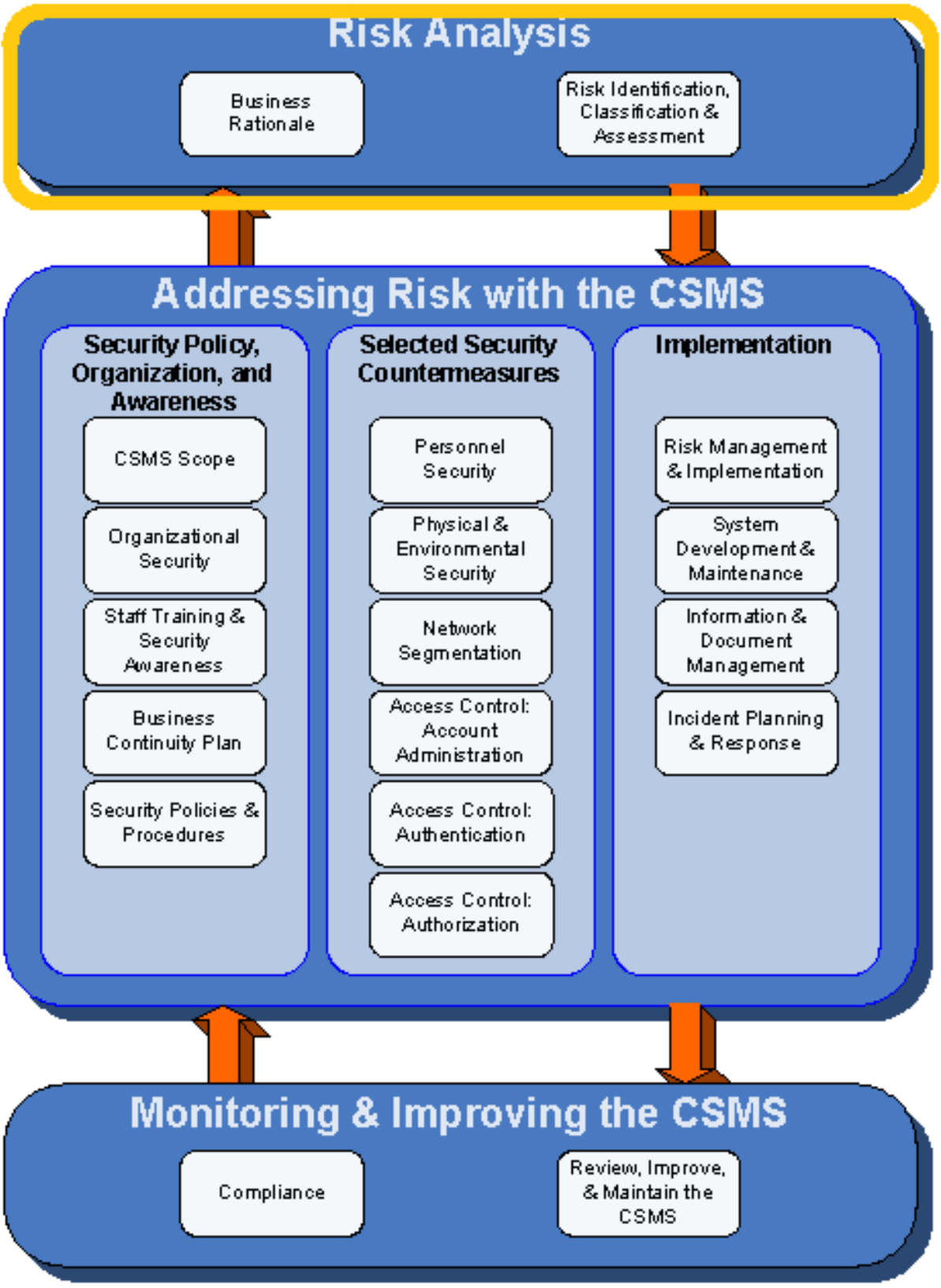
Additional Resources

Setting the Standard for Automation™


Enterprise
WLAN
Web Server
Enterprise Firewall
Internet
Plant DMZ
Data Historian
Maintenance Workstation
Domain Controller
Control Center
Domain Controller
SIS
SIS HMI
SIS Engineering Workstation
IAMS
Handheld Programmer
FS-PLC
Serial or Ethernet
BPCS
BPCS Engineering Workstation
IAMS
Domain Controller
BPCS HMI
Control PLC
Discrete Wiring
24 VDC
Block Valve
4-20 mA
Transmitter
Pump Controller
4-20 mA
Control Valve
24 VDC
4-20 mA
Transmitter


External Zone
CORPORATE FIREWALL
Internet
Dedicated Comm Path
Remote Operations & Facilities
Remote Business Partners and Vendors
Corporate Zone
Router
Core Corporate Switch
Corporate VPN
CORP DMZ
SIEM
Corporate Servers
Corporate Workstations
Web Servers
Email Servers
Infrastructure Servers
Wireless Access Points
CORPORATE LAN
CONTROL SYSTEM FIREWALL
Data Zone
CS Web Server
Database Server
Data Acquisition Server
Configuration Server
Control Workstations
CS DMZ (Applications, Database, Support)
Secondary Historian
External VPN Access
CS LAN FIREWALL
External Business Comm. Server
CONTROL SYSTEM LAN
Control Zone
Control Room Workstations
HMI
Primary Historian
Field level and Device Firewalls
CS MODEM Pool
RTU/PLC
Field Locations
CS PBX
Sensors & Actuators

memorize?


Risk Analysis
Business Rationale
Risk Identification, Classification & Assessment
Addressing Risk with the CSMS
Security Policy, Organization, and Awareness
CSMS Scope
Organizational Security
Staff Training & Security Awareness
Business Continuity Plan
Security Policies & Procedures
Selected Security Countermeasures
Personnel Security
Physical & Environmental Security
Network Segmentation
Access Control: Account Administration
Access Control: Authentication
Access Control: Authorization
Implementation
Risk Management & Implementation
System Development & Maintenance
Information & Document Management
Incident Planning & Response
Monitoring & Improving the CSMS
Compliance
Review, Improve, & Maintain the CSMS

S=Safety **E**=Environmental **F**=Financial **R**=Reputation Risk Colors/Numbers from Stakeholder Risk Matric Chart. Typical Green (little or no risk) to Yellow, Orange, Red (High Risk)

UTL=Unmitigated Threat Likelihood **SL-T**=Security Level Target **MTL**=Mitigated Threat Likelihood **ATL**=Adjusted Threat Likelihood

				Consequence														
	Threat Scenario				Impact													
Zone	Threat Source	Threat Action	Vulnerabilities	Consequence Description	S	E	F	R	Max	UTL	Risk	SL-T	Countermeasures	MTL	Risk	Recommendations	ATL	Risk
Process Control Zone	Authorized personnel	Inserts USB into Operator Station with general malware	* OS Computers are in the Control Room * USB Ports are not blocked or disabled * Autorun not disabled * No antivirus	* Denial of service on operator station that spreads to all OS on PCN * All OS and Servers need to be rebuilt * 24 - 72 hours downtime * Rework batch * Supply chain impact	1	1	2	3	3	5	15	2	* Policies and procedures	5	15	* Disable unused USB ports (e.g. GPO, registry, SEP, etc.) * Relocate OS computers to the server room and KVM to Control Room * Segment the Tag & Batch servers and EWS from the PCN and Control LAN (e.g. eliminate all dual-homed computers) * Install and maintain Antivirus * Stricter enforcement of policies * Upgrade OS and application software to supported version	2	6
		Inserts USB into Operator Station with targeted malware	* OS Computers are in the Control Room * USB Ports are not blocked or disabled * Autorun not disabled * No antivirus	* Loss of control with potential compromise of the safety of the process * Runaway reaction leading to explosion	5	5	5	5	5	2	10	1	* Policies and procedures	2	10	* Disable unused USB ports (e.g. GPO, registry, SEP, etc.) * Relocate OS computers to the server room and KVM to Control Room * Segment the Tag & Batch servers and EWS from the PCN and Control LAN (e.g. eliminate all dual-homed computers) * Install and maintain Antivirus * Stricter enforcement of policies * Upgrade OS and application software to supported version	1	5
		Plugs laptop infected with general malware into the Control LAN	* Unused ports on Control LAN switch are enabled * No policy governing use of laptops * No antivirus on Tag and Batch servers * Lack of segmentation allows for propogation	* Denial of service on operator station that spreads to all OS on PCN * All OS and Servers need to be rebuilt * 24 - 72 hours downtime * Rework batch * Supply chain impact	1	1	2	3	3	4	12	2	* Laptops are running a supported OS, are patched and running antivirus	4	12	* Develop policies to prohibit use of laptops on Control LAN * Block unused ports on Control LAN switch * Segment the Tag & Batch servers and EWS from the PCN and Control LAN (e.g. eliminate all dual-homed computers) * Install and maintain Antivirus	1	3
		Plugs laptop infected with targeted malware into the Control LAN	* Unused ports on Control LAN switch are enabled * No policy governing use of laptops * No antivirus on Tag and Batch servers * Lack of segmentation allows for propogation	* Loss of control with potential compromise of the safety of the process * Runaway reaction leading to explosion	5	5	5	5	5	2	10	1	* Laptops are running a supported OS, are patched and running antivirus	2	10	* Develop policies to prohibit use of laptops on Control LAN * Block unused ports on Control LAN switch * Segment the Tag & Batch servers and EWS from the PCN and Control LAN (e.g. eliminate all dual-homed computers) * Install and maintain Antivirus	1	5
		Engineer remotes into the EWS from the Plant Business Zone using VNC and makes changes without knowledge of current process conditions	* By default VNC credentials are in "clear text" * VNC file transfer capabilities * EWS is dual-homed	* Possible process upset or modification leading to loss of batch	1	1	2	1	2	4	8	1		4	8	* Develop and enforce MoC process * Eliminate VNC	1	2
		Unauthorized person uses the VNC credentials to gain access to EWS	* No lock-out on VNC	* Loss of control with potential compromise of the safety of the process * Runaway reaction leading to explosion	5	5	5	5	5	3	15	2		3	15	* Develop and enforce MoC process * Eliminate VNC	1	5

ISA/IEC 62443 Cybersecurity Certificate Programs Frequently Asked Questions

Apply for the ISA/IEC 62443
- Requirements
- FAQs
- Take the Exam
- Renew
- Directory

Onsite ISA Training at Your Plant

Search for ISA Cybersecurity Training

ISA's Cybersecurity Resources Brochure

White Paper on Cybersecurity

Certifications and Certificates

Program Definition

Why did ISA develop the ISA/IEC 62443 Cybersecurity Certificate Programs?
ISA has developed this program to increase knowledge and awareness of the ISA/IEC 62442 standards. The first certificate in the program is the ISA/IEC 62443 Cybersecurity Fundamentals Specialist. Other specialization certificates are also available in the areas of risk assessment, system design, and operations/maintenance.

The new ISA/IEC 62443 Cybersecurity Fundamentals Specialist certificate program is designed for professionals involved in IT and control system security roles that need to develop a command of industrial cybersecurity terminology and understanding of the material embedded in the ISA/IEC 62443 standards.

Who can say they hold a certificate?
The ISA/IEC 62443 Cybersecurity certificates are awarded to those who successfully complete a designated training course and pass a 75-100 question multiple choice exam.

How does the ISA/IEC 62443 Cybersecurity Certificate Program compare to other security programs?
Review the comparison chart here.

- top -

Training Course Requirements

Why are courses required for the ISA/IEC 62443 certificate program exam candidates?
Certificate programs are typically associated with mastery of specific course content and may or may not require work experience. The ISA/IEC 62443 certificate program was developed by ISA working with industry experts. The program(s) increase knowledge/awareness and application of the ISA/IEC 62443 standard through mastery of the course material and examination.

What training courses can I take to qualify to take the ISA/IEC 62443 Cybersecurity Fundamentals certificate exam?
ISA's two-day classroom course, Using the ISA/IEC 62443 Standards to Secure Your Industrial Control System (IC32), must be sucessfully completed in order to be eligible to take the ISA/IEC 62443 Cybersecurity Fundamentals certificate exam. Or, ISA's multi-week, online course: Cyber Security for Automation, Control and SCADA Systems (IC32E) is also an eligible option to complete and sit for the exam.

For other exam specialization areas, there are specific related coursework for same.

What if I already took the IC32 or IC32E courses?
If you took either course LESS THAN one year from the date you wish to take the exam, you do not have to retake the course and can register for the certificate exam. If you took either course MORE THAN one year from the date you wish to take the exam, you must retake the course in order to be eligible to sit for the certificate exam.
Will course participants receive CEUs for the courses taken?
Yes. The number of CEUs is determined by the number of instructional hours, and awarded upon successful completion of the course. Completing course post-tests and receiving CEUs for course completion are not connected to passing scores on one of the certificate exams.

What if a course is rescheduled by a candidate or ISA?
A candidate is not eligible to sit for the exam until he or she successfully completes the prerequisite course. Click here for information regarding course cancellations/rescheduling.

- top -

Documentation

What paperwork must be completed to take one of the exams?
No application is required for the ISA/IEC 62443 Cybersecurity certificate exams.

What are the pre-requisites for the certificate program?
There are no required prerequisites for this program; however, it is highly recommended that applicants have:

- Three to five years of experience in the IT cybersecurity field with some experience in an industrial setting-with at least two years specifically in a process control engineering setting
- Some level of knowledge or exposure to the ISA/IEC 62443 standards
- **More advanced courses have recommended coursework, in addition to experience, but it is not required. Certificate 1 attainment is required to go onto all other certificate levels.**

- top -

Fees

What are the fees for the certificate program?
Fees for required courses can be found on the course registration page. The exam fee for an ISA/IEC 62443 certificate exam is $200. There are no group discounts for certificate exam fees. This fee includes one electronic exam.

Can an exam be rescheduled without incurring fees?
Applicants may reschedule an exam appointment during the six (6) month eligibility period by contacting Prometric at least 2 days (48 hours) prior to the scheduled exam time for Prometric locations in the United States/Canada and at least 5 days (120 hours) prior to the scheduled exam time for all other Prometric locations. No reschedule fee will apply.

Prometric Location	Advance Notice Required to Reschedule with no fee
United States/Canada	At least 2 days (48 Hours) Prior to Scheduled Exam Date
All other locations	At least 5 Days (120 hours) Prior to Scheduled Exam Date

What are the reschedule fees?
Candidates who do not appear for their scheduled exam appointment and do not give proper advance notice of intent to reschedule their exam will incur a fee of $150.

Can a candidate retest and what is the retest fee?
Applicants may retest within the six (6) month eligibility period for a fee of $150. If you are outside the six (6) month eligibility period, you must register again for the required course and exam and re-take both.

What if a candidate cannot make the scheduled appointment or is late for the appointment?
For candidates who fail to appear for a scheduled exam, or arrive more than 15 minutes after the scheduled start time, the $150 reschedule fee will apply. The exam must be rescheduled within the candidate's six (6) month eligibility period.

What forms of payment does ISA accept for the certificate program fees?
ISA will accept check, certified check, money order, or wire transfer (in U.S. Dollars), credit card and purchase orders. Make checks payable to ISA. For wire transfer account information, please contact ISA Customer Service at info@isa.org or +1 919-549-8411. ISA accepts AMEX, Discover Card, Master Card, and VISA credit cards.

Payment should be received with the course registration.

Is the certificate program exam fee refundable?
ISA/IEC 62443 certificate program fees are refundable, less a $50 processing fee, if you decide not to take the exam after completing the course and within the six-month eligibility window.

- top -

Testing

The ISA/IEC 62443 Cybersecurity Certificate Program exams are offered electronically through the Prometric global network of testing centers in early 2014. For testing center locations, visit www.prometric.com/isa. The exams are not offered the day after completing the required course.

How does one become eligible to take an ISA/IEC 62443 certificate exam?
Certificate program applicants must register for the required course and the exam, and successfully complete the required course. Click here to review the certificate program requirements.

When will applicants find out if they are eligible to take an ISA/IEC 62443 certificate program exam?
Within 5 business days of completion of the required course, an eligibility email that contains the information needed to schedule a paper/pencil exam (or a computer-based exam at Prometric, when available) will be sent to the exam candidate.

How long is an applicant eligible to take an ISA/IEC 62443 certificate program exam?
The certificate exam and any retests must be taken within six (6) months of the last day of the certificate program course.

What if the required course is not completed?
If the applicant is still interested in pursuing the certificate, he/she must register for the course and exam again and re-take the course. Once the course is successfully completed, the candidate is eligible to sit for the exam.

What is a passing score for an ISA/IEC 62443 certificate program exam?
Passing scores vary for all level exams based upon different number of questions at each level.

What if a candidate does not pass the certificate exam?
If a candidate fails the exam, he/she may retest one time within the initial six (6) month eligibility window for a fee of $150. If an applicant does not pass the exam within the six (6) month window after the course and would like to receive the certificate, the

applicant must register for the course and exam again and re-take both.

An ISA99/IEC 62443 certificate program exam must be taken within six (6) months of the last day of the certificate program required course. If a candidate fails the exam, he/she may retest one (1) time within the six (6) month eligibility period. If a candidate does not pass the exam within the six (6) month window after the course and would like to receive the certificate, the applicant must register for the course and exam again and re-take both.

Once the computer-based exam is available, applicants who sucessfully complete the program requirements will receive an email with an eligibility code to use to schedule their exam through Prometric. In this case, you would go to www.prometric.com/isa to review locations and schedule an appointment.

Once scheduled, how is an exam confirmed?
Exam appointments are confirmed by Prometric via email. ISA does not provide candidate email addresses to Prometric-the candidate provides the email address they wish to receive the exam confirmation.

What if an exam confirmation is not received from Prometric?
Contact Prometric Candidate Care at 800-853-6769 and ask that it be emailed to you again. ISA cannot provide the confirmation for you.

Who should be contacted to reschedule an exam appointment?
Candidates must contact ISA if an exam appointment needs to be rescheduled. If the appointment is not cancelled at least 2 days in advance at Prometric locations in the United States/Canada or at least 5 days in advance at other Prometric locations, a reschedule form must be completed and sent to ISA with payment before the candidate eligibility can be re-set.

- top -

Examination Process

Once a candidate is eligible, how much time is available for testing?
The eligibility period to take a certificate exam is six (6) months from the date the course is completed. You must complete all testing within the six (6) month eligibility period, including any reschedules or retests. Candidates have two hours to complete the exam.

Are there testing windows for taking certificate exams?
There are no testing windows for taking any of the certificate exams. Testing center availability is set by each Prometric testing center in the Prometric network. Some Prometric testing centers offer evening and Saturday appointments. Paper/Pencil exams can be schedule through ISA customer service: +1 919-549-8411.

When should a candidate arrive at the testing center?
Candidates should arrive at the testing center no later than 30 minutes prior to the scheduled exam time to sign-in and receive instruction. All examinations are given in a two hour time period.

What if the testing center cannot accommodate an exam appointment?
If technical difficulties or inclement weather cause the cancellation of an appointment or the closure of a Prometric testing center, Prometric will attempt to contact the candidate using the phone numbers provided to them by ISA. Last minute cancellation situations will be handled on a case-by-case basis, and ISA and Prometric will work together to reschedule the candidate as quickly as possible.

What should be brought to the testing center?
The Confirmation Letter from Prometric and a valid government issued photo ID with signature.

Are there any materials that are not allowed at the testing center?
All exams are closed book. No reference material will be allowed in the testing center. A location for personal items such as a pocket book, palmtop, mobile phone, or pager will be made available to you. Please note that storage space will be limited.

Will anything be provided to candidates at the testing center?
A whiteboard with marker will be provided when candidates check-in at the testing center, and a scientific calculator will be available as a hot button on the computer screen.

When are candidates notified of their certificate status?
Results are reported immediately at the testing center. If a candidate passes, a certificate will be mailed within thirty (30) days of the exam date. Failing candidates receive a diagnostic report of how they performed on the exam at the testing center.

What if the testing center does not provide the testing results?
If the testing center is unable to provide testing results, have the test center administrator complete a candidate incident report and then let ISA know by calling Customer Service at +1 919-549-8411.

- top -

Renewal

Because the ISA/IEC 62443 Cybersecurity Certificate Programs are *certificates* and not *certifications*, you are not required to renew your ISA/IEC 62443 certificate(s); however, once obtained your certificate(s) will only be considered **current** for three (3) years. After your three-year expiration date, your certificate's status will no longer be considered active and you will not be able to claim that you hold a current/active ISA/IEC 62443 certificate. Click here to learn more about extending the current status of your certificate(s).

- top -

Displaying Your ISA/IEC 62443 Certificate

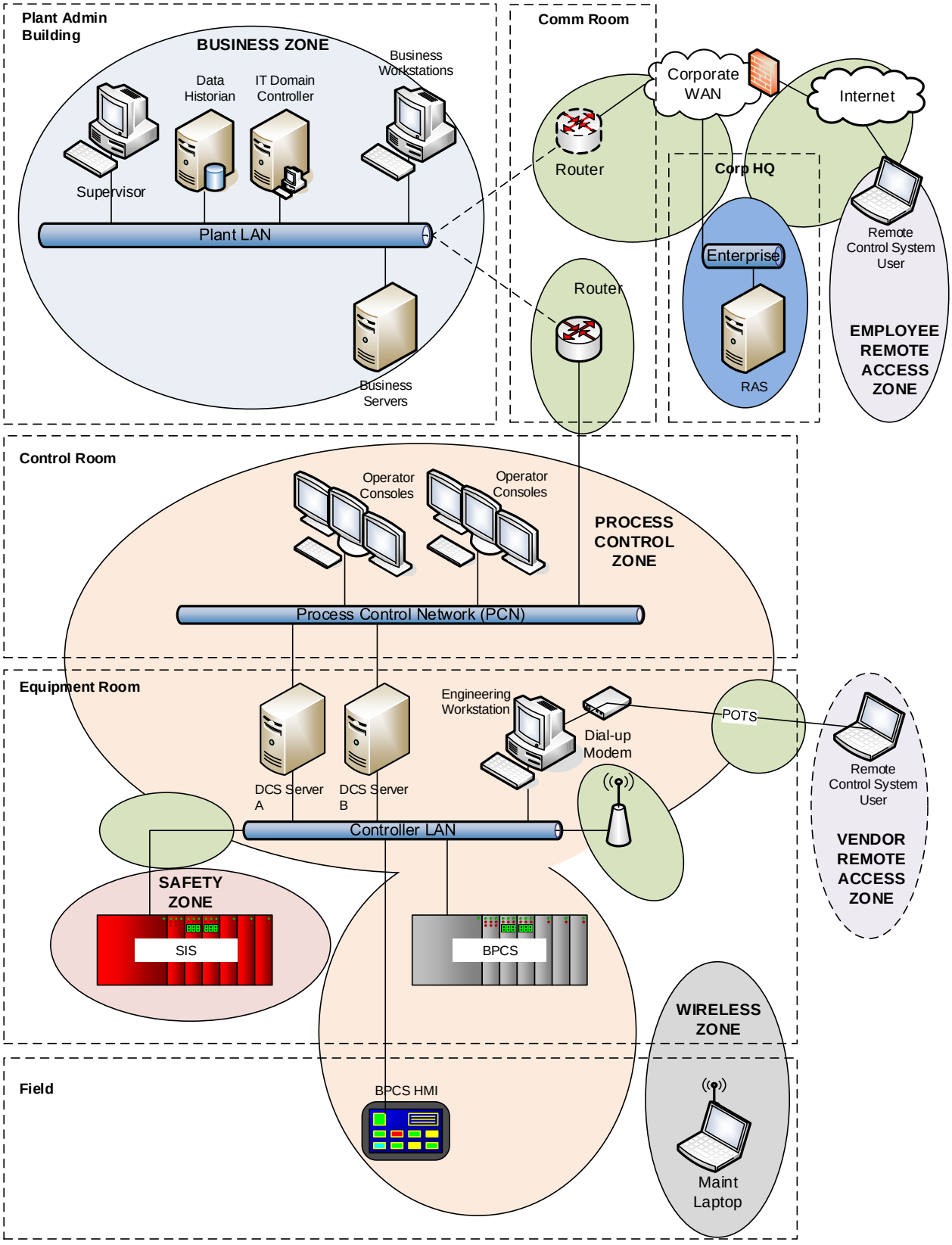
Program Credentials

How do I get a copy of my ISA/IEC 62443 certificate in case I lose it or if my supervisor wants one?
To receive a duplicate copy of your certificate, send a written request to ISA with your mailing address and payment of $15 for a duplicate certificate. Once your payment is received, a certificate will be mailed to you.

How should I display my ISA/IEC 62443 certificate designation(s) on business cards, in signature blocks, etc.?
ISA recommends the following for displaying or noting your credentials:

- If you have achieved ISA/IEC 62443 Certificate 1: **ISA/IEC 62443 Cybersecurity Fundamentals Specialist** (ISA/CFS)
- If you have achieved ISA/IEC 62443 Certificate 2: **ISA/IEC 62443 Cybersecurity Risk Assessment Specialist** (ISA/CRS)
- If you have achieved ISA/IEC 62443 Certificate 3: **ISA/IEC 62443 Cybersecurity Design Specialist** (ISA/CDS)
- If you have achieved ISA/IEC 62443 Certificate 4: **ISA/IEC 62443 Cybersecurity Maintenance Specialist** (ISA/CMS)

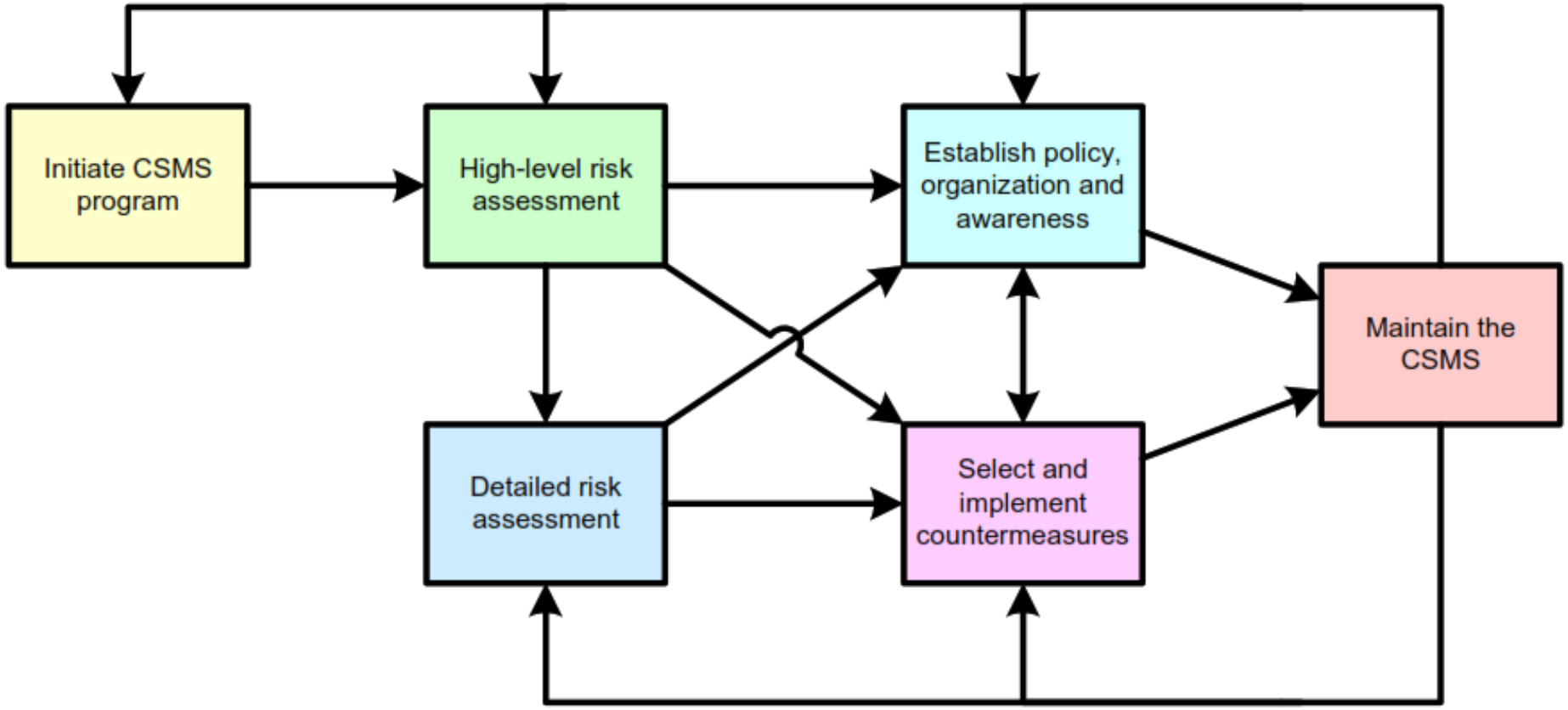
Because these are certificate programs and not certification programs, you should not list your ISA/IEC 62443 certificate designations directly after your name. On your business card (signature block, resume, etc.), you should display/include your ISA/IEC 62443 certificate designation in an area distinctly separate from your name and certificate/licensure/degree designations (e.g. CAP, PE, MBA, etc.). When possible, include "Certificate" or "Certificate Holder" after your ISA/IEC 62443 designation listing (e.g. ISA/IEC 62443 Cybersecurity Fundamentals Specialist Specialist Certificate Holder).


Plant Admin Building
BUSINESS ZONE
Business Workstations
Data Historian
IT Domain Controller
Supervisor
Plant LAN
Business Servers
Comm Room
Corporate WAN
Internet
Router
Corp HQ
Router
Enterprise
RAS
Remote Control System User
EMPLOYEE REMOTE ACCESS ZONE
Control Room
Operator Consoles
Operator Consoles
PROCESS CONTROL ZONE
Process Control Network (PCN)
Equipment Room
Engineering Workstation
Dial-up Modem
POTS
DCS Server A
DCS Server B
Controller LAN
SAFETY ZONE
SIS
BPCS
Remote Control System User
VENDOR REMOTE ACCESS ZONE
WIRELESS ZONE
Field
BPCS HMI
Maint Laptop

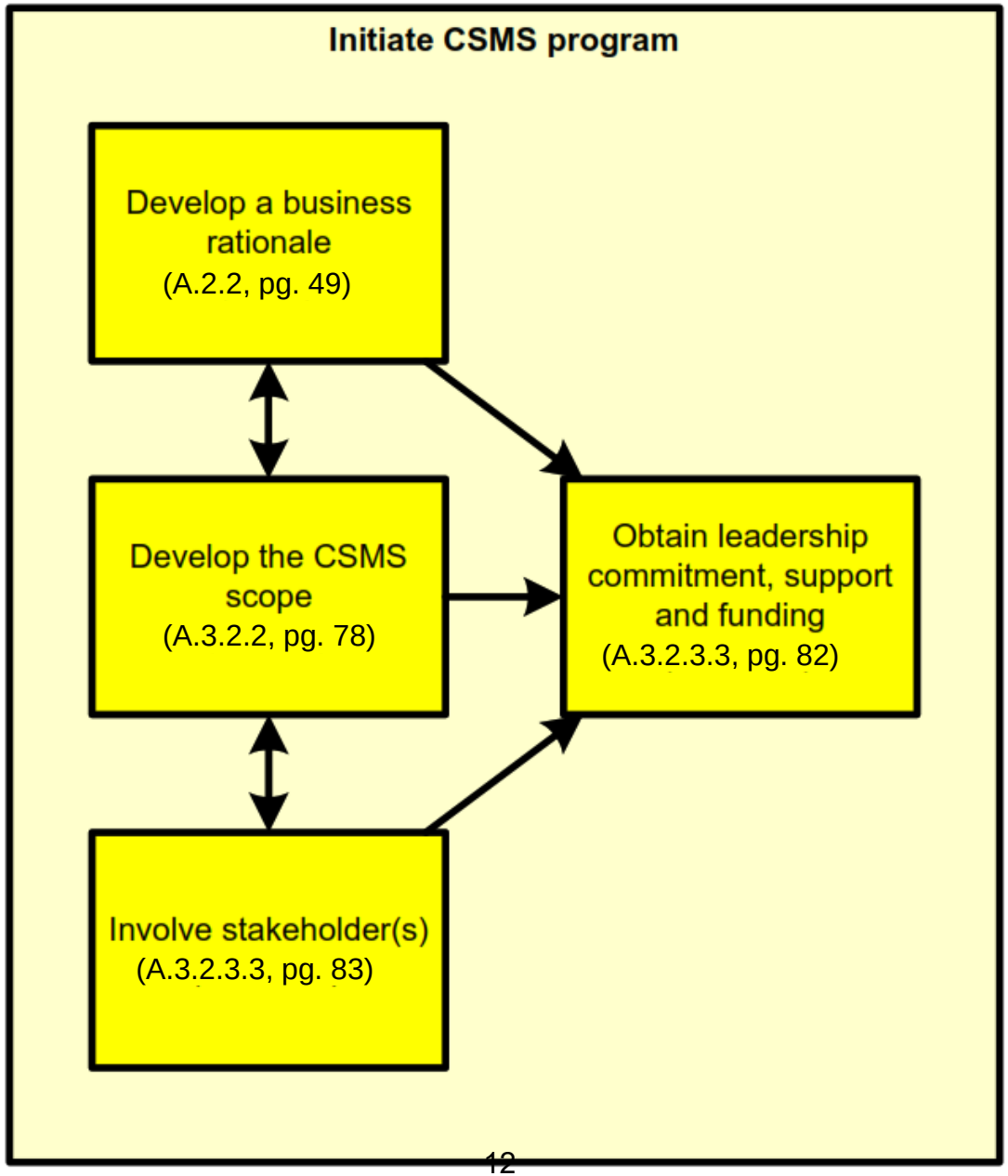
CSMS Boils Down to Six Top Level Activities

Standards
Certification
Education and Training
Publishing
Conferences and Exhibits

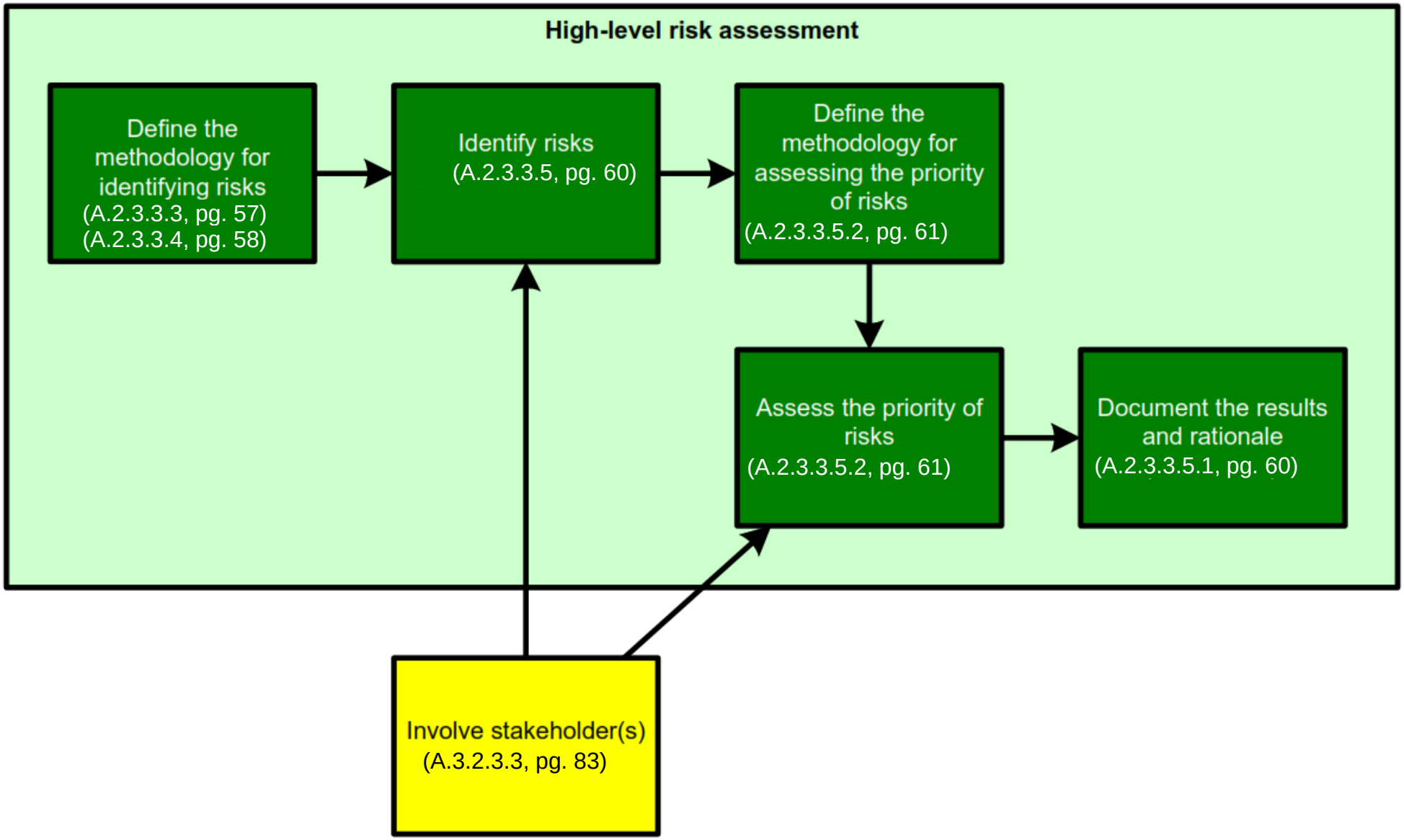
Description of the Process



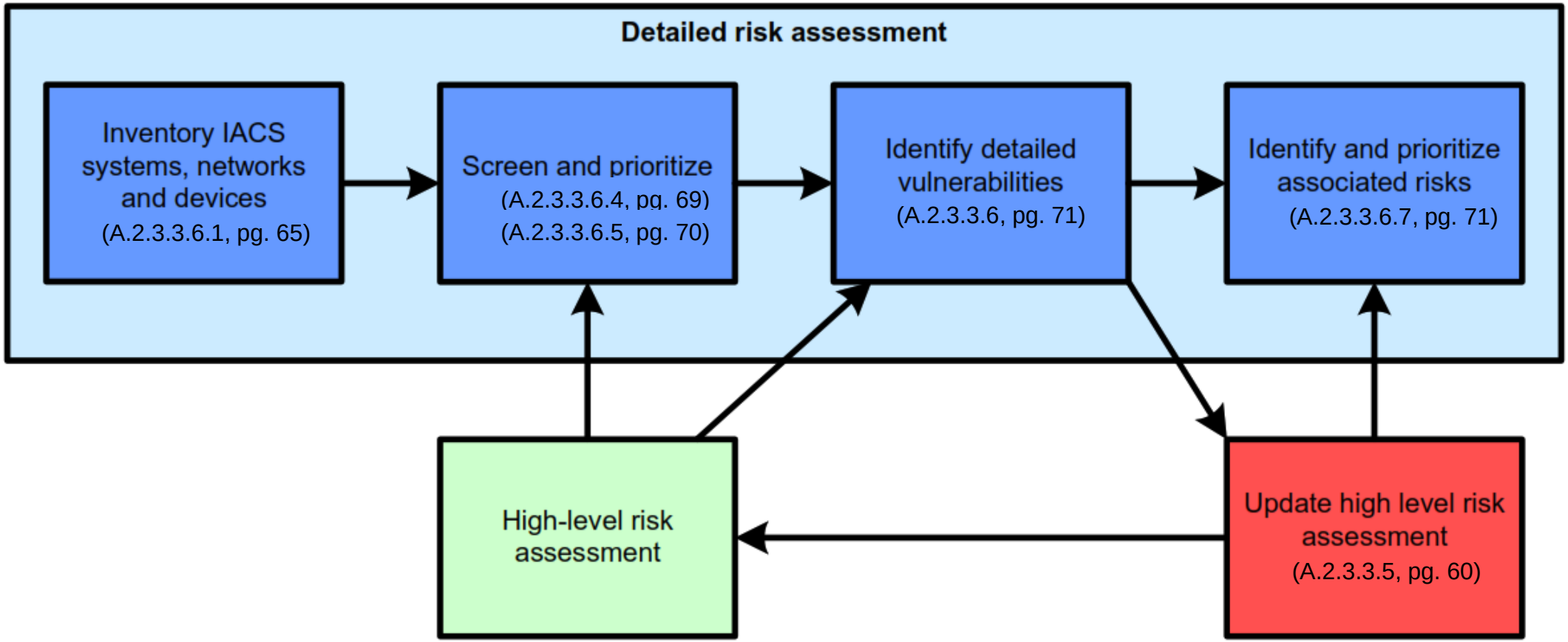
Initiate the CSMS Program



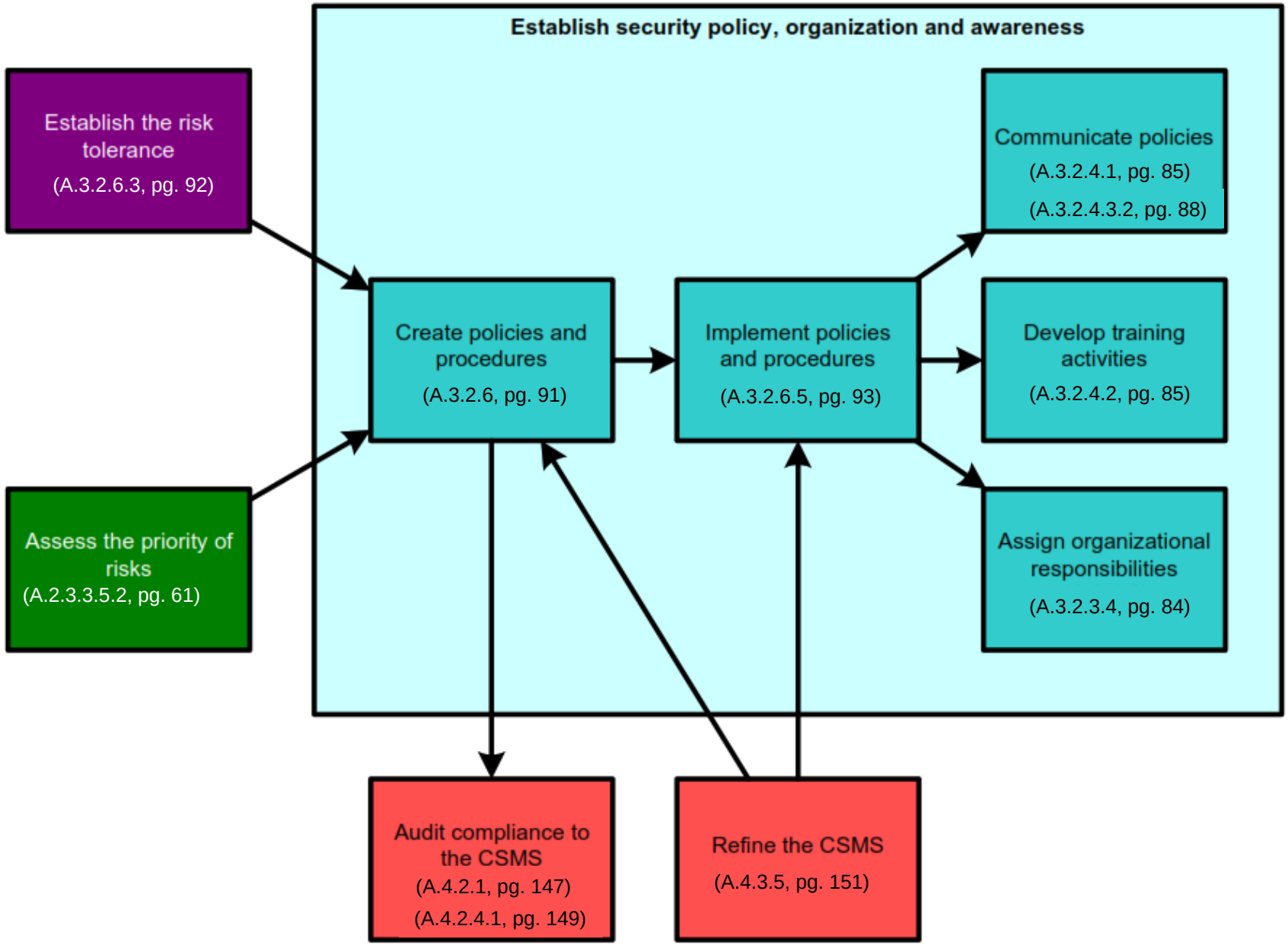
High-level Risk Assessment



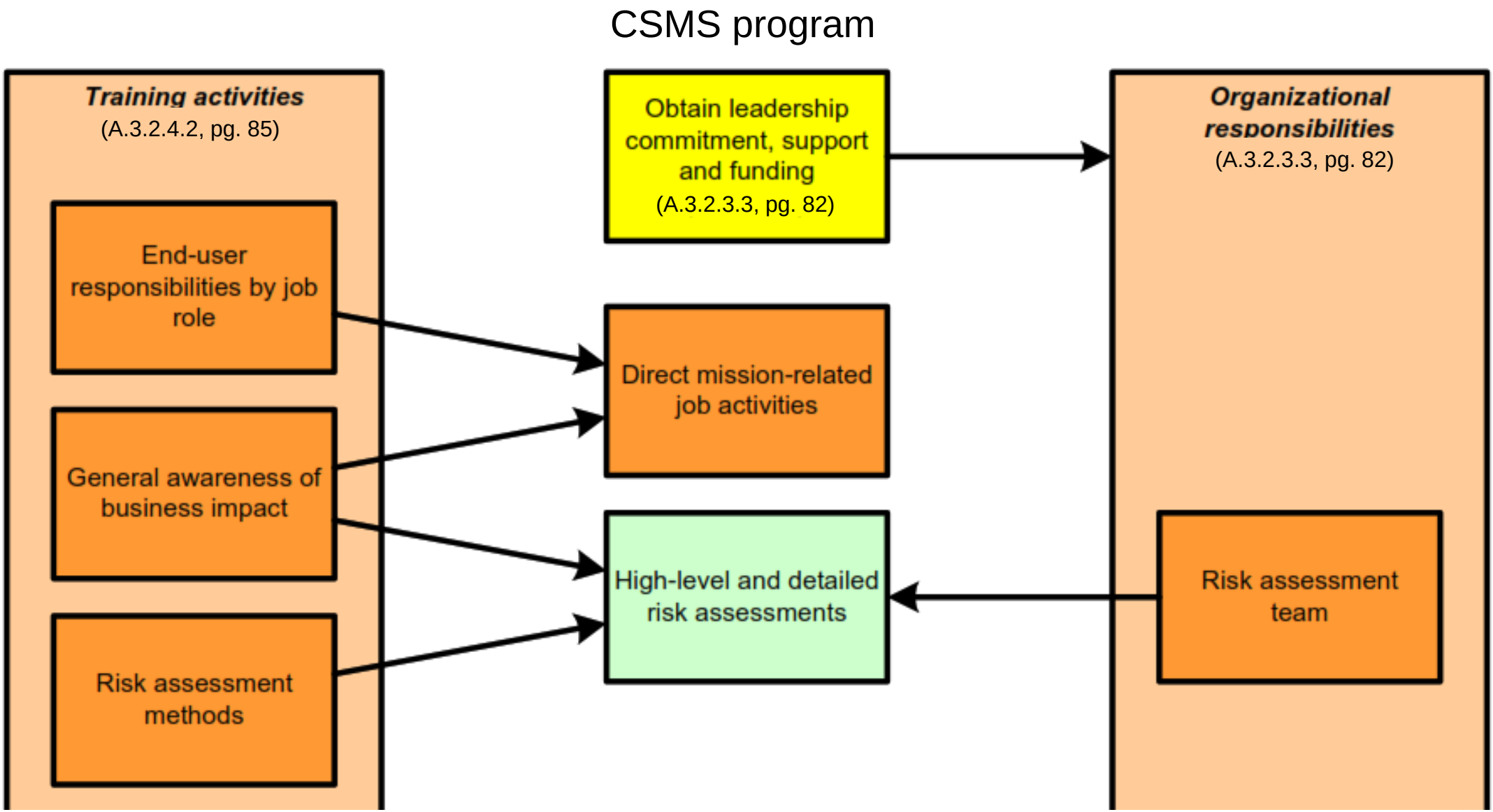
Detailed Risk Assessment



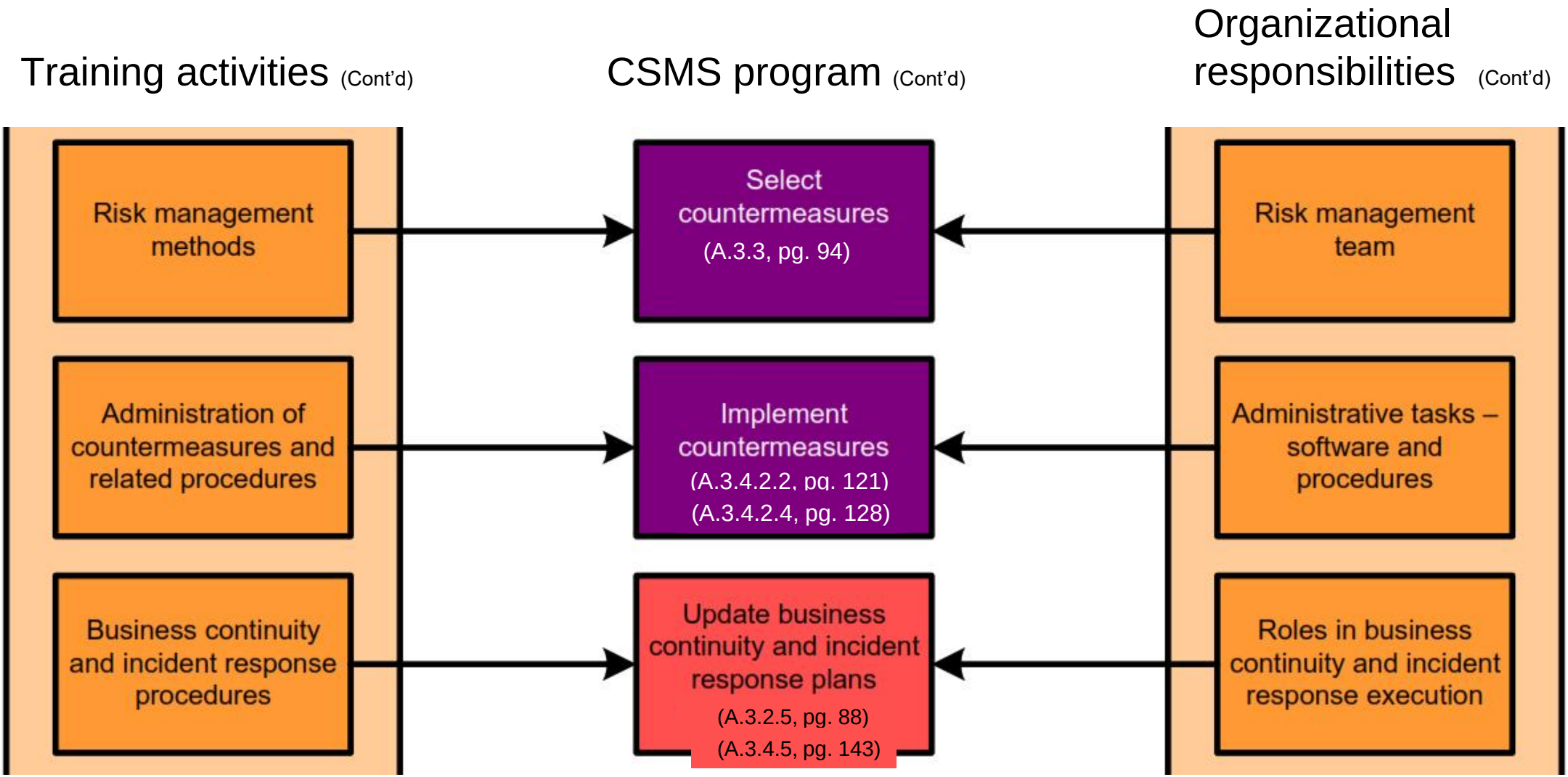
Establish Policy, Organization & Awareness



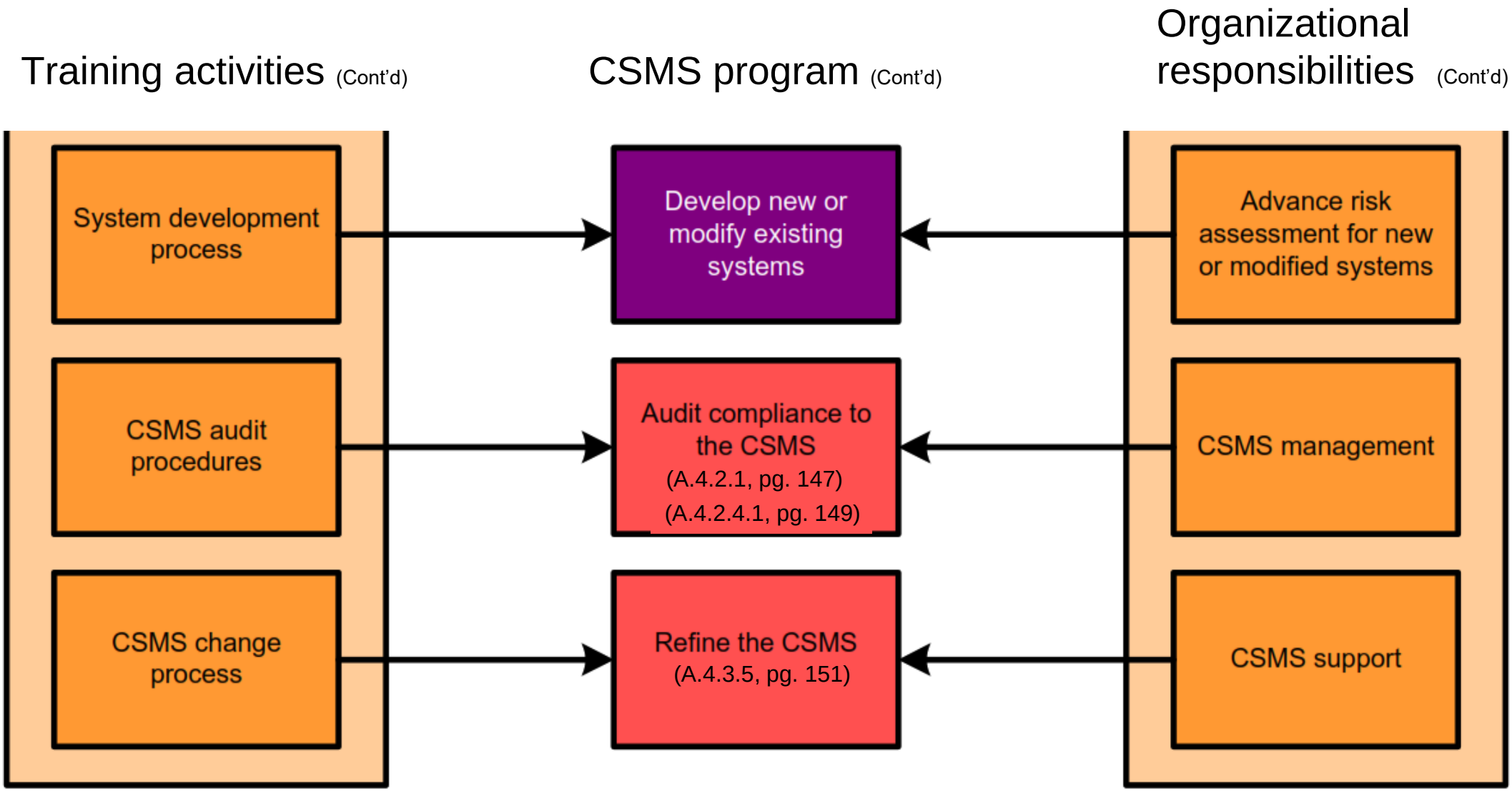
Training and Assignment of Responsibilities (Cont'd)



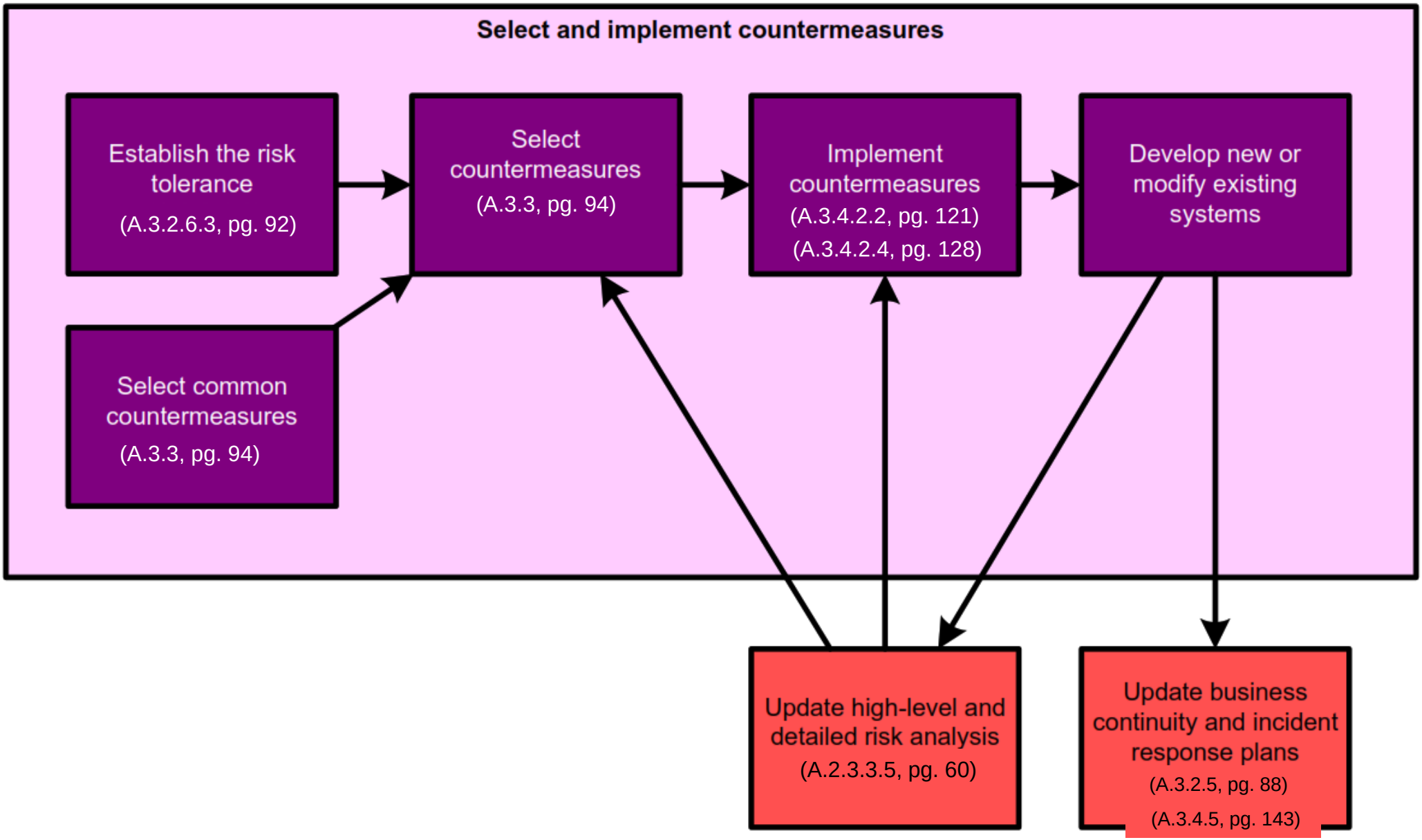
Training and Assignment of Responsibilities (Cont'd)



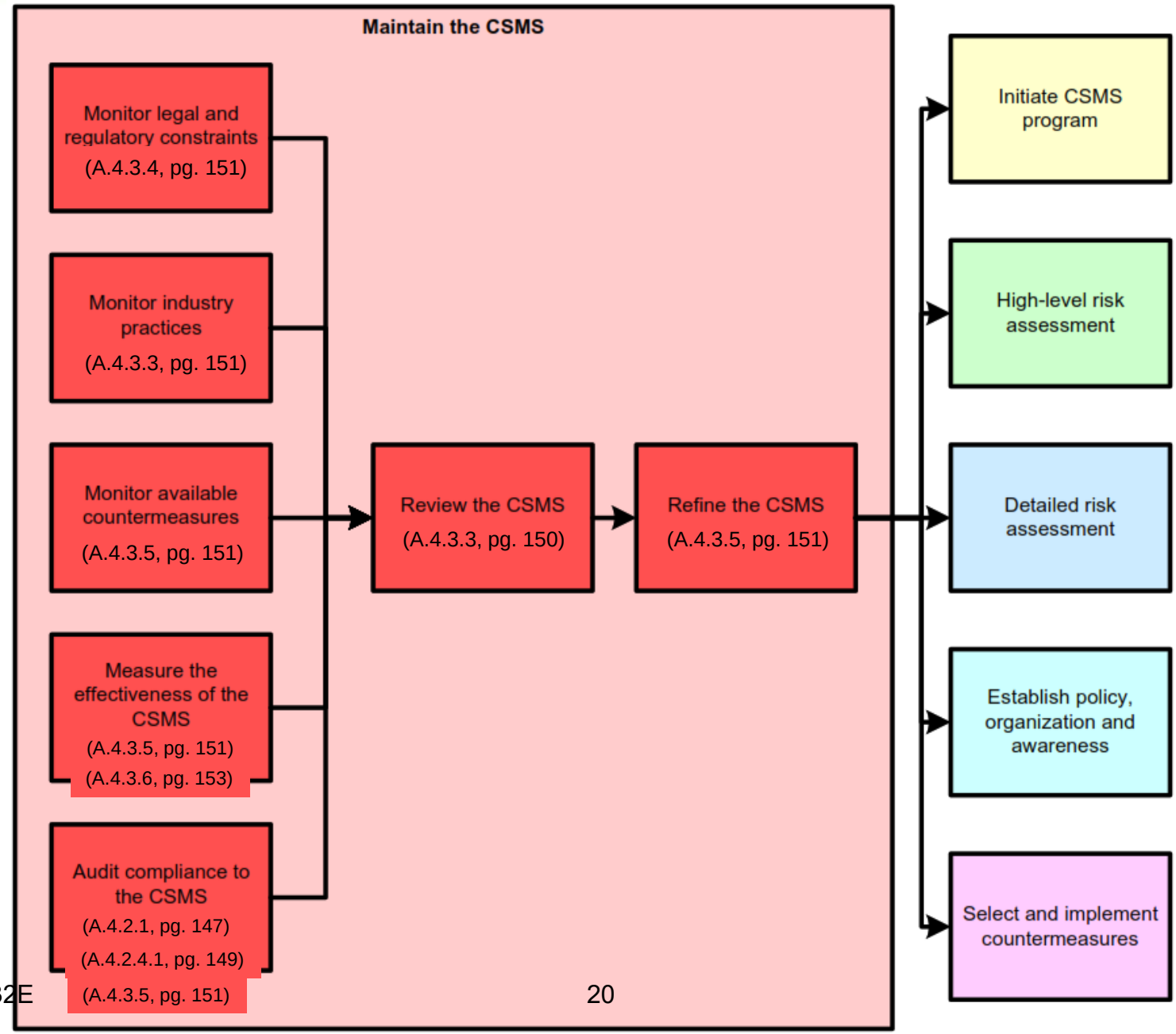
Training and Assignment of Responsibilities (Cont'd)



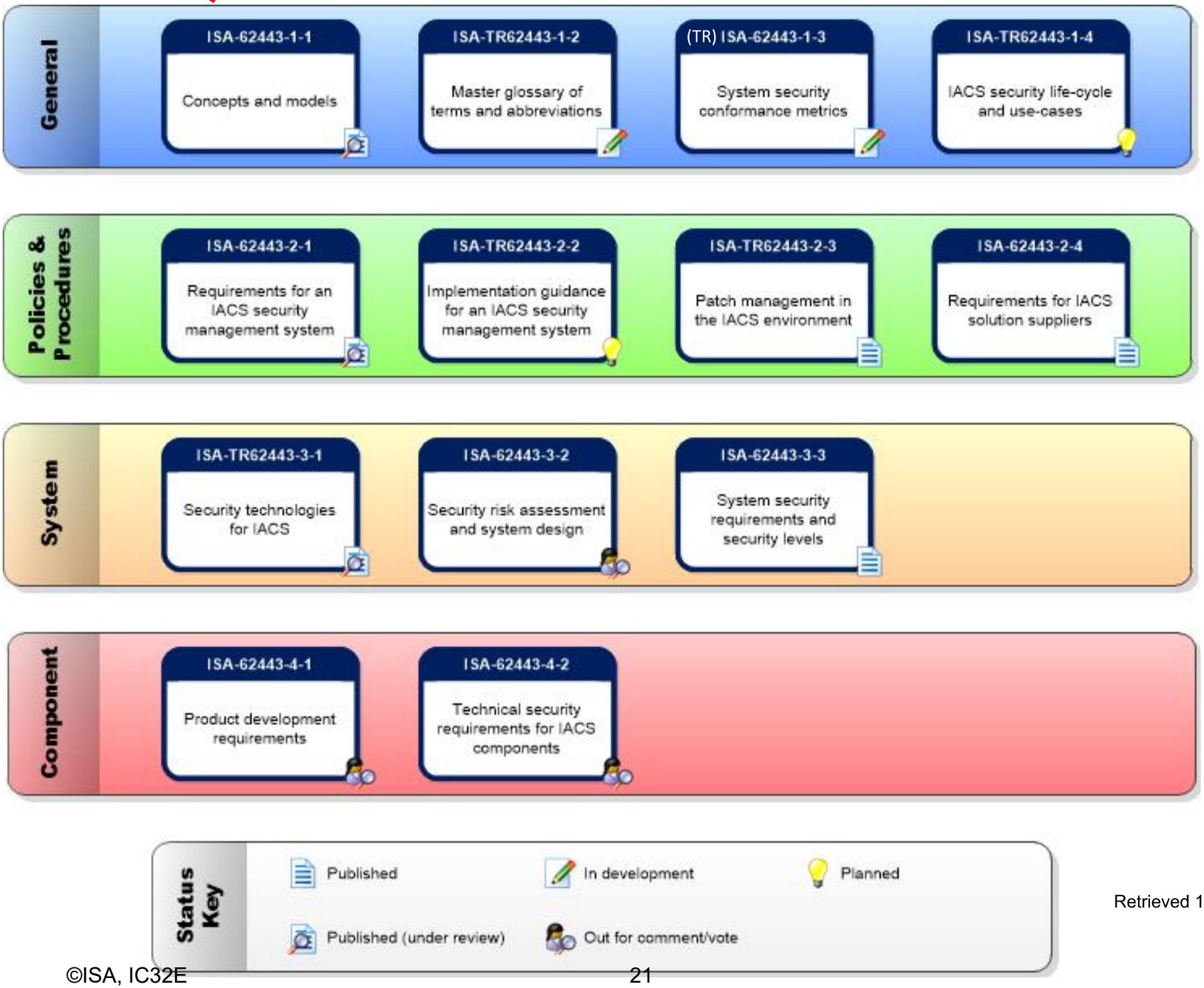
Select and Implement Countermeasures



Maintain the CSMS

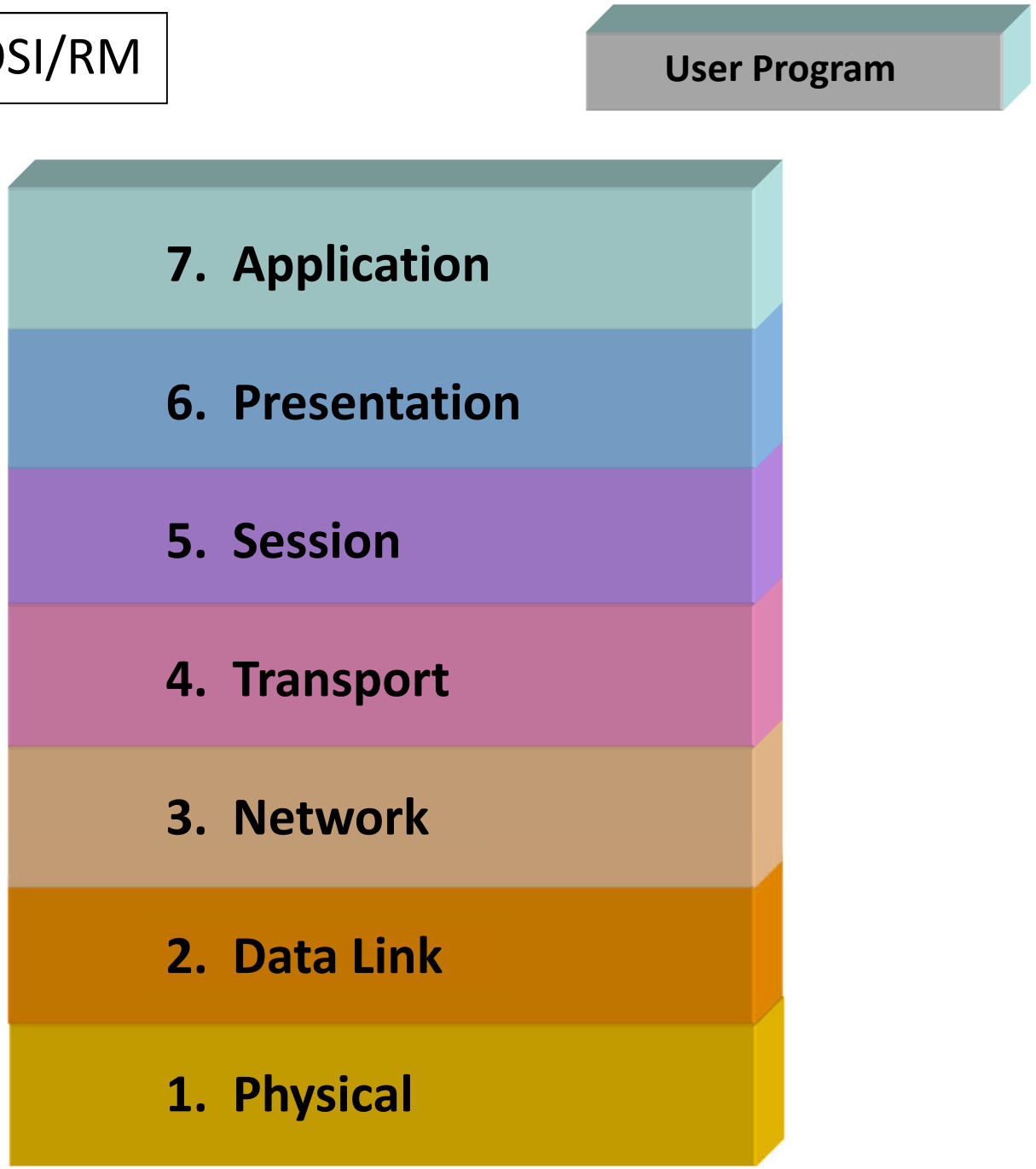


memorize?



Retrieved 16 Dec 2016

ISO Seven Layer OSI/RM



The ISO Open System Interconnection Reference Model (OSI/RM) defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.

- **Application (Layer 7)** This layer supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Telnet and FTP are applications that exist entirely in the application level. Tiered application architectures are part of this layer.

- **Presentation (Layer 6**) This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer.

- **Session (Layer 5)** This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.

- **Transport (Layer 4)** This layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.

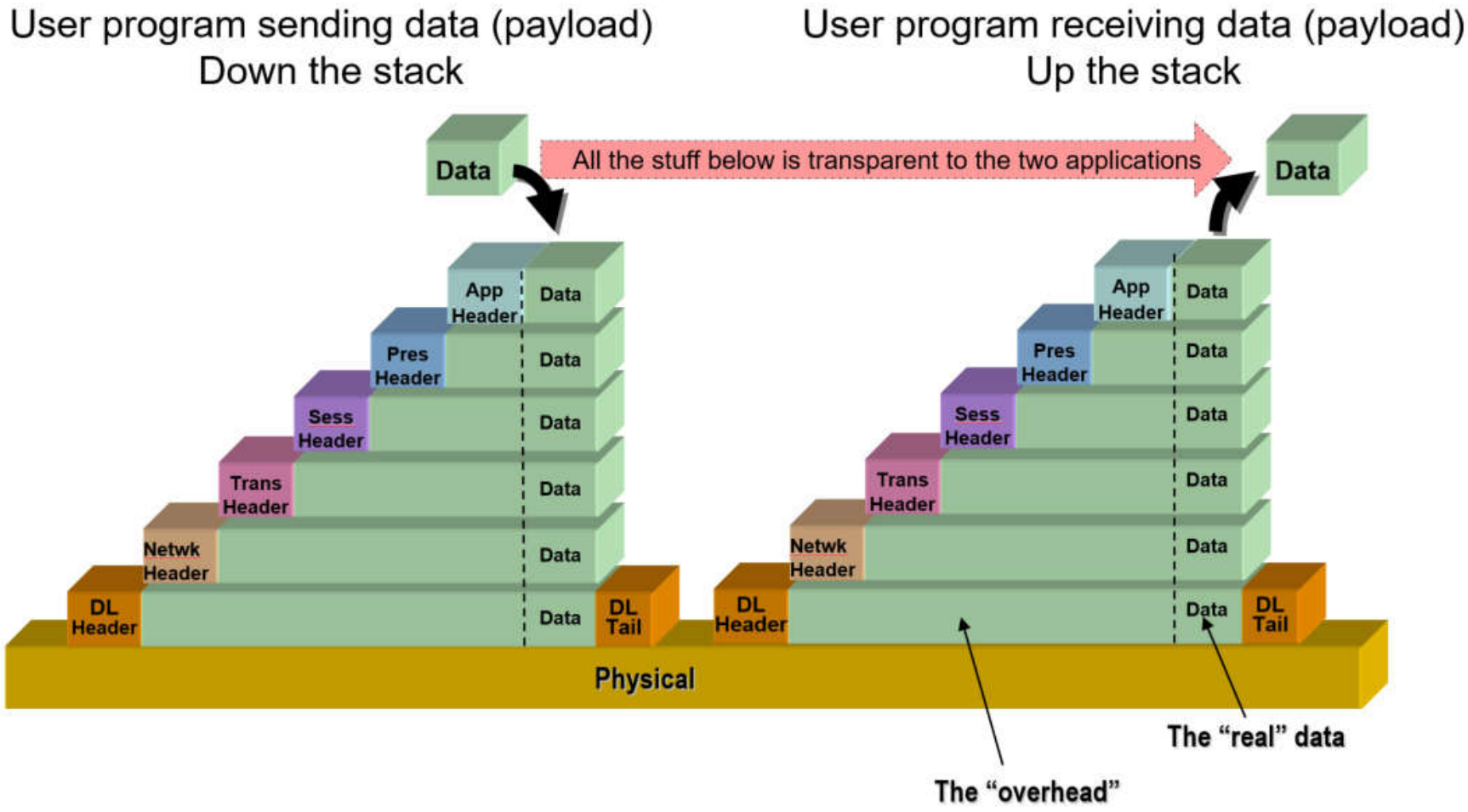
- **Network (Layer 3)** This layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.

- **Data Link (Layer 2)** At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sub layers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sub layer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.

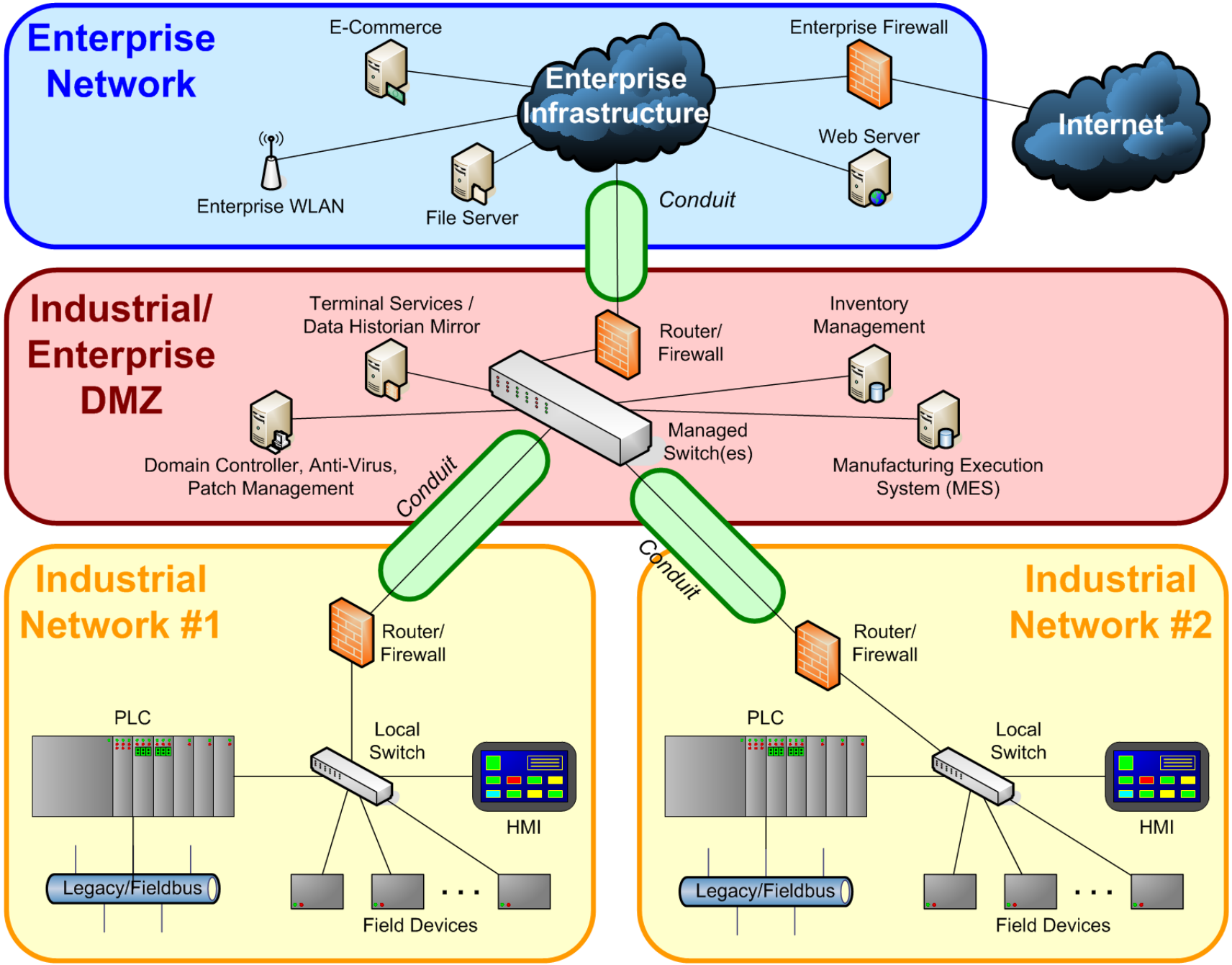
- **Physical (Layer 1)** This layer conveys the bit stream - electrical impulse, light or radio signal -- through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components.

Encapsulating the Data

- **Data** passes down and up through the layers
  - Each layer adds or removes instructions (a header)

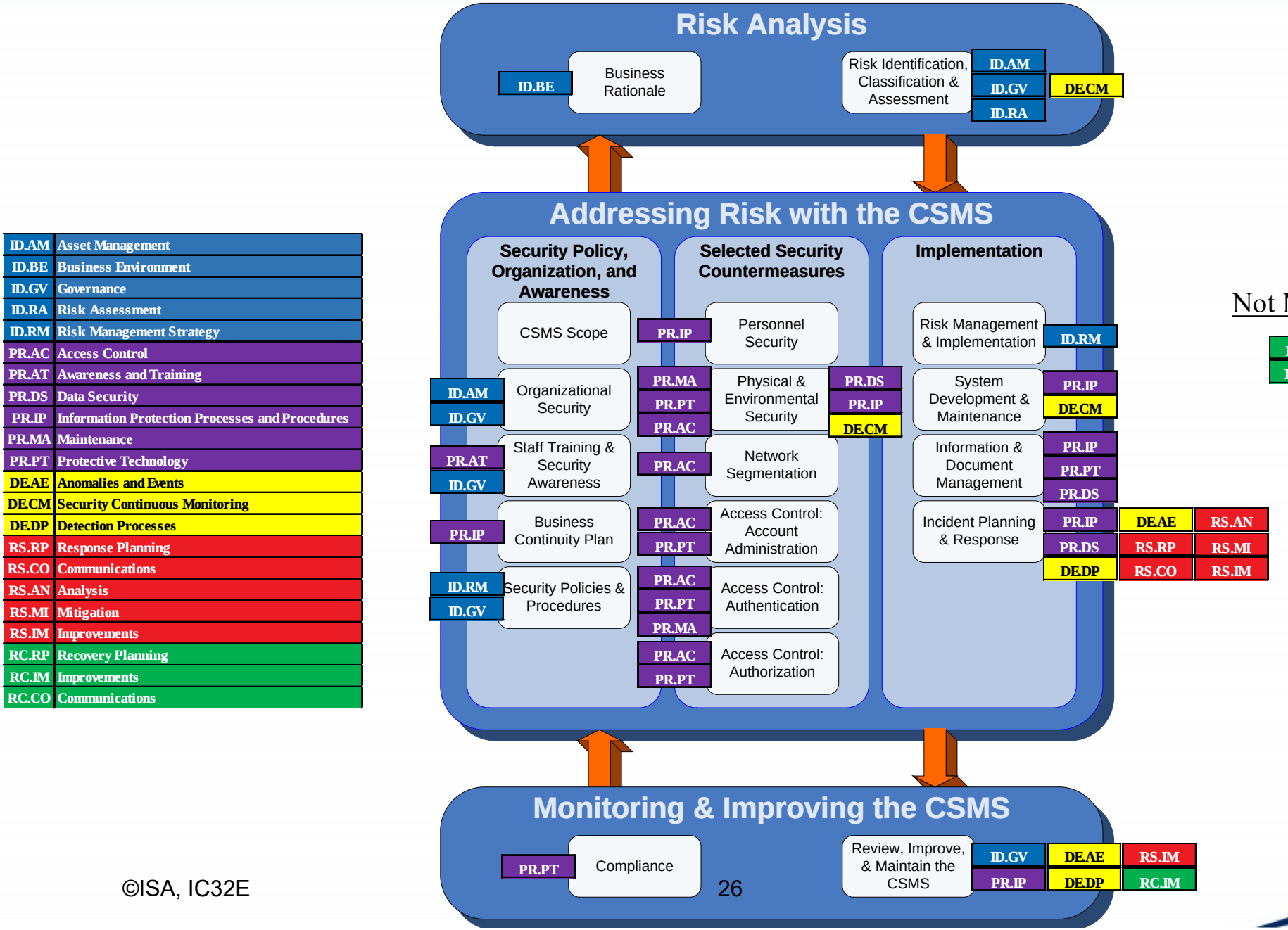


3 of 3


Enterprise Network
E-Commerce
Enterprise Infrastructure
Enterprise Firewall
Internet
Web Server
Enterprise WLAN
File Server
Conduit
Industrial/ Enterprise DMZ
Terminal Services / Data Historian Mirror
Router/ Firewall
Inventory Management
Managed Switch(es)
Domain Controller, Anti-Virus, Patch Management
Manufacturing Execution System (MES)
Conduit
Conduit
Industrial Network #1
Router/ Firewall
PLC
Local Switch
HMI
Legacy/Fieldbus
Field Devices
Industrial Network #2
Router/ Firewall
PLC
Local Switch
HMI
Legacy/Fieldbus
Field Devices

Mapping the NIST Framework Categories to ISA 62443-2-1

memorize mapping NIST to ISA-62443-2-1?



ID.AM	Asset Management
ID.BE	Business Environment
ID.GV	Governance
ID.RA	Risk Assessment
ID.RM	Risk Management Strategy
PR.AC	Access Control
PR.AT	Awareness and Training
PR.DS	Data Security
PR.IP	Information Protection Processes and Procedures
PR.MA	Maintenance
PR.PT	Protective Technology
DE.AE	Anomalies and Events
DE.CM	Security Continuous Monitoring
DE.DP	Detection Processes
RS.RP	Response Planning
RS.CO	Communications
RS.AN	Analysis
RS.MI	Mitigation
RS.IM	Improvements
RC.RP	Recovery Planning
RC.IM	Improvements
RC.CO	Communications

Not Mapped:

RC.RP
RC.CO

Notes

Notes
Notes
Notes
Notes
Notes

Setting the Standard for Automation™