Functional Analysis Methods:
A Case Study in Nuclear Power

Brad Yeates- Southern Company
Matt Gibson – Progress Energy

May 2011 ICSJWG- Dallas

Introduction

- We will present insights into using functional analysis to establish a cyber security design aligned with operational goals by establishing a reasonable basis and obtaining management buy-in.

- We will present concepts with a practical case-study integrated throughout the presentation.

Engineering Engagement

Concept

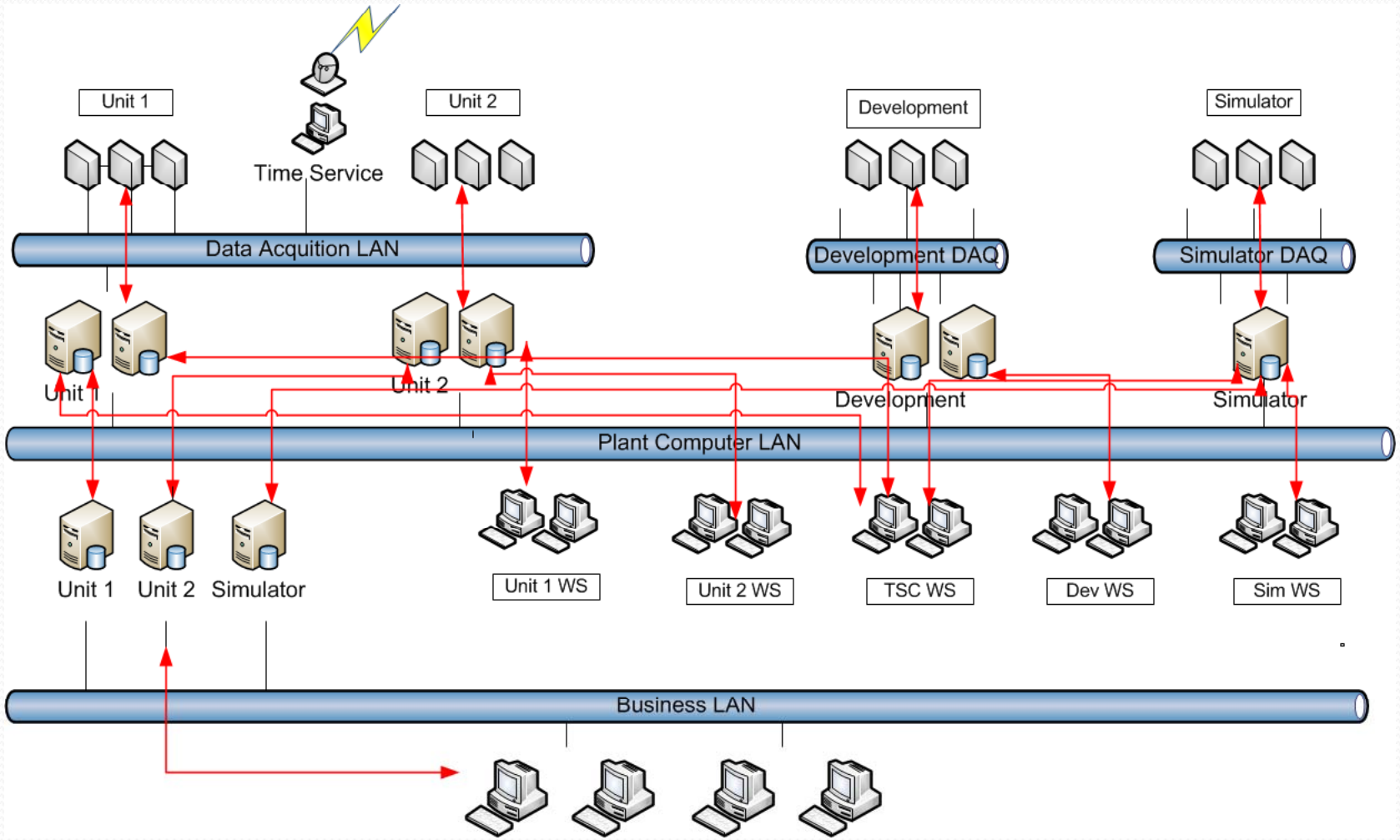
- Engage the Architect- Engineer, Vendors, and in-house engineering at the conceptual phase.
  - Develop Security Architecture Goals
  - Use functional analysis to shape and validate goals
  - Develop System Design Input based on those goals
  - Apply at the Plant and System level

Case Study

- Based on an actual Plant Computer replacement at a nuclear power facility.
- The vendor was cooperative and motivated to enhance their cyber security.
- The Cyber enhancement came after the conceptual design phase and procurement specifications were contracted.
- The Project Manager was less cooperative and highly sensitive to anything that increased costs or challenged the schedule.

Original Flat LAN Concept

Case Study



Top Down Approach

Concept

- Establish System Functions
  - Use Human Factors Engineering(HFE) and Business Process Analysis techniques
  - Consider the System Functional Granularity
  - Evaluate Data flows
  - Match Architecture features to Security controls and Vulnerability mitigation.
  - Write it down in specifications or criteria documents

Security Architecture Planning Goals

Concept

- **Integrity** –Ensures that information and control are unmodified, accurate and correct.
- **Availability**- Ensures that information and Controls are usable on demand.
- **Confidentiality**- Ensures that information and controls is available to authorized individuals only

HFE and Business Process Analysis

Concept

Human Factors Engineering and Business Process Analysis(BPA) can be applied to Security Architectures

- BPA
  - Why am I doing a certain task? What's the business reason and importance? Include the “Cyber Security “ burden.
- Task Analysis-
  - Evaluate how Functions are Accomplished. What are the inputs and output? How can they be secured?
- Functional Allocation
  - Based on task analysis, allocate functions to specific systems and subsystems and then to security controls. Produces a granularity and drives segmentation and technical controls inheritance

Goals for Cyber Enhancement

Case Study

- Isolate Control Room Functionality: Any external failure does not have an adverse impact to operator indications.
- Intrusion Prevention & Detection: Provide network and host level intrusion prevention and detection.
- Data Diode Ready: Change Info Server protocol to be a true one-way data flow that is Data Diode ready.
- Malware Protection: Protect from malware, including zero-day attacks, without performance degrading virus scans.
- Device Control: Prohibit unauthorized devices and media from connecting to any equipment.
- Support Effective Configuration Change Control: Provide a mechanism to facilitate Separation-of-duties when making changes to the, hardware, executable code and device connections.
- Regulatory Compliance: Implement a foundation that will allow the full implementation NEI 08-09 controls without a major design change.

Segment Control Objectives

Concept

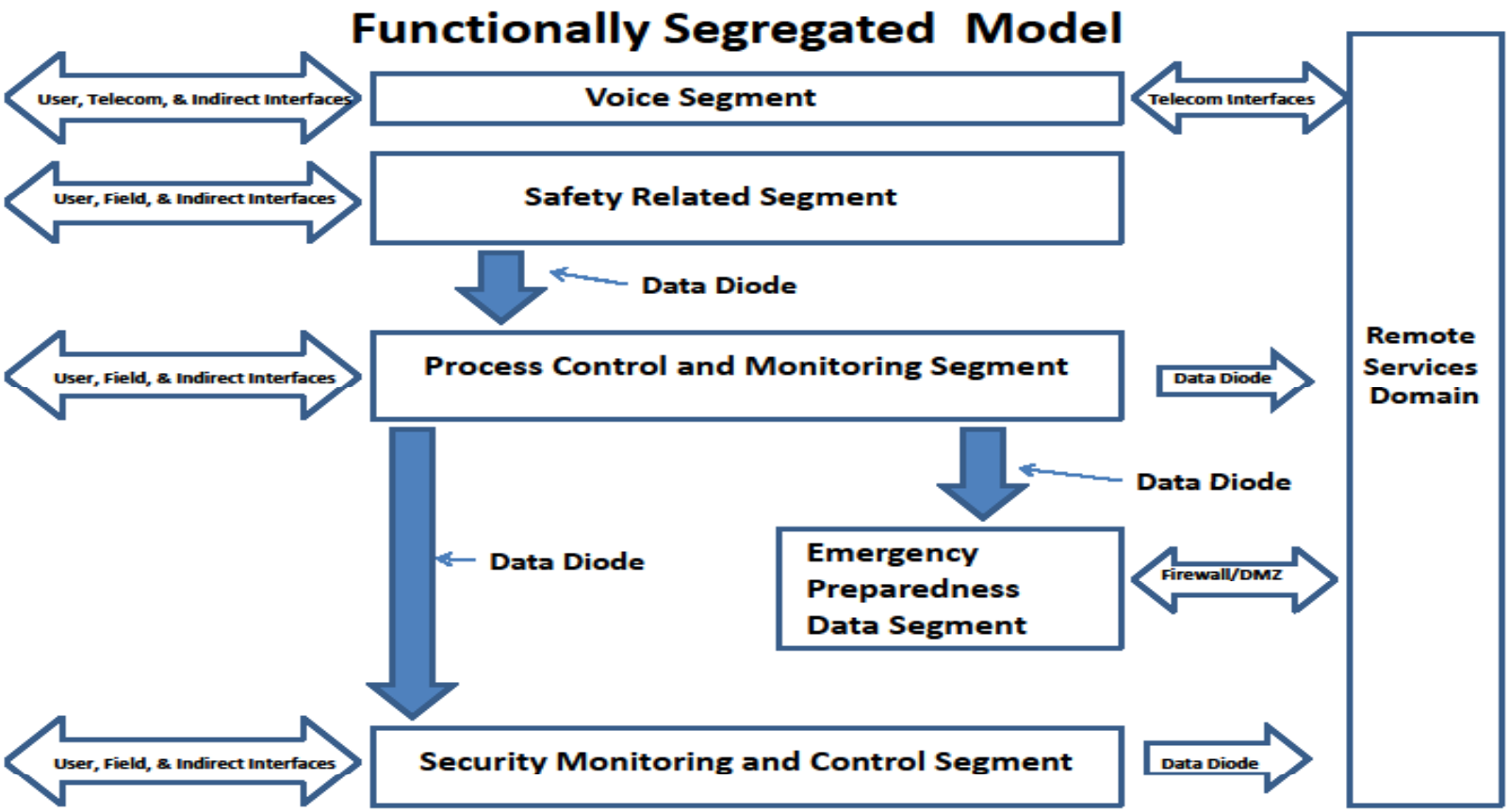
- Static configurations are desirable
  - Eliminate ad-hoc connections
  - Unused connections disabled
  - Used connections monitored and permanently connected.
  - Static IP addresses and manual ARP tables.
  - Use Deterministic traffic shapes.
  - Whitelisting for malware detection, device control, and configurations control.

Security Architecture Design

Concept

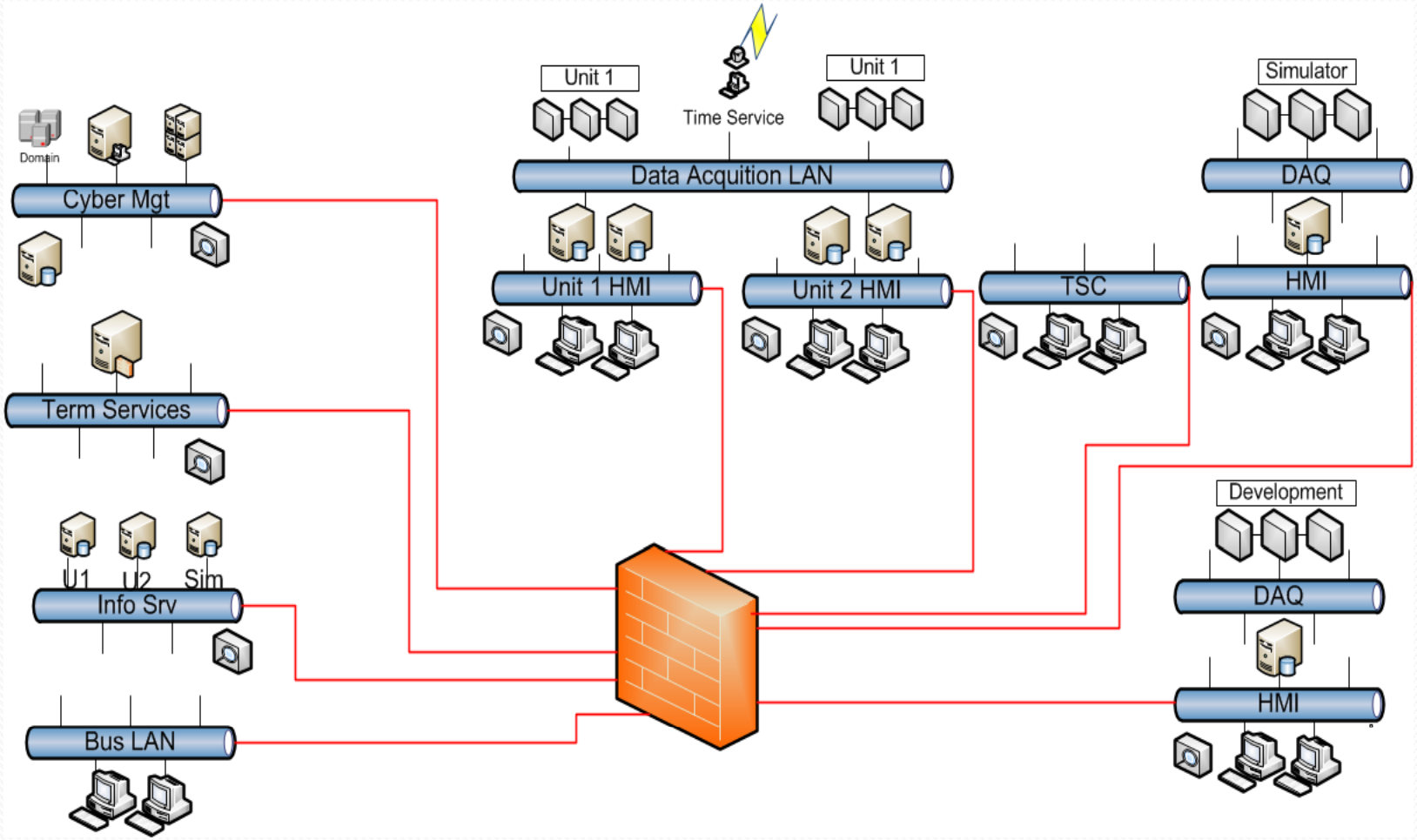
- Using the results of Functional Allocation establish Design Input
- Segment the system or plant based on the functional allocation.
- Establish the Segment boundary interface requirements.
  - Segments can be completely segregated.
- Allocate segments to specific security levels
- Establish the needed security controls within segments. Include Common controls and controls inheritance.

Functional Segmentation Concept



Functionally Segmented Network

Case Study



Configuration Change Control

Case Study

- All network switches are locked and un-used ports are disabled. Any network changes require cyber administrator authorization.
- All new devices require cyber administrator authorization
- All changes to executable code require cyber administrator authorization
- This provides effective separation-of-duties to authorize changes, beyond normal work-order configuration controls.

Segment Control Objectives (cont.)

Concept

- Use deterministic interfaces and monitoring techniques where possible
  - Where possible, use Unidirectional Gateways for deterministic data flow.
  - Use ingress and egress Firewall rules with static ports, addresses, and protocols.
  - Non-IP interfaces when they provide isolation
  - Choose well bounded network traffic to improve IDS performance.

Data Diode Ready

Case Study

- Modified the protocol that facilitates traffic flow to each Information Server.
  - Changed from a TCP connection to a UDP data stream. (Connection vs. connectionless.)
  - Changed Information Server end to listen for data, instead of initiating a connection.
  - Changed Plant Computer to initiate and stream a data flow.
  - Implemented in-stream data integrity checks and packet numbering to allow identification of data errors.
  - Alarm function changed to the Information Server side if data flow is interrupted.

Malware Protection

Case Study

- Utilized commercial whitelisting / application control technology
- Enforced with ring zero driver that loads 1st on every server and workstation and cannot be removed, except by an authorized administrator.
- The administrator creates a cryptographic Hash of every executable and limits execution to specific users and machines using "policies" that are embedded in the ring zero driver.
- Provides deterministic protection from malware, including "zero-day" threats.
- Provides undetectable performance overhead that is not susceptible to debilitating virus scan activities.
- Does not require an outside connection to obtain current virus signatures.

Intrusion Prevention & Detection

Case Study

- Specific rules on the firewall allow authorized connections between LAN segments and block/alarm unauthorized connections.
- Deep packet inspection technologies on the firewall block/alarm unauthorized packets from transitioning LAN segments, even if they are contained in an authorized connection.
- Network sensors are installed on each LAN segment to perform deep packet inspection and alarm on any unauthorized intra-segment traffic. (Out-of-band connection not shown on drawing.)
- Advanced analytic capabilities in the cyber-management segment are used to profile authorized traffic and alarm on anomalous traffic.
- Application and Device Control block and alarm on any unauthorized executable code and device connections.

Segment Control Objectives (cont.)

Concept

- Leverage Physical Security controls
  - Align network segments to physical security boundaries when possible.
    - Protected Area
    - Vital Area
    - Security zones
    - Owner Controlled Area
  - Utilize tampers alarms and alternate controls. Required on most Security CDA's

Device Control

Case Study

- This includes all external devices such as USB devices, Modems, printers, etc; Media such as CD-ROM/ DVD disks, and internal devices such as disk controllers etc.
- Uses the same driver and policy enforcement engine as described above in the Whitelisting / Application control.
- All device connections are specifically authorized by vendor device code and serial number.
- Devices are authorized to specific users and are limited to specific machines.
- Any unauthorized connections are blocked and alarmed.
- Authorized connections are logged.

Questions

?