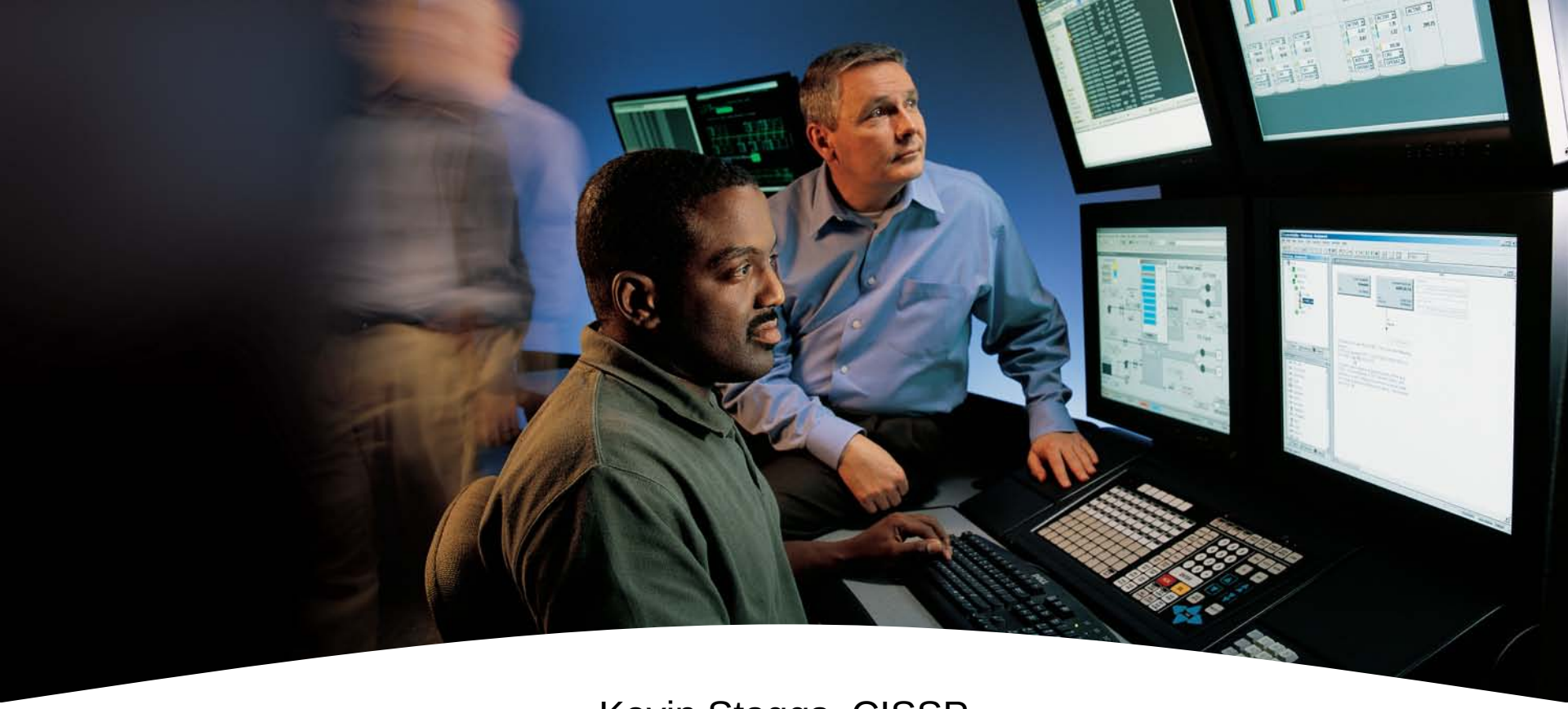


Kevin Staggs, CISSP

Designing Robust, Secure Industrial Automation and Control Systems

Honeywell

Agenda

- Migration of Industrial Automation and Control Systems from proprietary to open systems based and the challenges
- Industry response
- Introduction to ISA99 Security Standards for IACS
- Discussion

Very Brief History of IACS

- Computer based control systems – 60’s
  - Central computer, dumb terminals, serial communications
- Distributed HMI and control systems – mid 70’s
  - Microprocessor based controllers
  - Proprietary closed redundant network
- Distributed control systems – early 80’s
  - Proprietary closed redundant networks
- Open system based systems – early 90’s
  - Linux first, then Windows
  - Adoption of Ethernet for communications

Security attributes of proprietary systems

- Availability
  - Done through redundancy
- Integrity
  - Most done through obscurity of proprietary nature of the system
  - Communications integrity in proprietary network designs
- Confidentiality
  - None
- Authentication
  - Employed by the company
- Authorization
  - Access to the control room and physical keylock on system
- Auditing
  - None

Move to open systems

- Little understanding of the IT industry by both vendors and process engineers
  - Benefits of open systems well understood
  - Minimal understanding of the concept of Least Privilege
  - Risks of open systems not understood
- Significant benefits from open systems
  - Many manufacturing operations are comprised of many different systems that have to all work together
  - Allowed integration of data from multiple systems – OPC Standard
- Creation of very complex systems of systems with very little systems analysis

So what happened?

- Little understanding of the IT industry by both vendors and process engineers
  - Benefits of open systems well understood
  - Risks of open systems not understood
  - IT protection mechanisms not implemented
- Process roles were not integrated into the systems
- Significant benefits from open systems
  - Many manufacturing operations are comprised of many different systems that have to all work together
  - Allowed integration of data from multiple systems – OPC Standard
- Creation of very complex systems of systems with very little systems analysis

So what happened?

- 2000 - Maroochy Shire Sewage Spill
- 2003 – Slammer worm impacts multiple control systems
- 2005 – Zotob worm shuts down 13 auto plants
- 2006 – Browns Ferry nuclear power plant shut down due to excessive network traffic
- 2008 – Hatch nuclear power plant shut down due to update of enterprise system
- 2010 – Stuxnet suspected to be a directed attack on specific SCADA system

NERC top 10 vulnerabilities

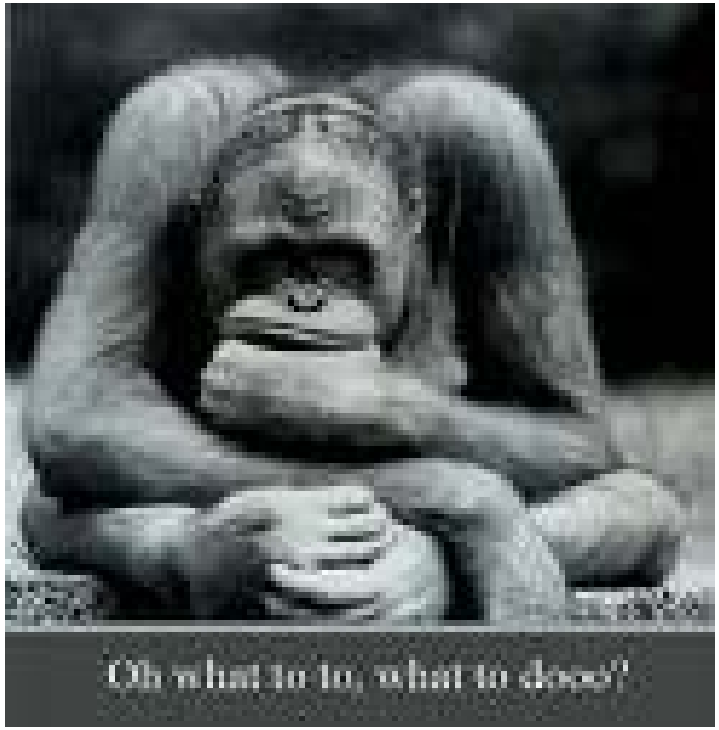
- *“Inadequately managed, designed, or implemented critical support infrastructure”*
- *“Control systems command and control data not authenticated.”*
- *“Unauthorized or inappropriate applications or devices on control system networks.”*
- *“Insufficient application of tools to detect and report on anomalous or inappropriate activity.”*
- *“Use of a non-dedicated communications channel for command and control and/or inappropriate use of control system network bandwidth for non-control purposes.”*

NERC top 10 vulnerabilities – last 5

- *“Use of inadequately secured wireless communication for control.”*
- *“System administration mechanisms and software used in control systems are not adequately scrutinized or maintained.”*
- *“Remote access to the control system without appropriate access control.”*
- *“Inadequately designed control system networks that lack sufficient defense-in-depth mechanisms.”*
- *“Inadequate policies, procedures, and culture that govern control system security.”*

Industry response has been multiple answers

- NERC CIP
- Chemical Sector Guidance Documents
- NIST 800-53
- NIST 800-82
- ANSI/ISA-TR99.00.01-2007
- ANSI/ISA-99.00.01-2007
- ANSI/ISA-99.02.01 -2009



Lots to pick from, but are they right?

Industry thought leaders formed ISA99

The ISA99 Committee addresses industrial automation and control systems whose compromise could result in any or all of the following situations:

- endangerment of public or employee safety
- loss of public confidence
- violation of regulatory requirements
- loss of proprietary or confidential information
- economic loss
- impact on entity, local, state, or national security

ISA99 participation

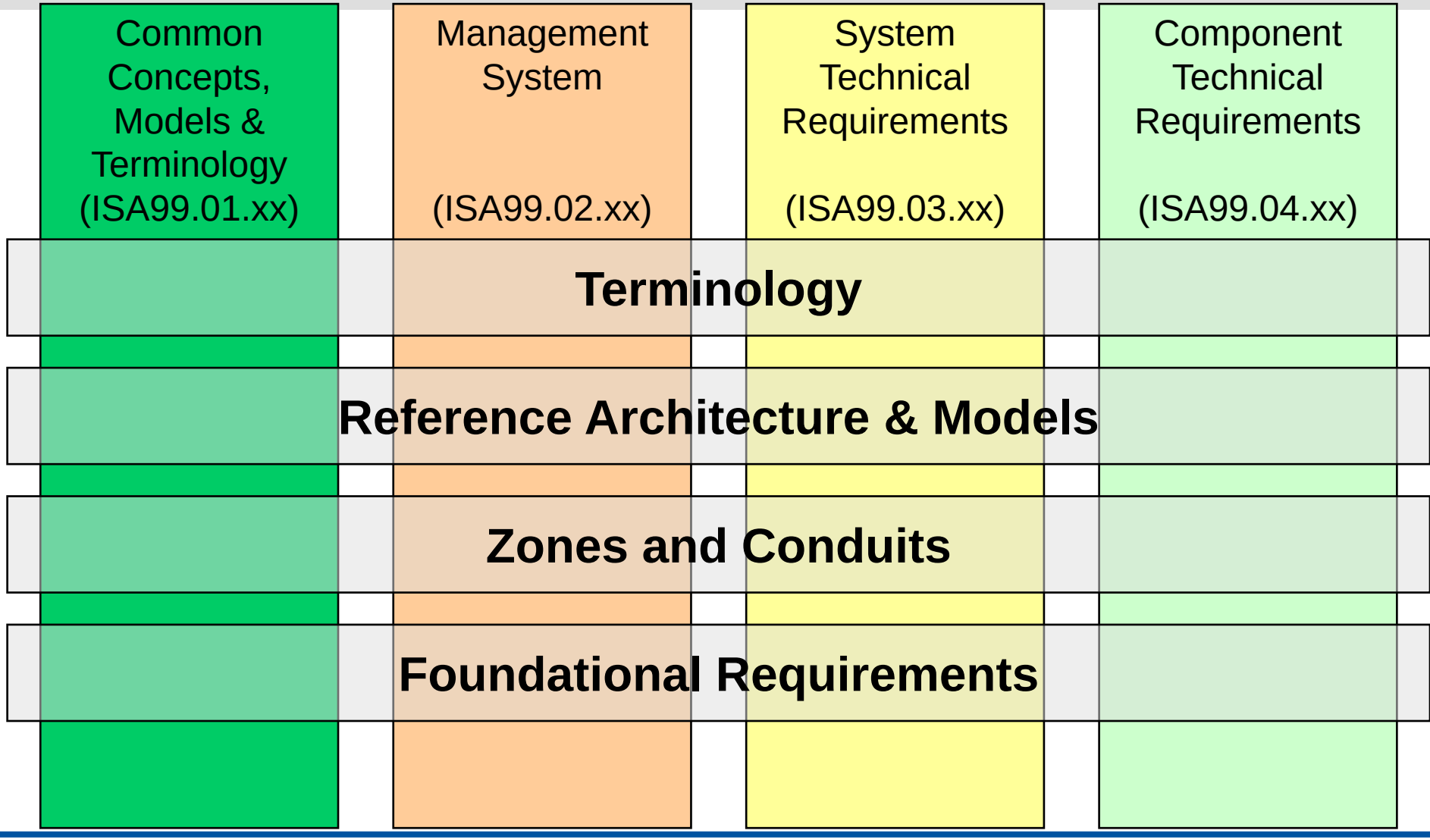
- Over 250 members from more than 200 companies
- Sectors include:
  - Chemical Processing
  - Petroleum Refining
  - Food and Beverage
  - Power
  - Pharmaceuticals
  - Process Automation Suppliers
  - IT Suppliers
  - Government Labs
  - Consultants

Work Product Types (*)

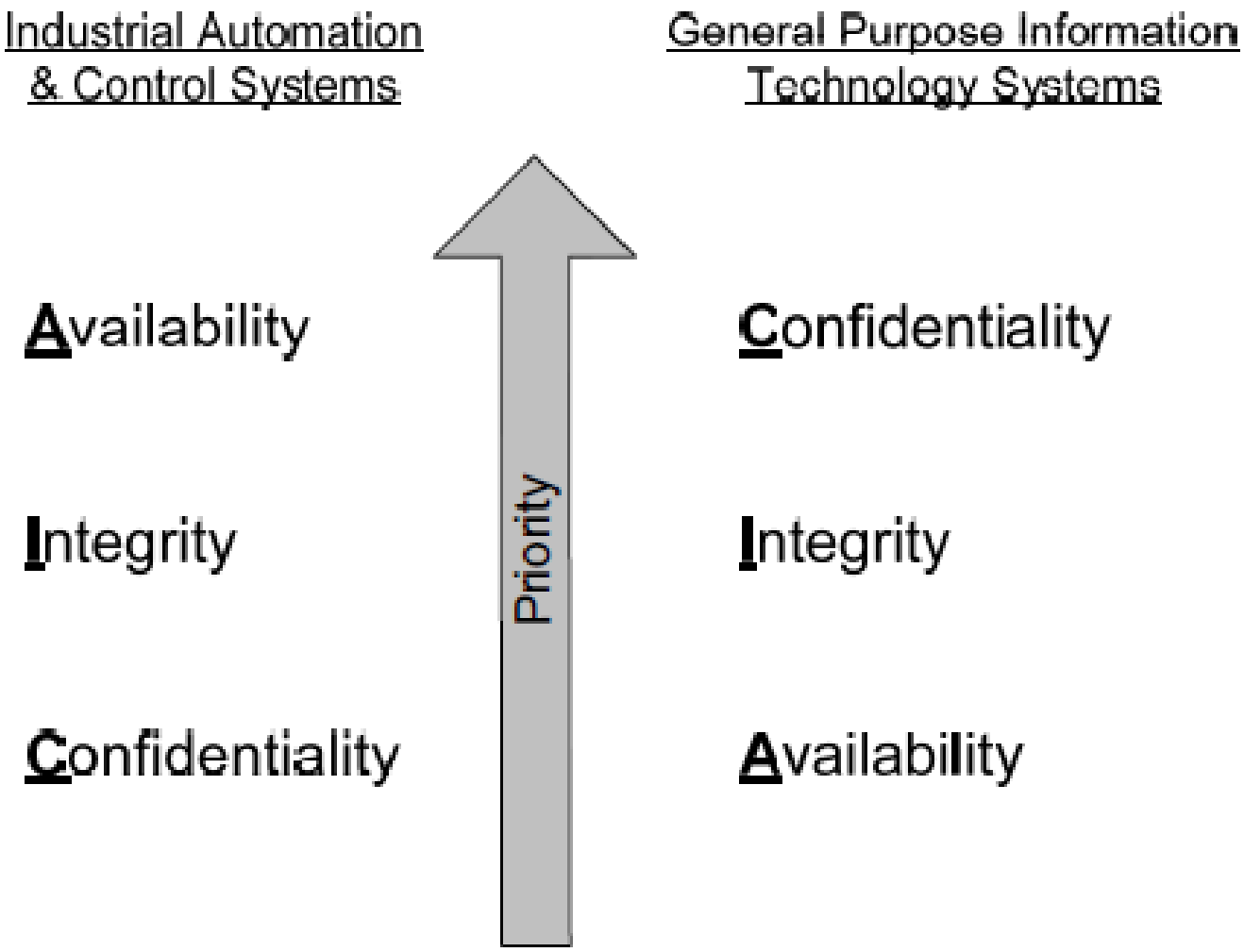
- STANDARD: A document that embodies requirements (normative material) that, if not followed, could directly affect safety, interchangeability, performance, or test results. In general, such requirements should already be widely recognized and used. Standards also include Draft Standards for Trial Use (DSTU), which are draft standards intended for subsequent submittal to ANSI for approval as American National Standards. A standard may contain informative material as long as it is clearly identified as such.
- RECOMMENDED PRACTICE: A document that embodies recommendations (informative material) that are likely to change because of technological progress or user experience, or which must often be modified in use to accommodate specific needs or problems of the user of the document.
- TECHNICAL REPORT: A document that embodies informative material. For example, reports of technical research, tutorials, and factual data obtained from a survey, or information on the "state-of-the-art" in relation to standards on a particular subject.

(*) – From ISA Standards and Practices Department Procedures

Common Topics Across Standards…



CIA objectives of an IACS



Foundational security requirements

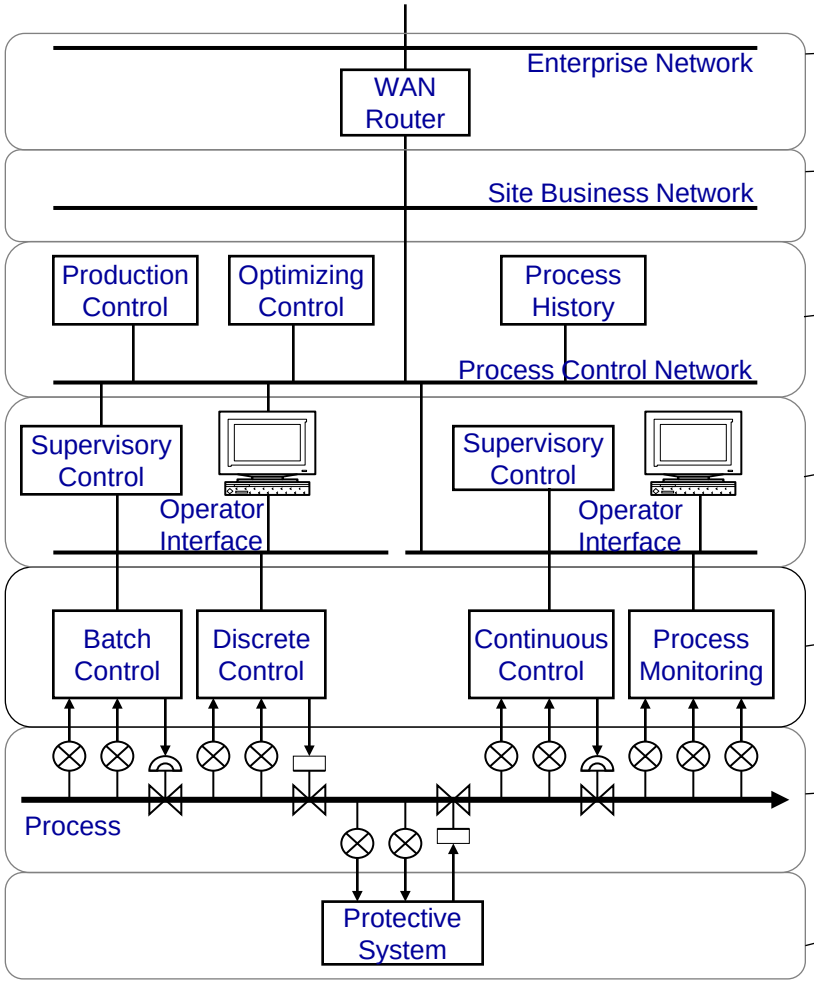
- **Access Control (AC)**
  - Control access to selected devices, information or both to protect against unauthorized interrogation of the device or information.
- **Use Control (UC)**
  - Control use of selected devices, information or both to protect against unauthorized operation of the device or use of information.
- **Data Integrity (DI)**
  - Ensure the integrity of data on selected communication channels to protect against unauthorized changes.
- **Data Confidentiality (DC)**
  - Ensure the confidentiality of data on selected communication channels to protect against eavesdropping.

Foundational security requirements

- **Restrict Data Flow (RDF)**
  - Restrict the flow of data on communication channels to protect against the publication of information to unauthorized sources.
- **Timely Response to Event (TRE)**
  - Respond to security violations by notifying the properauthority, reporting needed forensic evidence of the violation, and automatically taking timely corrective action in mission critical or safety critical situations.
- **Resource Availability (RA)**
  - Ensure the availability of all network resources to protect against denial of service attacks.

Honeywell

Traditional Hierarchical Model of Control



Level 5 - Enterprise

Level 4 - Site Business Planning

Level 3 - Site Manufacturing Operations

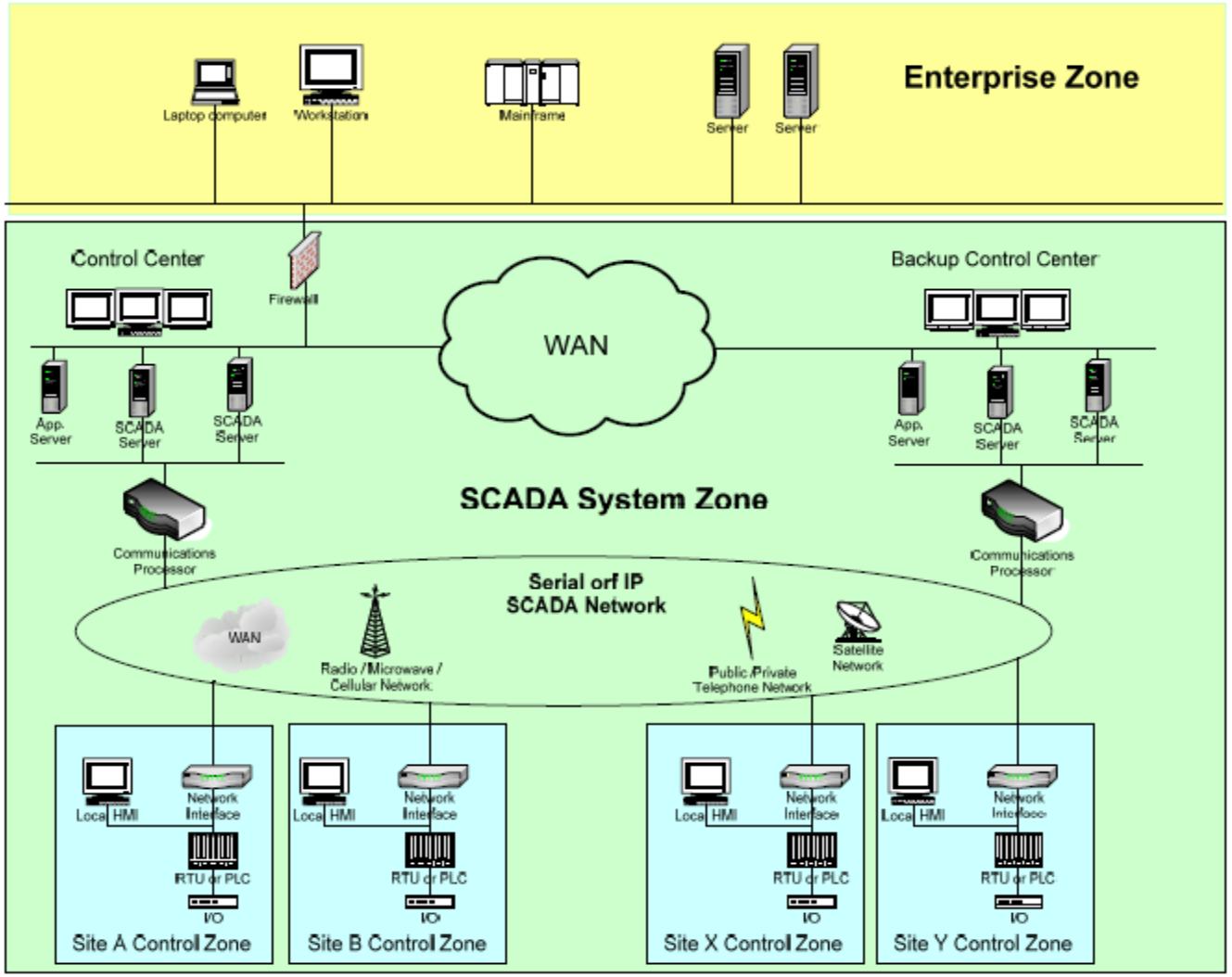
Level 2 - Area Supervisory Control

Level 1 - Basic Process Control

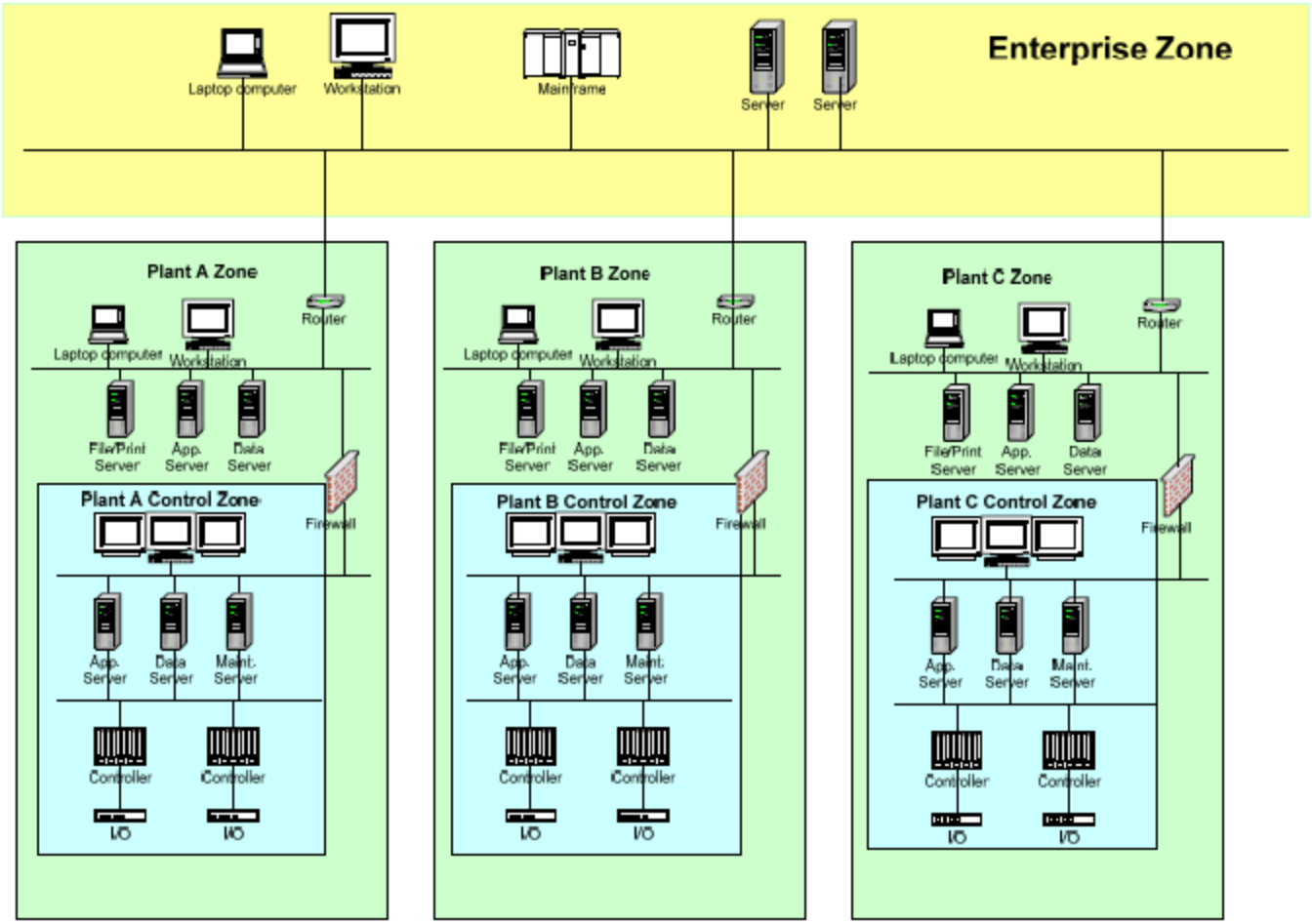
Level 0 - Field Instrumentation

Safety-Critical
- Protective Systems
- Safety Instrumented Systems

SCADA System reference model



DCS reference model

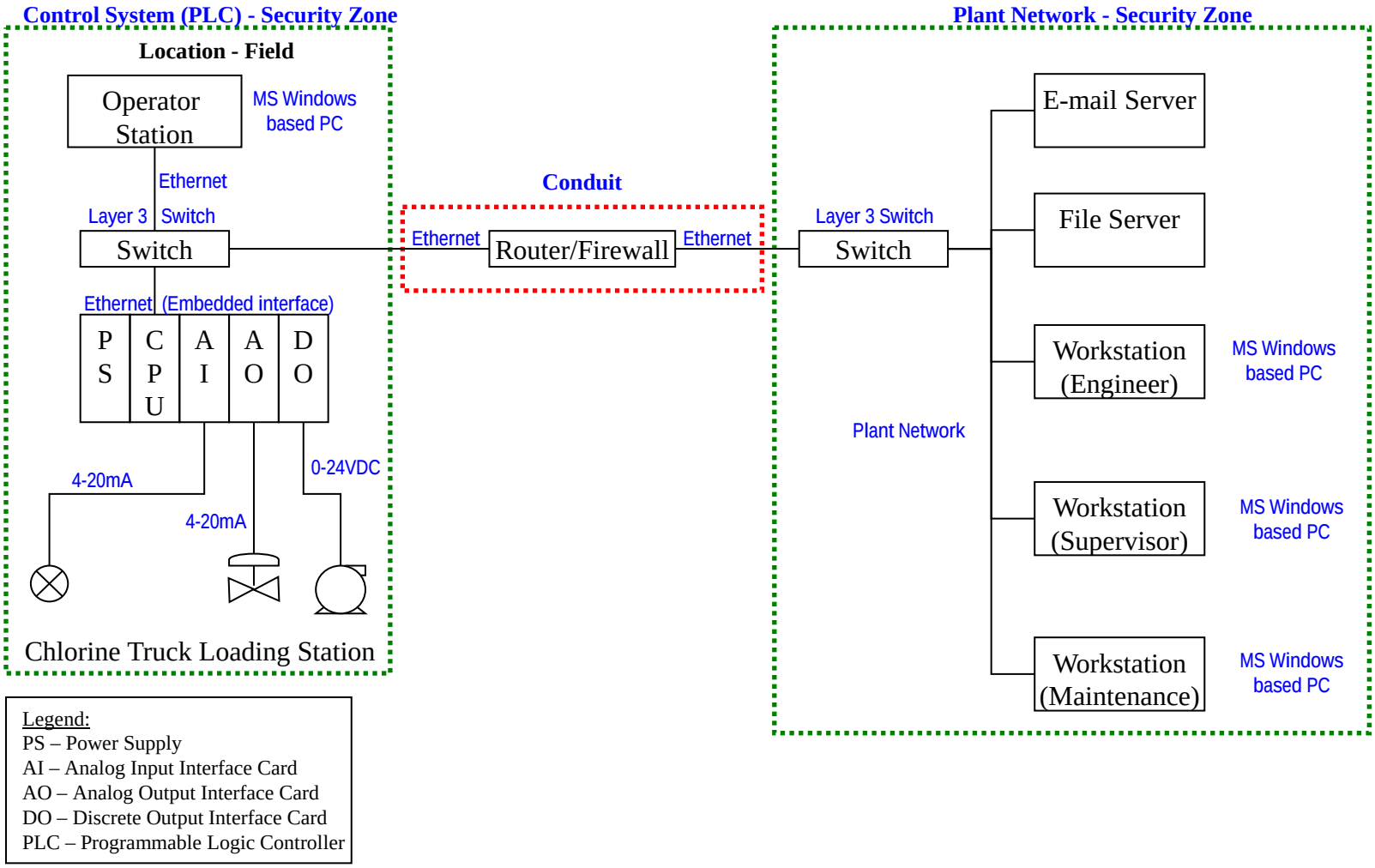


ISA99 Zones and Conduits Model

- A methodology and standard defining network segmentation allocating systems components into security zones
- A methodology and standard for defining security assurance levels for the security zones
- A methodology and standard defining the communications that occur between security zones through conduits

Honeywell

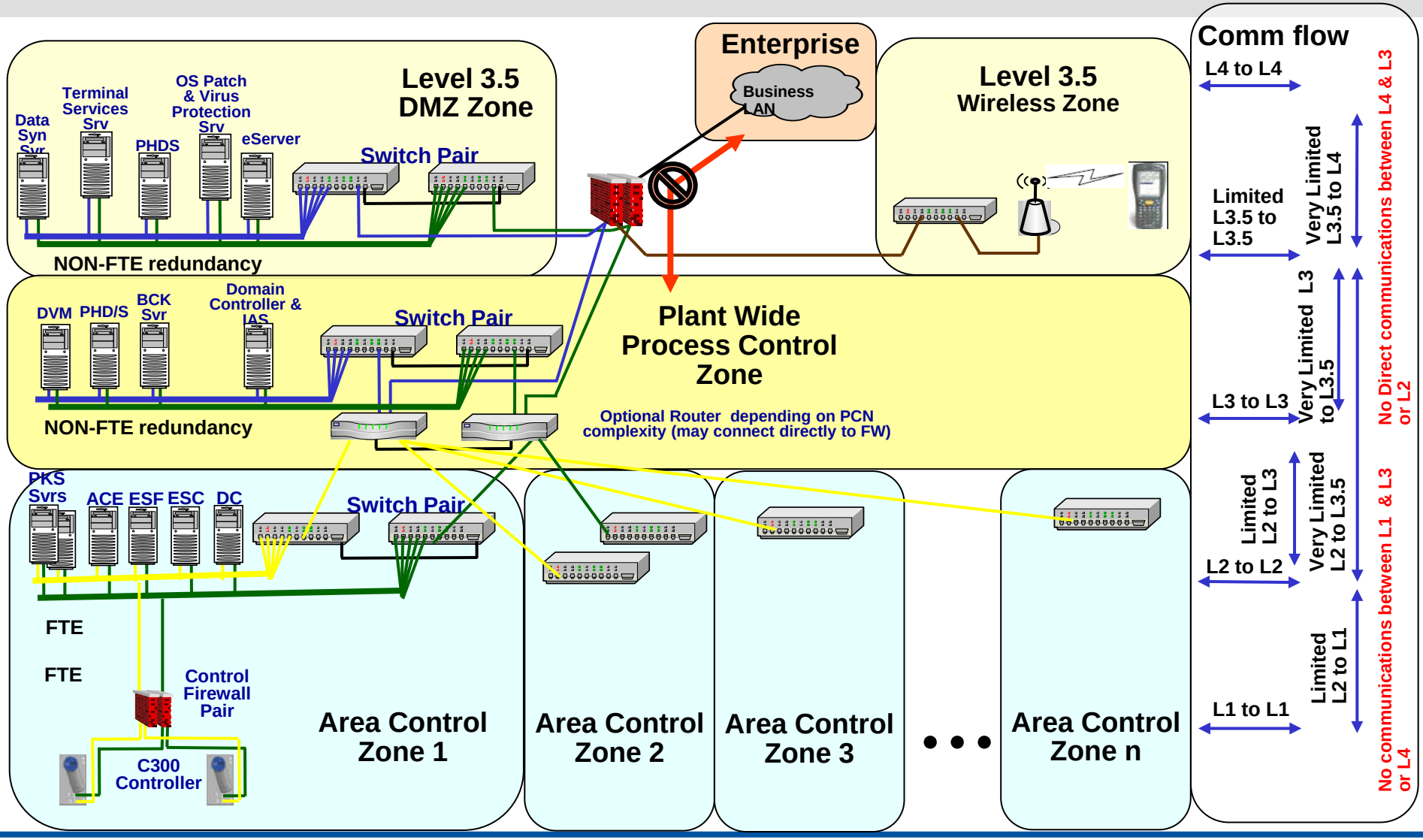
A simple example using zones and conduits



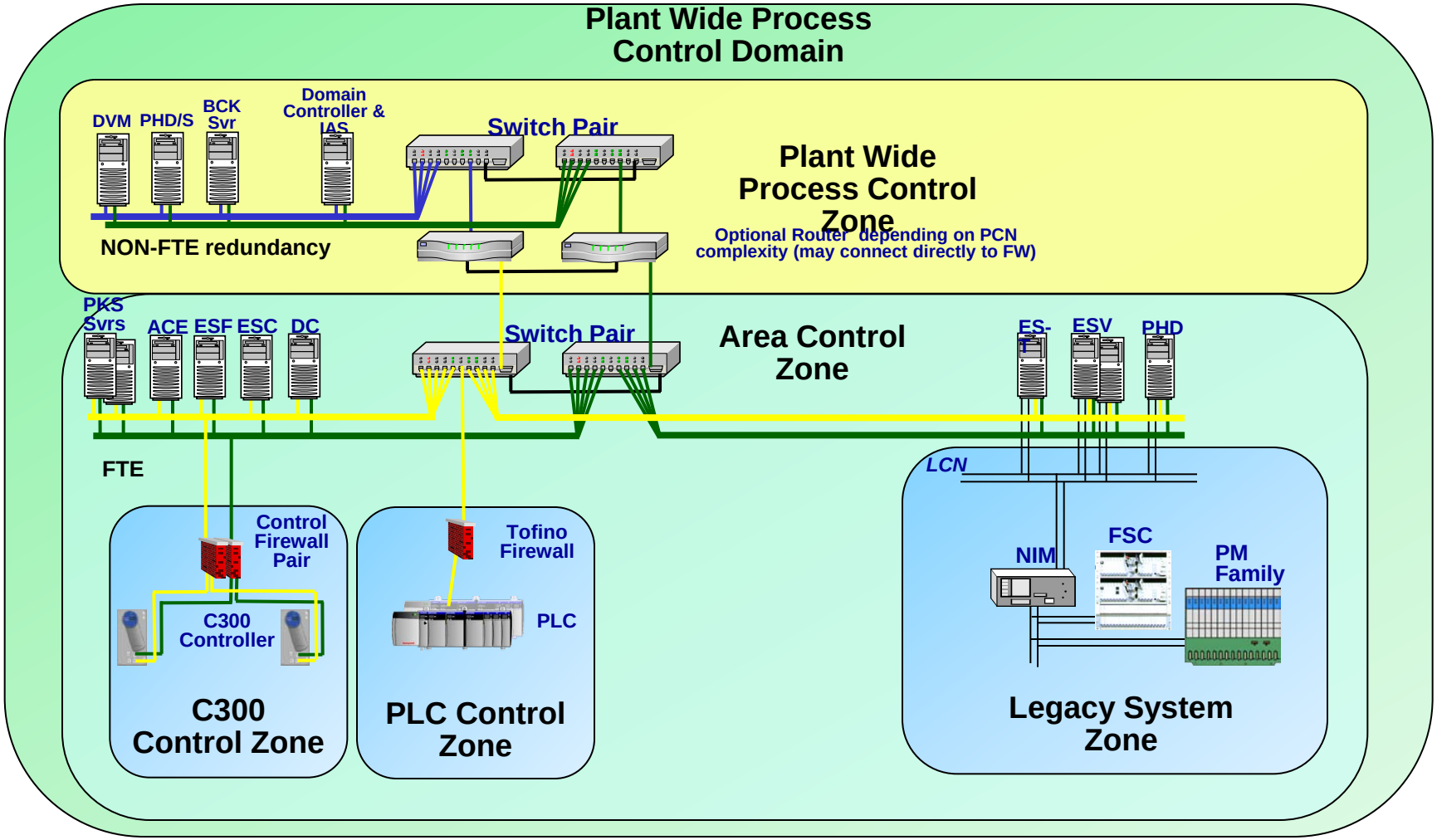
Legend:
PS – Power Supply
AI – Analog Input Interface Card
AO – Analog Output Interface Card
DO – Discrete Output Interface Card
PLC – Programmable Logic Controller

Honeywell

A more complex example of zones and conduits

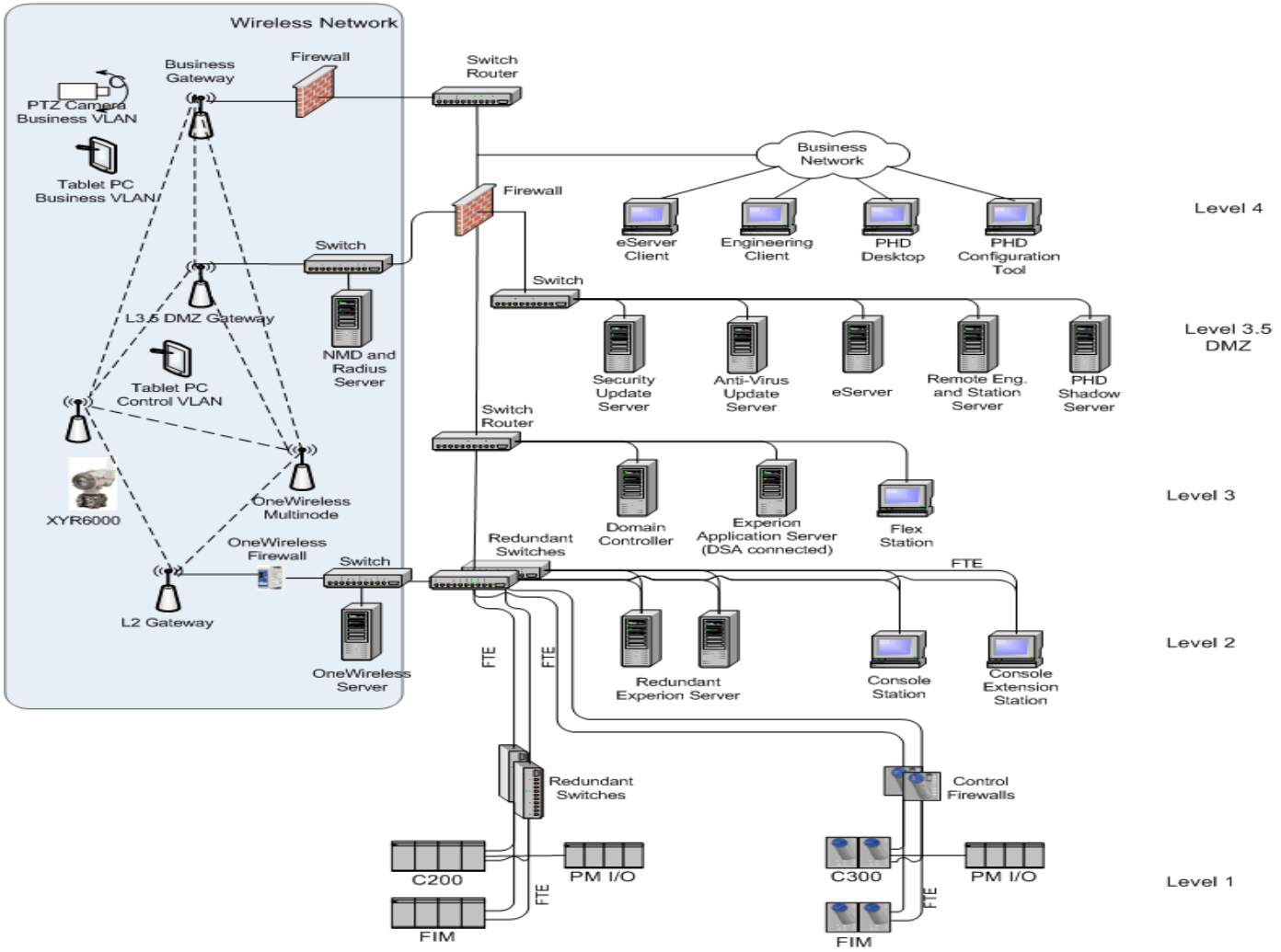


Protecting the controllers



Honeywell

Wireless for all levels of the plant



Where do we go from here

- Completion of the ISA99 standard
- All foundational requirements can be implemented in Levels 2 and above today
- Definition of roles for an IACS
- Implementation of least privilege

Challenges and opportunities

- Long term integration with legacy systems and controllers
- Integration of security reference monitors for physical equipment and IACS Data
  - Currently IACS data is protected using standard IT practices
  - Authorization to physical equipment is implemented in the IACS
  - Reference monitors not integrated very well
- Implementation of security in the controllers and PLCs