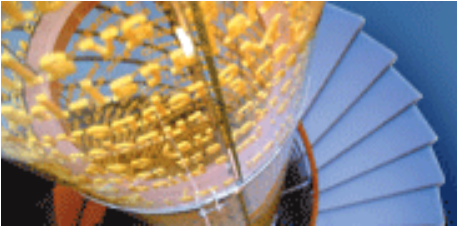

HALMSTAD UNIVERSITY

Establishing Secure Enclaves
Lecture 5

Urban Bilstrup

Urban.Bilstrup@hh.se

Outline (Chapter 7)

- Introduction
- Identifying Functional Groups
- Establishing Enclaves
- Securing Enclave Perimeters
- Securing Enclave Interior

Introduction

- The concepts of Defense in Depth, are focused on the separation of devices, ports, services, and even users into functional groups.
- The logic is simple: by isolating functional groups, the attack surface of any one group is minimized.
- The group itself can be secured using a variety of products and techniques, turning the group into a secure enclave.
- The enclave will be much more difficult to penetrate because the isolation of its services will deter attempts to scan and enumerate the enclosed network devices

Introduction

- Once defined, the enclave then needs to be secured, ideally, every enclave would be secured to the highest degree possible.
- Realistically, costs and other factors make this goal unattainable, so it is also necessary to identify those enclaves that represent the highest risk to safety and reliability, so that the strongest perimeter defenses can be implemented where they are needed the most (understanding the criticality of an enclave may be required for regulatory compliance purposes as well).

Introduction

- Perimeter defenses may consist of firewalls, Network IDS and IPS devices (**NIDS** and **NIPS**), router Access Control Lists (ACLs), application monitors, and/or similar security products.
- The enclave interior must also be secured to protect the enclave against inside attacks and/or an attack that somehow circumvents the established perimeter defenses
- Interior defenses consist primarily of host security systems, such as Anti-Virus, Anti-Malware, Host IDS (HIDS), and **application whitelisting** systems.

Identifying Functional Groups

- A “functional group” refers to anything directly involved in or responsible for a given function.
- When identifying functional groups, assess all assets (physical devices), systems (software and applications), users, protocols, and other items.
- Attempt to separate two items, such as a protocol from an asset.
- If the two can be separated without impacting either item’s primary function, they belong to two functional groups.

Identifying Functional Groups

Common functional groups to consider when building enclaves in industrial networks include :

- Control Loops
- Supervisory Controls
- Control Processes
- Control Data Storage
- Trading Communications
- Remote Access

and even less tangible groups such as:

- User groups and
- Industrial Protocol groups.

Identifying Functional Groups

- Functional groups based on network connectivity are easy to understand because networks by nature connect devices together: how the different devices are connected on the network clearly qualify those items that belong to an interconnected group and those that are excluded by a hard perimeter.

- Networks should be considered both
  - physically (what devices are connected to other devices via network cables or wireless connections) and,
  - logically (what devices share the same routable network space or subnet).

Network Connectivity – Physical

- Physical network boundaries are easy to determine using a network map.
- Ideally (although not realistically) all control system networks will have a hard physical boundary in the form of an air gap.
- Realistically, there will be interconnection points consisting of a single link, preferably through a firewall and/or other defensive devices.

Network Connectivity – Logical

- Logical network boundaries are defined by the use of routers to separate a physical network into multiple address spaces.
- The router provides a logical demarcation between each network.
- This forces all communications from one logical network to another to go through the router, where ACLs and other protective measures can be implemented.

Functional Groups – Control Loops

- A control loop consists of the devices responsible for a particular automated process.
- In most instances, a control loop will consist of a **PLC** and any related **inputs** and **outputs**.
- If an IED is a direct input or output of the control logic, those devices share a functional group with the controller; if not, they do not.
- The functional groups created **will be numerous**, and each will contain a relatively small number of devices (a specific PLC or RTU and a collection of relays and IEDs).

Functional Groups – Control Loops

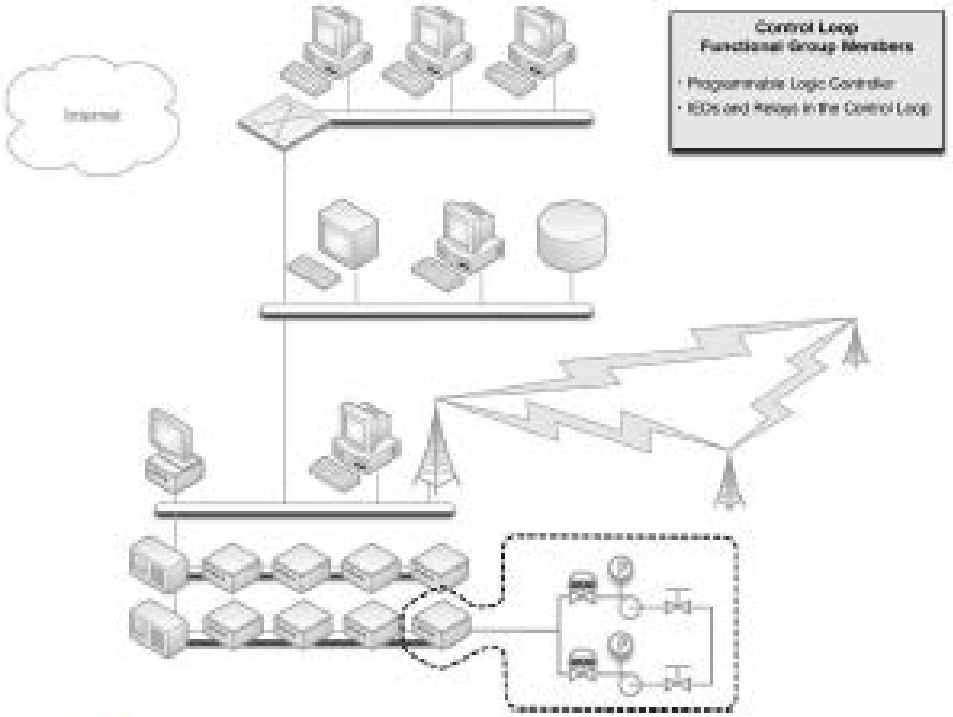

FIGURE 7.1

A Functional Group Based on a Control Loop.

Functional Groups – Supervisory Controls

- Each control loop is also connected to some sort of supervisory control—typically an HMI—that is responsible for the configuration, monitoring, and management of the automated process.
- Because the HMI is responsible for the PLC, these two devices belong to a common functional group.
- However, because the HMI is not directly responsible for those IEDs connected to the PLC, these items are not necessarily in a common functional group as the HMI.
- All PLCs controlled by the HMI are included, as are any “master” HMI or control management systems that might have responsibility or control over the initial HMI.

Functional Groups – Supervisory Controls

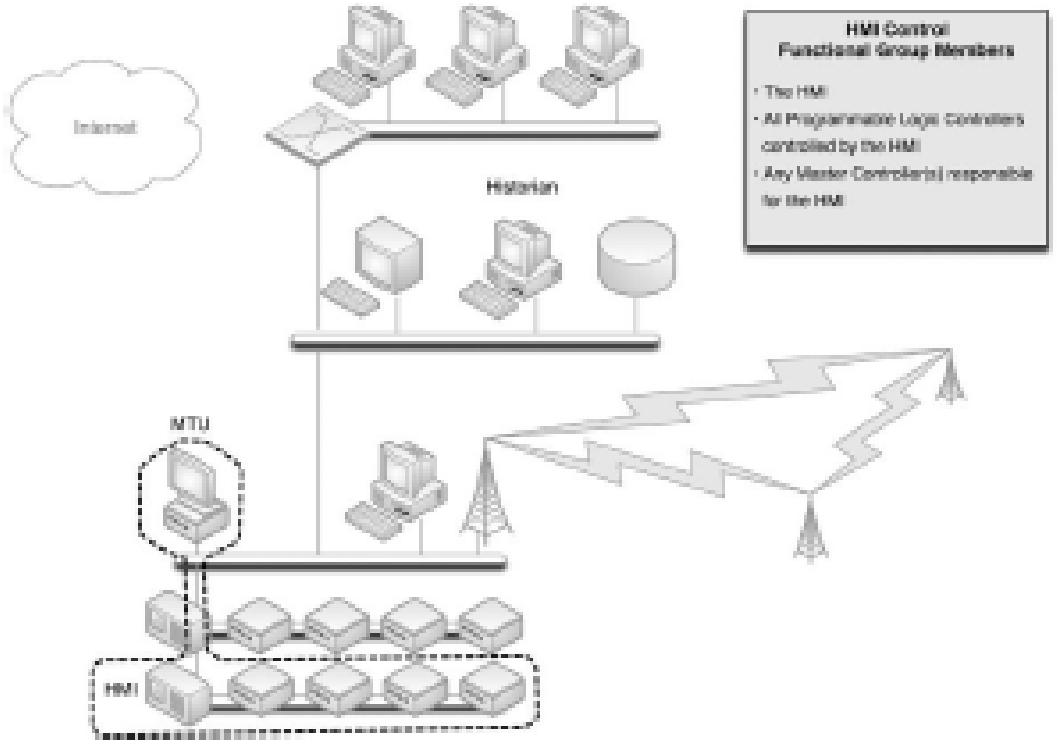

FIGURE 7.2

A Functional Group Based on an HMI.

Functional Groups – Control Process

- If a Master Controller or Master Terminal Unit (MTU) is used to manage multiple HMIs, each responsible for a specific part of a larger control process that device represents the root of yet another functional group—this time containing all relevant HMIs.
- Here we can also introduce the concept of process communication and historization.
- If an MTU interfaces with an ICCP server is present, the ICCP server should also be included in the MTU's functional group.
- Similarly, if the process information from the MTU is fed into a Data Historian, that system should also be included.

Functional Groups – Control Process

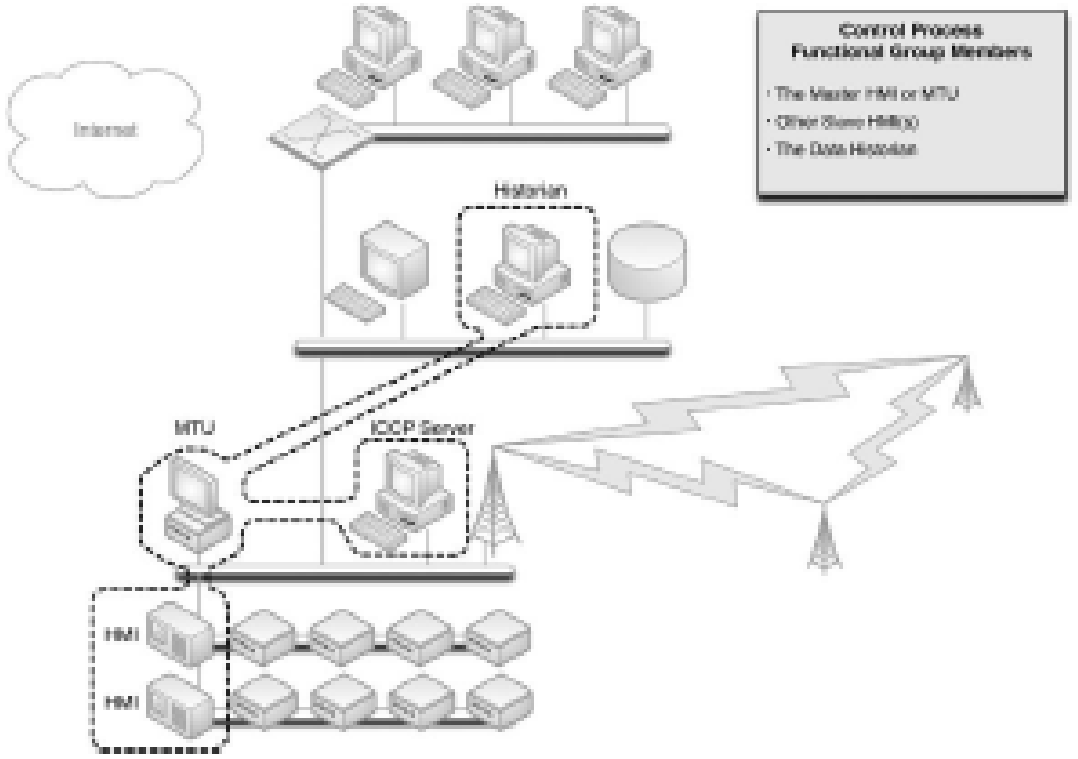

FIGURE 7.3

A Functional Group Based on a Control Process.

Functional Groups – Control Data Storage

- Many industrial automation and control system devices generate data, reflecting current configurations, the status of a process, alarms, and other information (this information is typically collected and “historized” by a Data Historian).

- The Data Historian system may connect to many—potentially all—devices throughout the control system network, supervisory network, and in some cases the business network.

Functional Groups – Control Data Storage

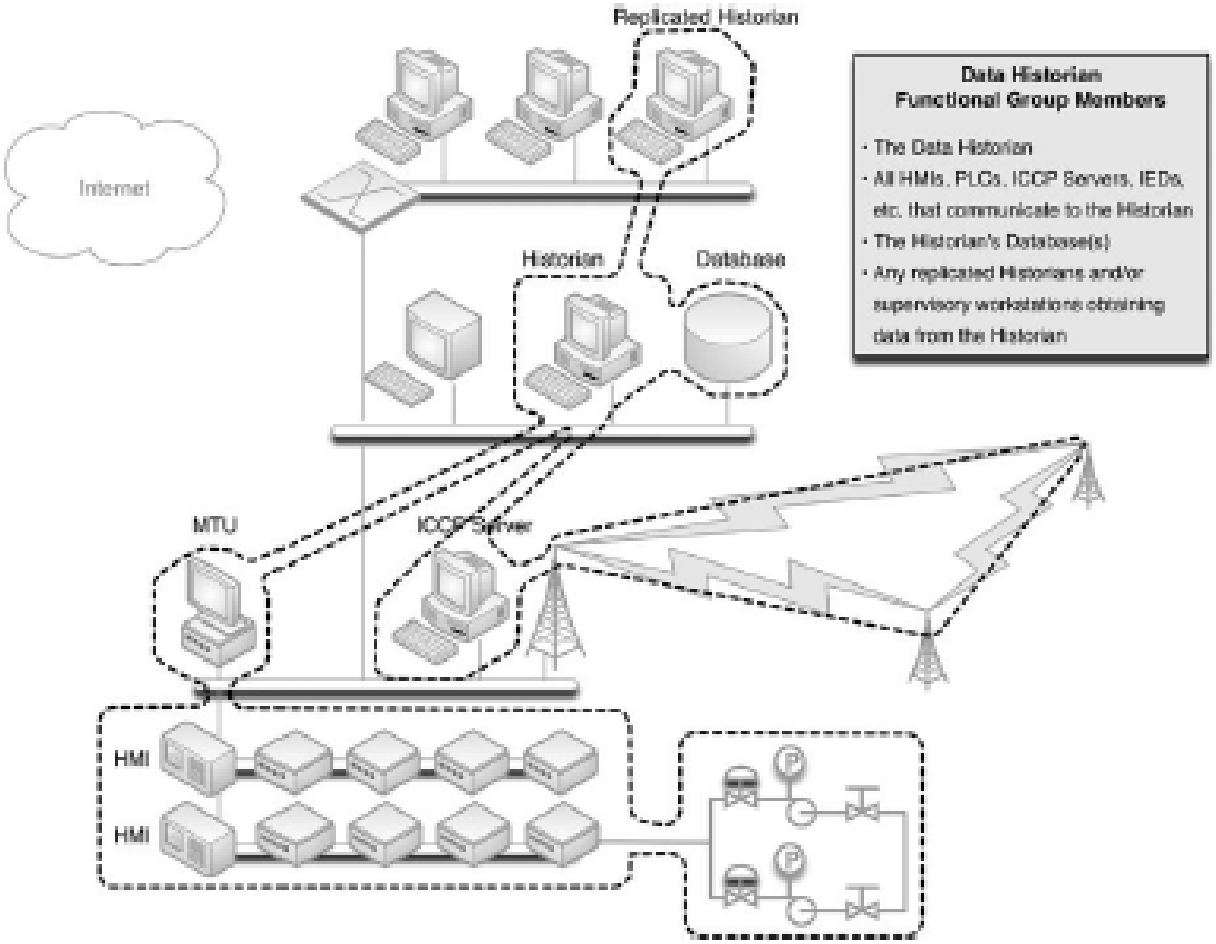

FIGURE 7.4

A Functional Group Based on Historization

Functional Groups – Trading Communication

- The need to communicate between control centers is sufficient enough to justify a specialized industrial protocol, developed specifically for that task: the Inter Control Center Communication Protocol (ICCP).
- ICCP connections require explicitly defined connections between clients and servers, and therefore, any operation utilizing ICCP to communicate with a field facility and/or a peer company will have one or more ICCP servers and one or more ICCP clients (these can be a single physical server or multiple distributed servers).
- This is an example of a functional group that extends over Wide Area Networks.

Functional Groups – Trading Communication

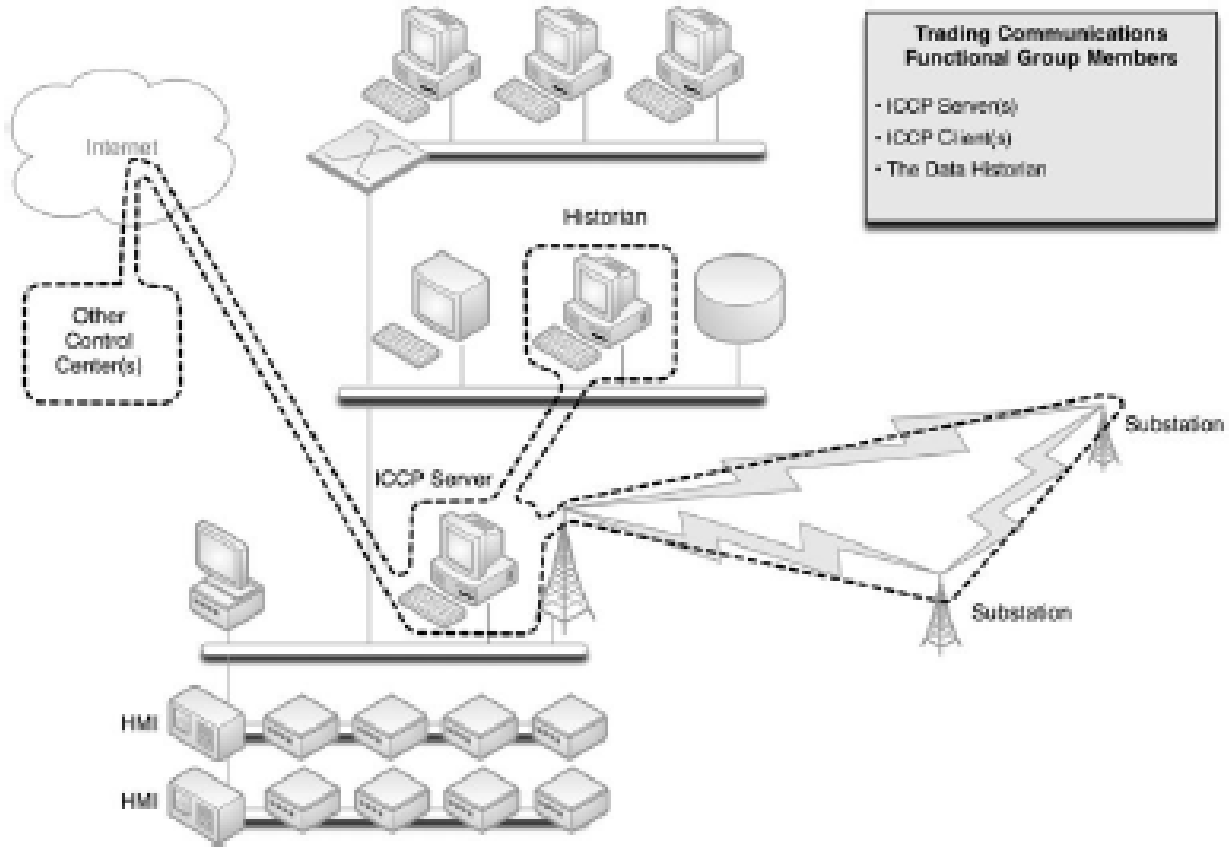

FIGURE 7.5

A Functional Group Based on the Inter Control Center Protocol for Trading Communication.

Functional Groups – Remote Access

- Many control systems and industrial devices—including HMIs, PLCs, RTUs, and even IEDs— allow remote access for technical support and diagnostics. This access could be via dial-up connection, or via a routable network connection.
- Remote access to control system devices, if it is provided, should be controlled via specialized virtual private networks (VPNs) or remote access servers (RAS), and should only allow explicitly defined, point-to-point connections from known entities, over secure and encrypted channels.

Functional Groups – Remote Access

- These explicitly defined users, the devices that they access, and any VPN or RAS systems that are used constitute a remote access functional group.
- By functionally isolating remote connections, additional security can be imposed.
- This is extremely important in order to avoid an open and inviting vector to an attacker.

Functional Groups – Remote Access

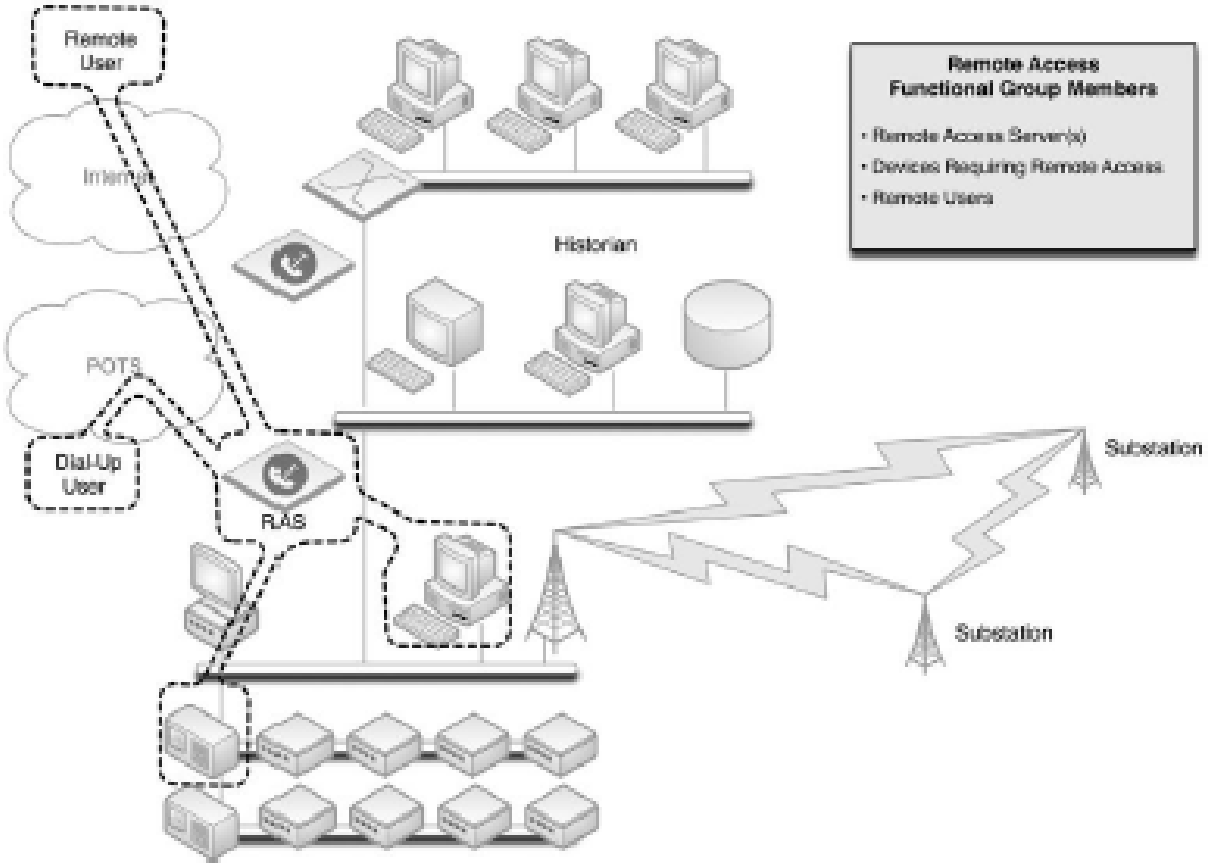

FIGURE 7.6

A Functional Group Based on Remote Access.

Functional Groups – Users and Roles

- Every system is ultimately accessed by either a user or another system. Until now, functional groups have been built around the latter: explicitly defining which devices should legitimately be communicating with other devices.
- For human interaction, such as an operator accessing an HMI to adjust a process, it is just as important to define which users should legitimately be communicating with which devices.
- This requires a degree of Identity and Authentication Management (IAM), which defines users and their roles.

Functional Groups – Users and Roles

- By placing a user in a functional group with only those devices he or she should be using, this type of activity could be easily detected and possibly prevented (remember, defining functional groups is only the first step to building a secure enclave).
- The groups must be further refined into actual enclaves, and then secured internally and at the perimeter.

Functional Groups – Users and Roles

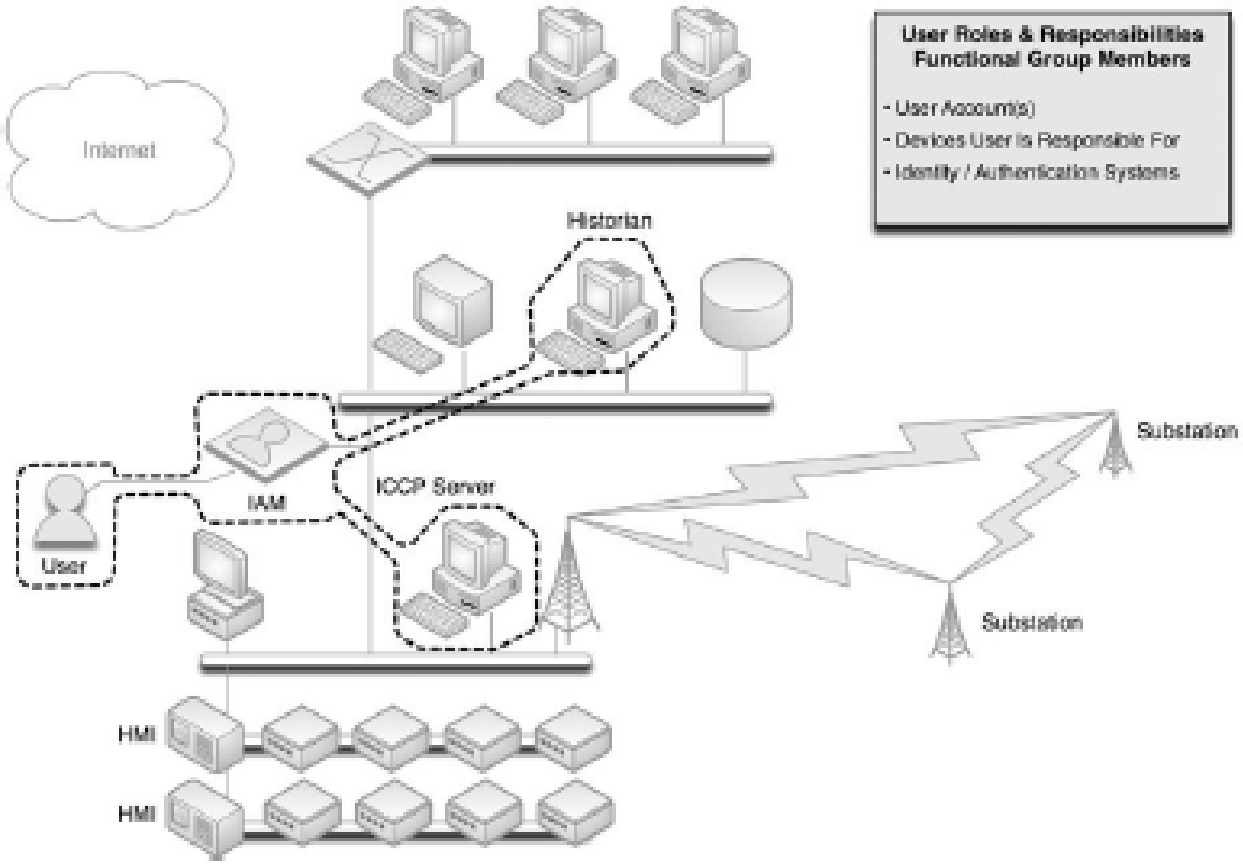

FIGURE 7.7

A Functional Group Based on Users and Roles.

Functional Groups – Protocols

- The protocols that a device uses in industrial networks can be explicitly defined, and so it should be, in order to create functional groups based on protocols.
- Only devices that are known to use DNP3 should ever use DNP3, and if any other device uses DNP3, it is a notable exception that should be detected quickly and prevented outright if possible.

Functional Groups – Protocols

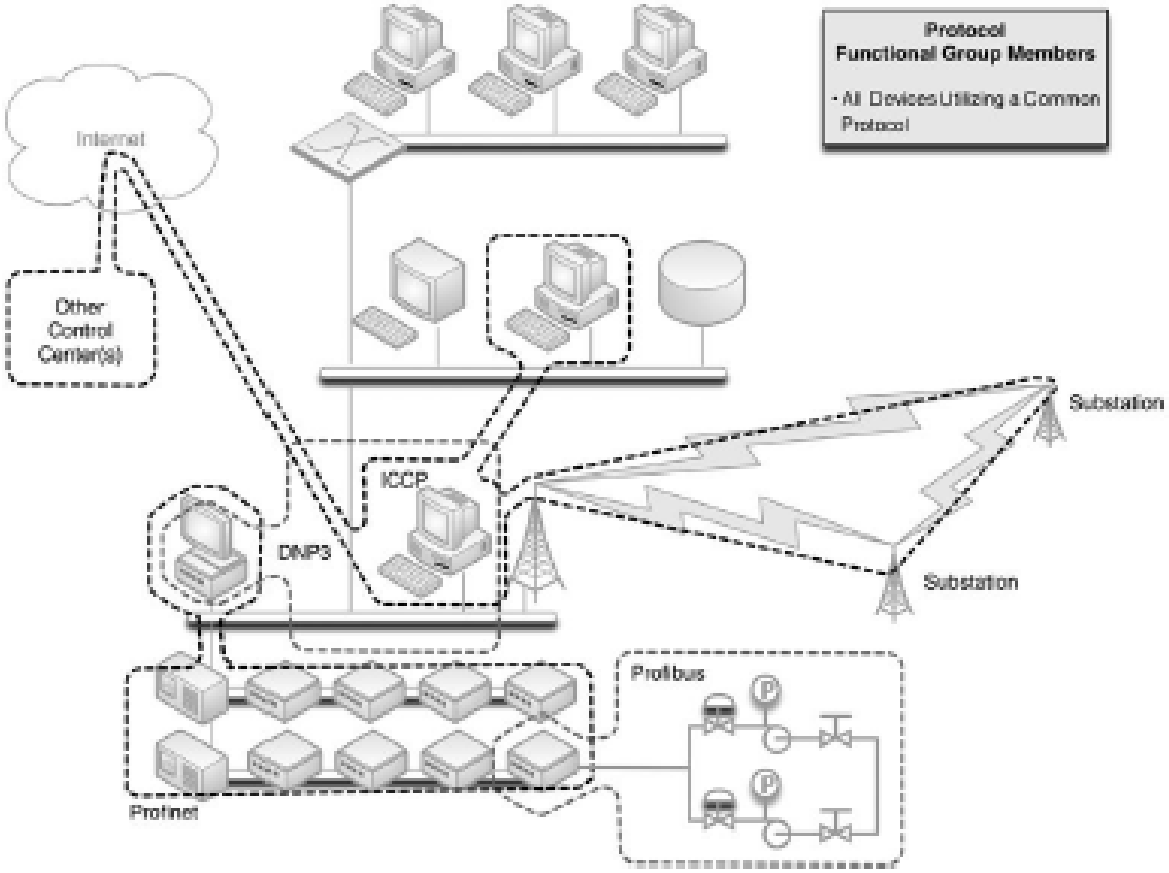

FIGURE 7.8

A Functional Group Based on Protocols.

Functional Groups – Criticality

- Enclave-based security is about isolating common influencing factors into functional groups so that they can be kept separate and secure from other non-influencing factors.
- Simply defining functional groups around criticality to identify enclaves will result in very few enclaves.
- In contrast, the more enclaves that are defined the stronger the security of the industrial network as a whole, and so
- A broader methodology—which identifies many more distinct enclaves—is preferred.

Functional Groups – Criticality

- Therefore, criticality should be assessed within the context of the previously defined functional groups.

- In this way the most critical systems will be protected by an additional layer of separation—within the inherent security of the enclave itself and then the additional protections between critical and noncritical items within that enclave.

Functional Groups – Criticality

- This will help to secure critical devices from the insider threat, such as a disgruntled employee who already has legitimate physical and logical access to the parent enclave.

- It also prevents lateral attack from one critical system to the next: if all critical systems are grouped together solely because they are all “critical,” a successful breach of one critical system puts the entire critical infrastructure at risk.

Using Functional Groups to Identify Enclaves

- Defining groups based on services, protocols, criticality, and other factors is an excellent way to eliminate unknown, unauthorized devices from a group.
- Simply, if two devices do not share a common quality, there is no way for them to communicate.
- Unfortunately, many devices support multiple protocols, applications, services, and other qualities, resulting in multiple overlapping functional groups.

Using Functional Groups to Identify Enclaves

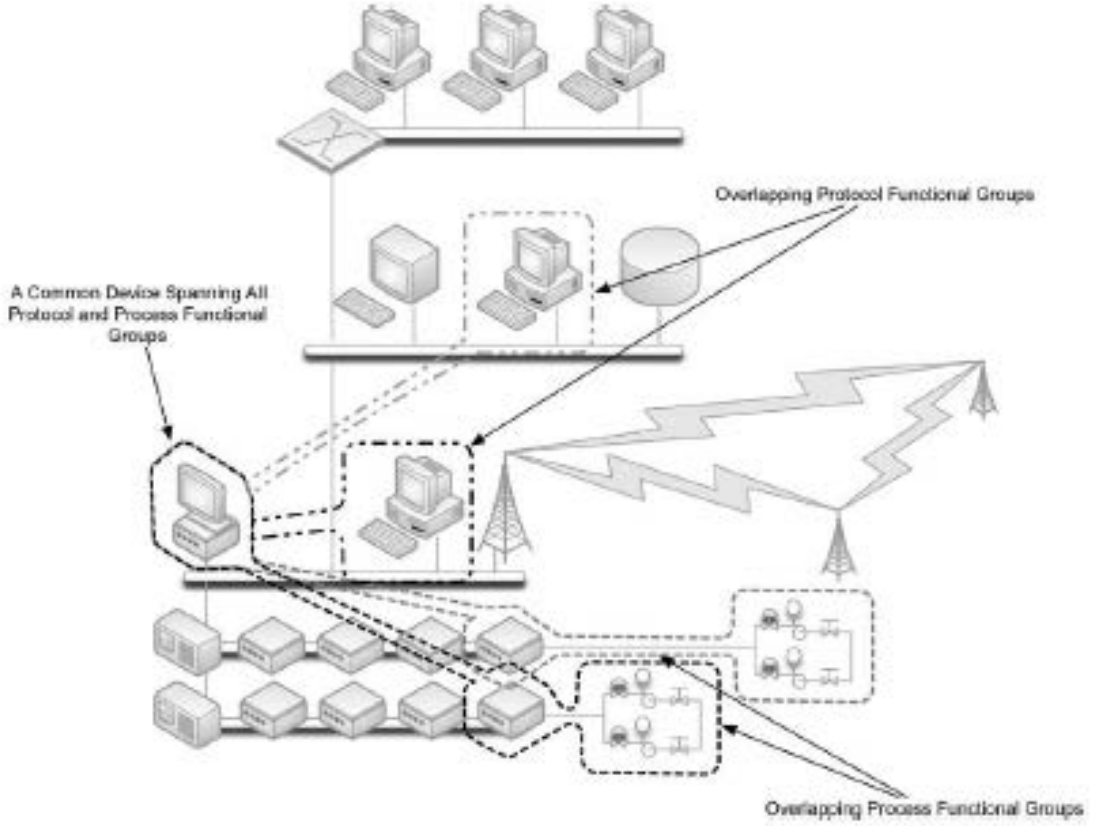

FIGURE 7.10

Overlapping Functional Groups.

Using Functional Groups to Identify Enclaves

- Ideally, every functional group would contain a clear demarcation from every other group, and each demarcation would be secured using a unique protective device.
- In many cases it is necessary to simplify the functional groups using a common quality shared between groups, effectively combining overlapping functional groups into a single, larger enclave.
- The process of distilling the many functional groups into manageable ones will result in several defined security enclaves, with a clear understanding of the boundaries of that enclave, and the users, devices, and protocols that are contained within.

ESTABLISHING ENCLAVES

- Once the process of pairing down the dozens of functional groups has been completed and the groups have been consolidated where necessary into larger overlapping groups, the enclaves can be established. Logically, the enclaves have already been defined at this point, with each consolidation of functional groups equating to a single security enclave.

The process of establishing enclaves can be summarized as follows:

1. Identifying the boundaries of each enclave so that perimeter defenses can be deployed in the correct location.
2. Making any necessary changes to the network so that the network architecture aligns with the defined enclaves.
3. Documenting the enclave for purposes of policy development and enforcement.
4. Documenting the enclave for purposes of security device configuration.

Perimeter Defense

- Once an enclave is identified, it must be mapped to the network so that clear electronic perimeters can be defined.
- It is a necessary process that should be performed for any industrial network regardless of regulatory concerns, as an enclave can only be secured if there are defined and control entry points.
- In many cases the demarcation of the enclave will be very clear; for example, there may be a single network connection between a control center's supervisory LAN and the control system network.
- In some instances, multiple connections might exist; all network connections into or out of an enclave comprise that enclave's electronic perimeter.

Perimeter Defense

- In some instances a single enclave may consist of multiple, geographically or otherwise separated groups, the enclave is still considered to be a single enclave.
- If there are any network connections between separated locations, they should be held to the same controls as the rest of the enclaves.
- There should be no communications across those links that do not originate and terminate within the enclave, and **if outside communication is required, it must occur through defined and secure access points.**
- A common method **of interconnecting distributed enclaves** is the use of a dedicated **VPN or other encrypted gateway**, while for extremely critical enclaves, a dedicated network connection or fiber cable may be used so that **physical separation** is maintained.

Perimeter Defense

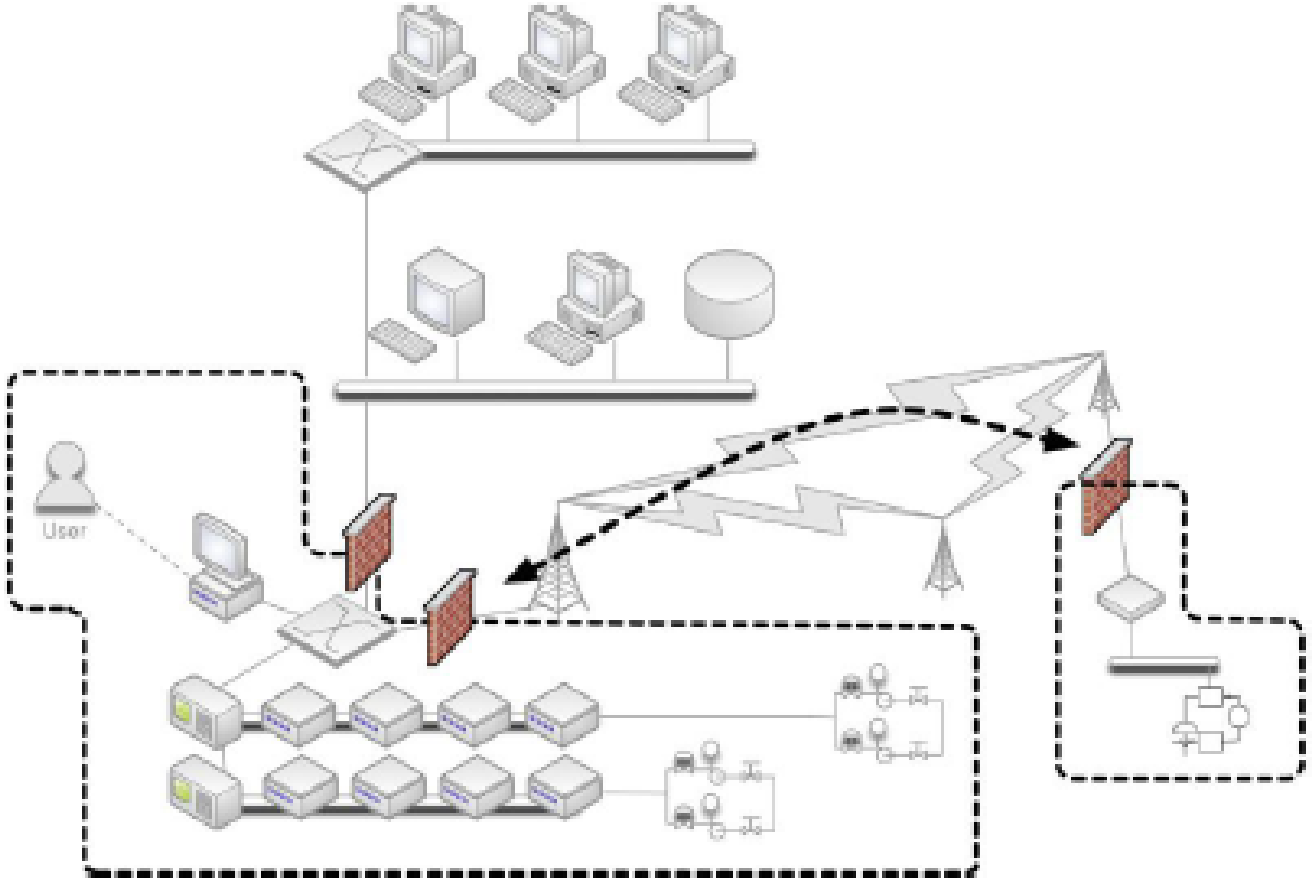

FIGURE 7.12

A Geographically Split Enclave.

Perimeter Defense

- The goal is that each enclave be isolated as strictly as possible, with as few connections as possible between that enclave and any other directly adjacent (or surrounding) enclave.
- By providing a single access point in and out of an enclave, that point can be secured using a perimeter security device such as a firewall or IPS.
- In the event of a single enclave that is split (geographically or by another enclave), inter-enclave communication can still be allowed: in this case through the use of perimeter firewalls, which effectively enforce a point-to-point route between the split enclaves (this path should also be encrypted).

Perimeter Defense

To establish an Electronic Security Perimeter (ESP) and effectively secure inbound and outbound traffic, two things must occur:

1. All inbound and outbound traffic must be forced through one or more known network connections that can be monitored and controlled.
2. One or more security devices must be placed in-line at each of these connections.

For each enclave, appropriate security devices should be selected and implemented using the recommendations below. **Typically, the criticality of the enclave dictates the degree of security that is required.**

Perimeter Defense

Table 7.1 Perimeter Security Requirements by Criticality

Criticality	Required Security	Recommended Enhancements
4 (highest)	NRC CFR 73.54: Unidirectional Perimeter, NERC CIP 005: Firewall or IDS or IPS	Application layer monitoring, Firewall, IDS and IPS
3	NRC CFR 73.54: Unidirectional Perimeter, NERC CIP 005: Firewall or IDS or IPS	Application layer monitoring, Firewall, IDS and IPS
2	NERC CIP 005: Firewall or IDS or IPS	Firewall and IDS and IPS
1	NERC CIP 005: Firewall or IDS or IPS	Firewall and IPS
0 (lowest)	NERC CIP 005: Firewall or IDS or IPS	Firewall and IPS

Perimeter Defense

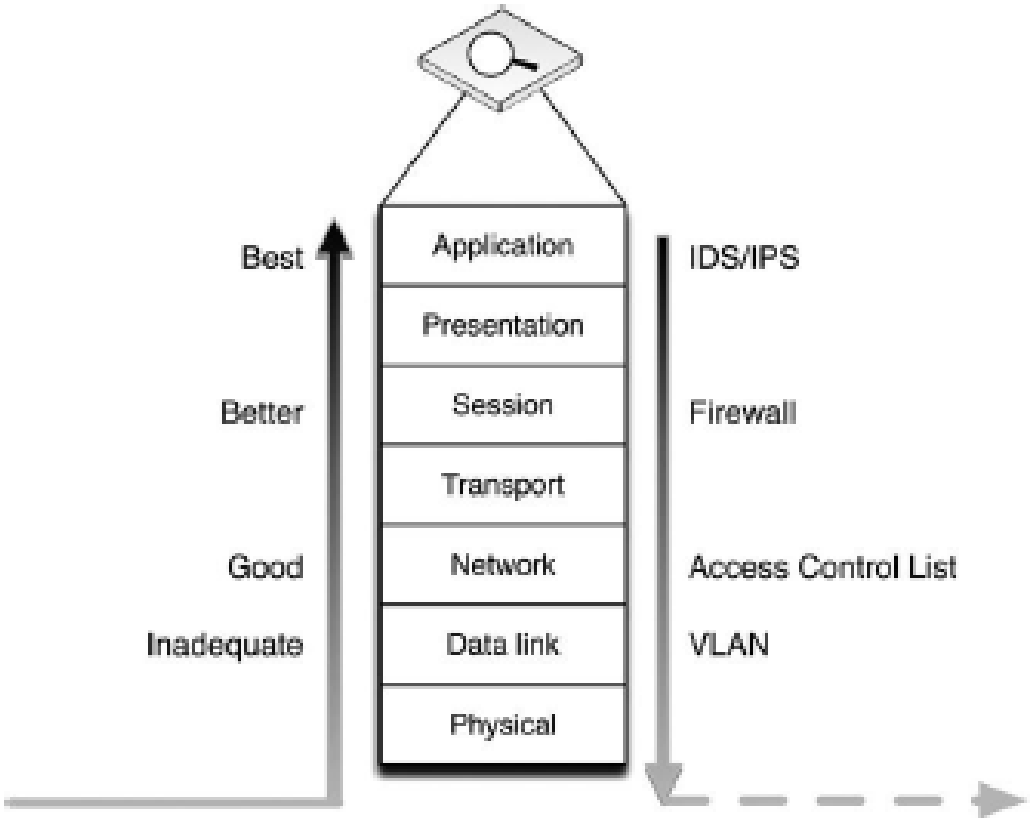

FIGURE 7.14

Relative Capabilities of Common Security Devices.

Perimeter Defense

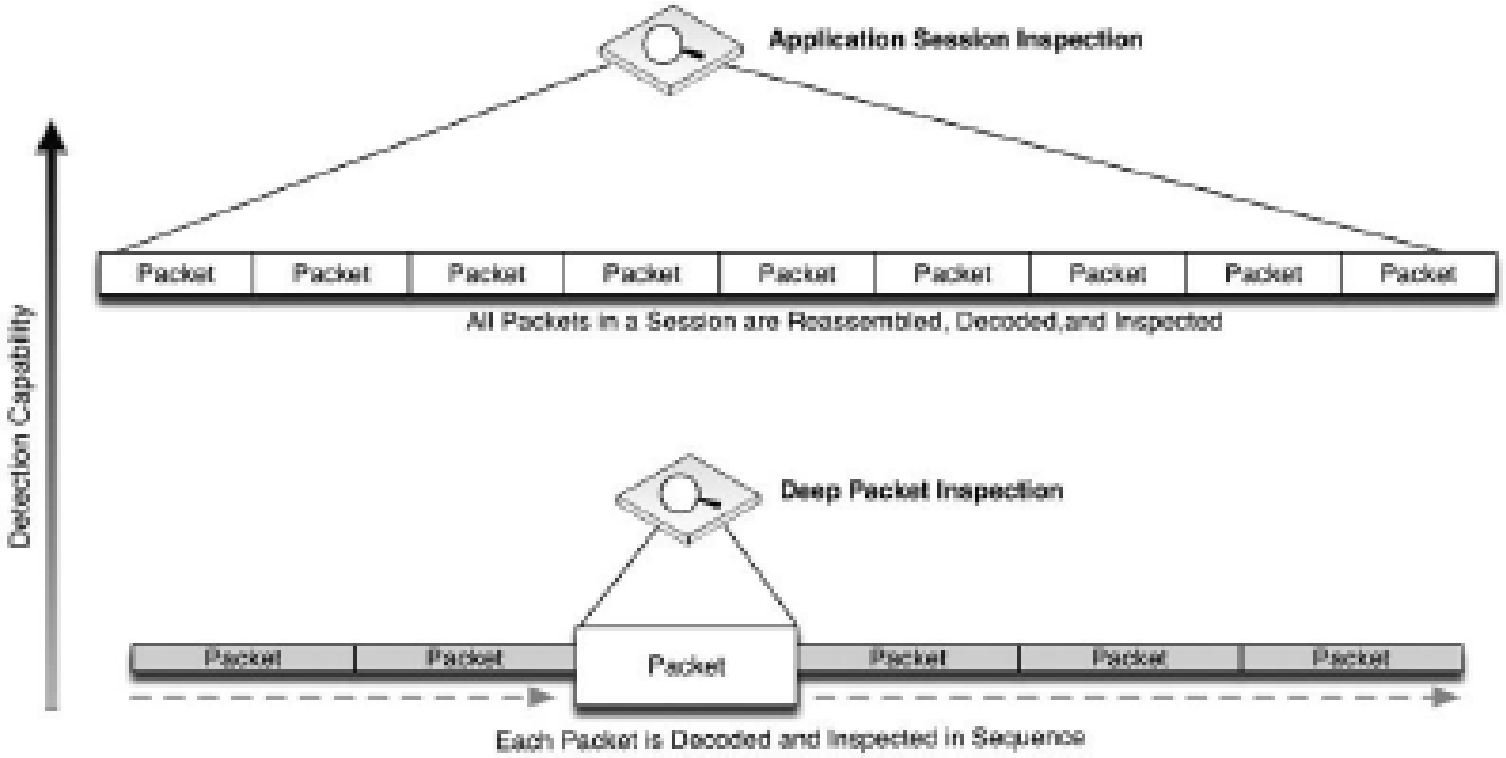

FIGURE 7.15

Application Session Inspection vs. Deep Packet Inspection.