ENGlobal®

GLOBAL THINKING...GLOBAL SOLUTIONS™

Incorporating Cyber Security into your Automation Project's Execution Methodology

Making industrial security a core competency within the automation project organization

Joel Langill
TÜV FSEng ID-1772/09, CCNA
Staff Engineer / Consultant
ENGlobal – Automation
Houston, Texas

ICSJWG 2010 Spring Conference
San Antonio, Texas

April 6-8, 2010

Topics of Discussion

- **Today's Automation Contractor**
  - Evolution of the Main Automation Contractor
  - MAC Scope of Supply
  - Project Lifecycle
  - Traditional Project Execution Methodology
- **Security Lifecycle Model**
- **Improving the Execution Methodology**
  - Organizational Changes
  - New Class of Engineering Services
  - Improvements to Solution Documentation
  - Solution Integrity Testing
- **Tomorrow's Automation Contractor**

Evolution of the Main Automation Contractor

- Beginning in the mid 1990’s, end-users started to require more than just a control system, but an all-inclusive automation “solution”
- Transition from stand-alone systems, to complete integrated solutions comprising Level 0 (instrumentation) through Level 3 (MES) applications
- Integration to Level 4-5 business applications became more common
- Shift from a commodity-based delivery model to a services-based one
- By the late 1990’s, vendors saw MAC projects as an opportunity to increase project revenue and extend after-market services
- Solution was so broad that it required both a vendor’s “in-house” products augmented with a large percentage of third-party components
- MAC became involved earlier in the project lifecycle, and often provided lifecycle support services after the EPC demobilized
- MAC required to establish and manage multiple “horizontal” and “vertical” project interfaces, often on a global basis

Growing MAC Scope of Supply

APPLICATIONS / SYSTEMS

- Analyzer Systems
- Burner Management
- Compressor Surge Control
- Cont. Emissions Monitoring
- Custody Transfer
- DCS
- Fire & Gas
- Laboratory Information Mgmt
- Machinery Monitoring
- Motor Control Centers
- Plant Information Mgmt
- PLC’s
- Safety Instrumented Systems
- SCADA
- Tank Gauging
- Turbine Speed Control

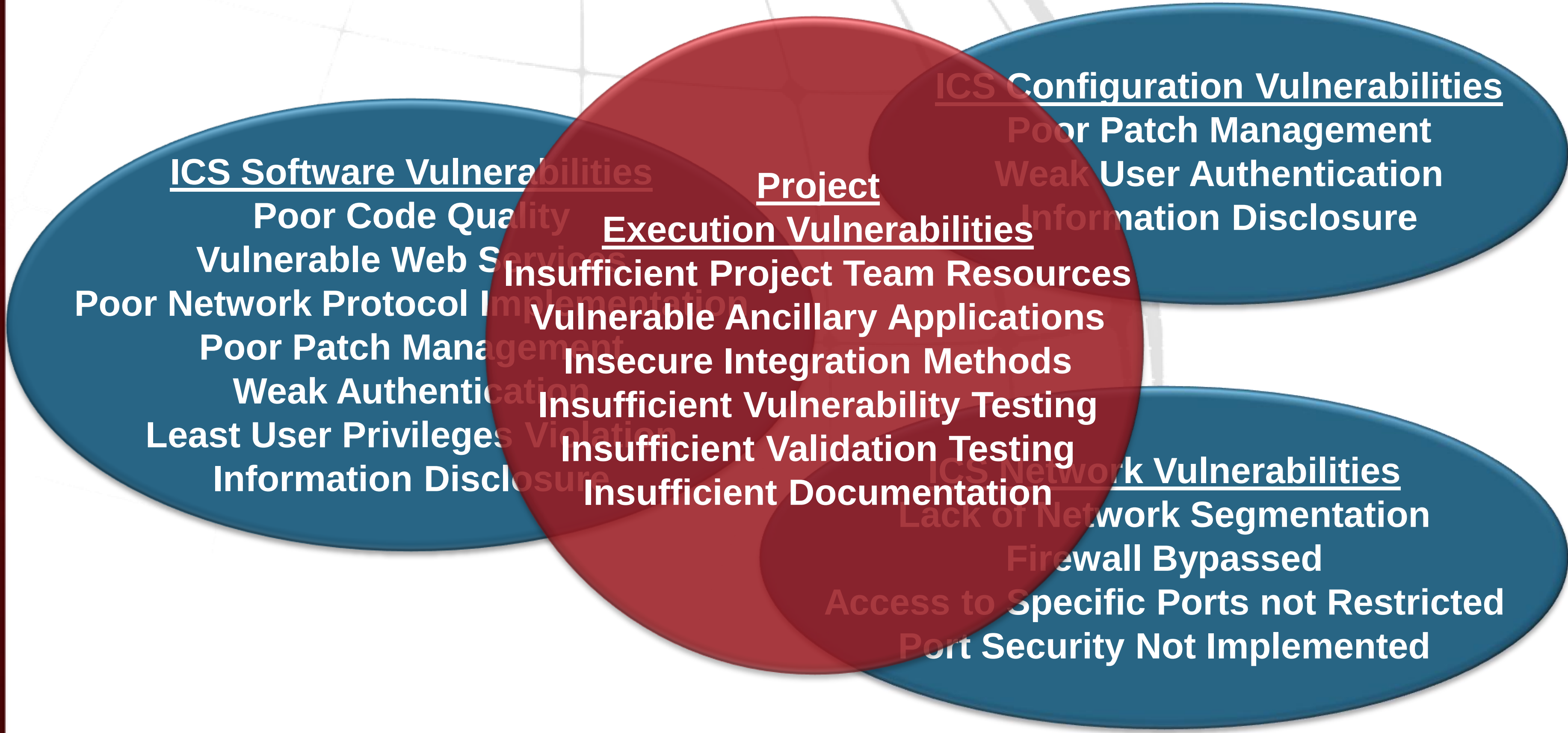
METHODS OF INTEGRATION

- DDE / NetDDE
- FTP / TFTP
- HTTP / HTTPS
- Modbus RTU/ASCII
- Modbus TCP
- .NET
- ODBC
- “Classic” OPC (MS DCOM)
- OPC-UA (XML)
- Profibus
- RPC
- SQL

Capabilities

Vulnerabilities

Common Control System Vulnerabilities



ICS Software Vulnerabilities
Poor Code Quality
Vulnerable Web Services
Poor Network Protocol Implementation
Poor Patch Management
Weak Authentication
Least User Privileges Violation
Information Disclosure

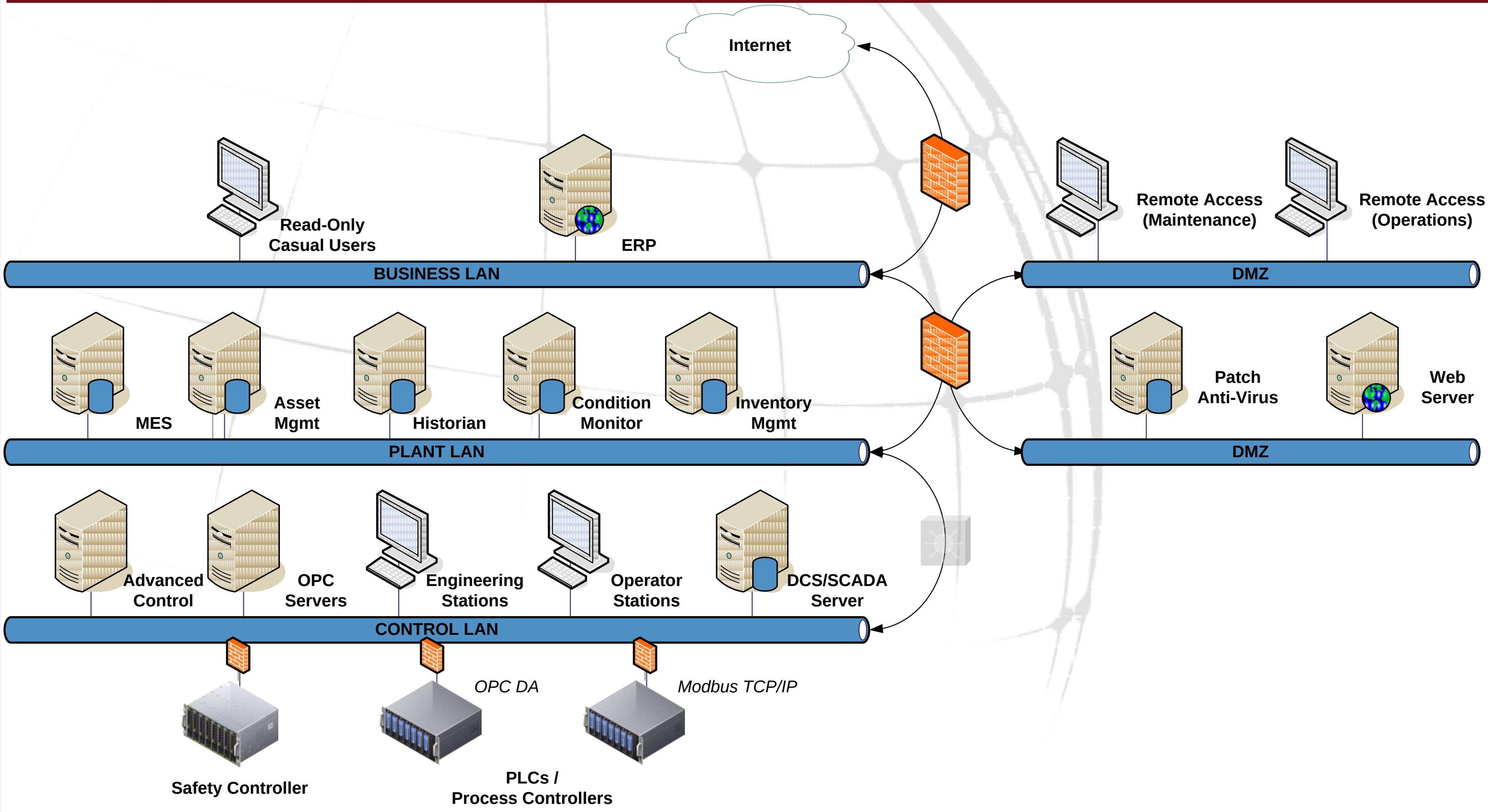
Project Execution Vulnerabilities
Insufficient Project Team Resources
Vulnerable Ancillary Applications
Insecure Integration Methods
Insufficient Vulnerability Testing
Insufficient Validation Testing
Insufficient Documentation

ICS Configuration Vulnerabilities
Poor Patch Management
Weak User Authentication
Information Disclosure

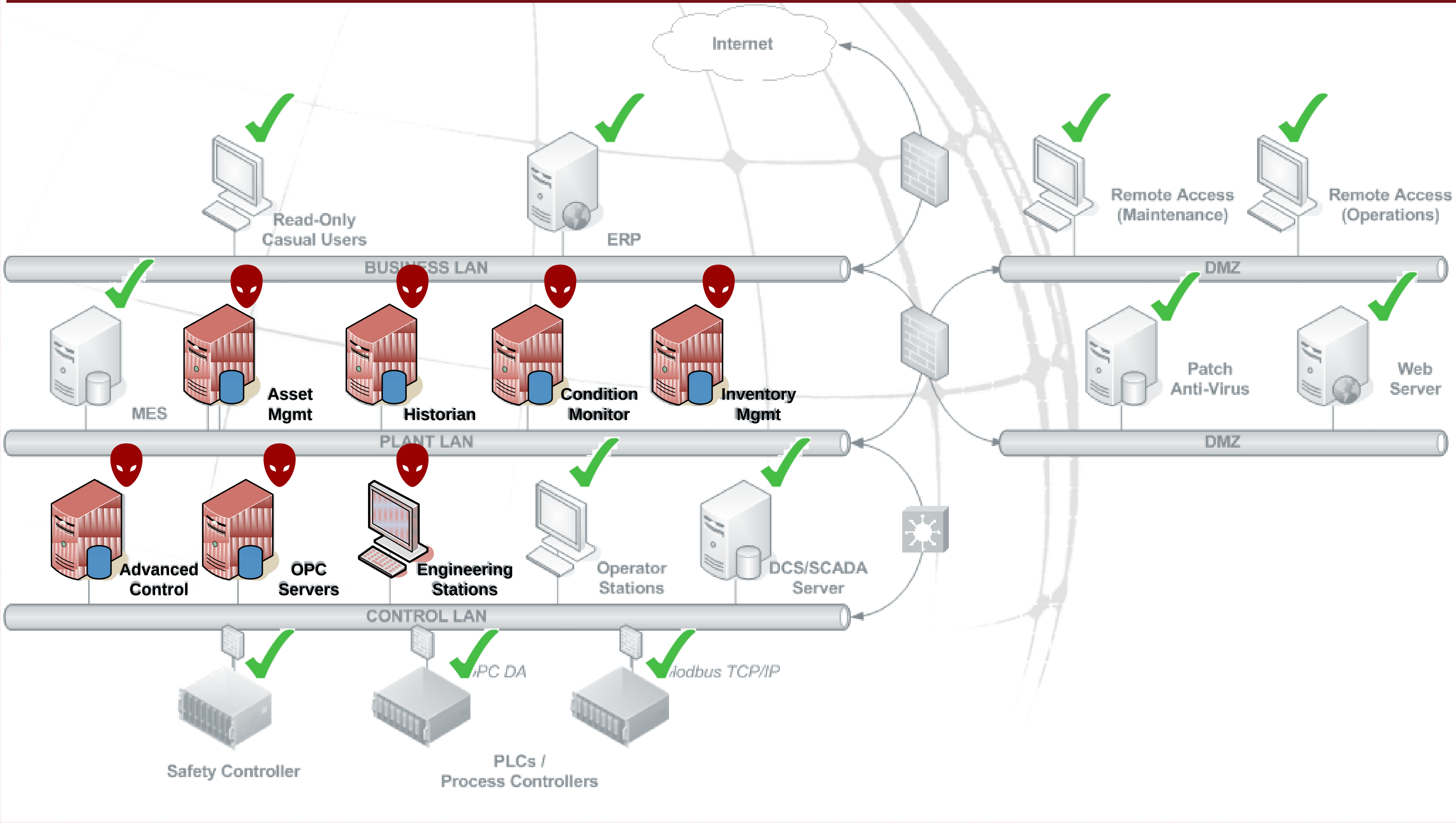
ICS Network Vulnerabilities
Lack of Network Segmentation
Firewall Bypassed
Access to Specific Ports not Restricted
Port Security Not Implemented

Source: "Common Cyber Security Vulnerabilities Observed in DHS Industrial Control Systems Assessments", DHS CSSP, July 2009

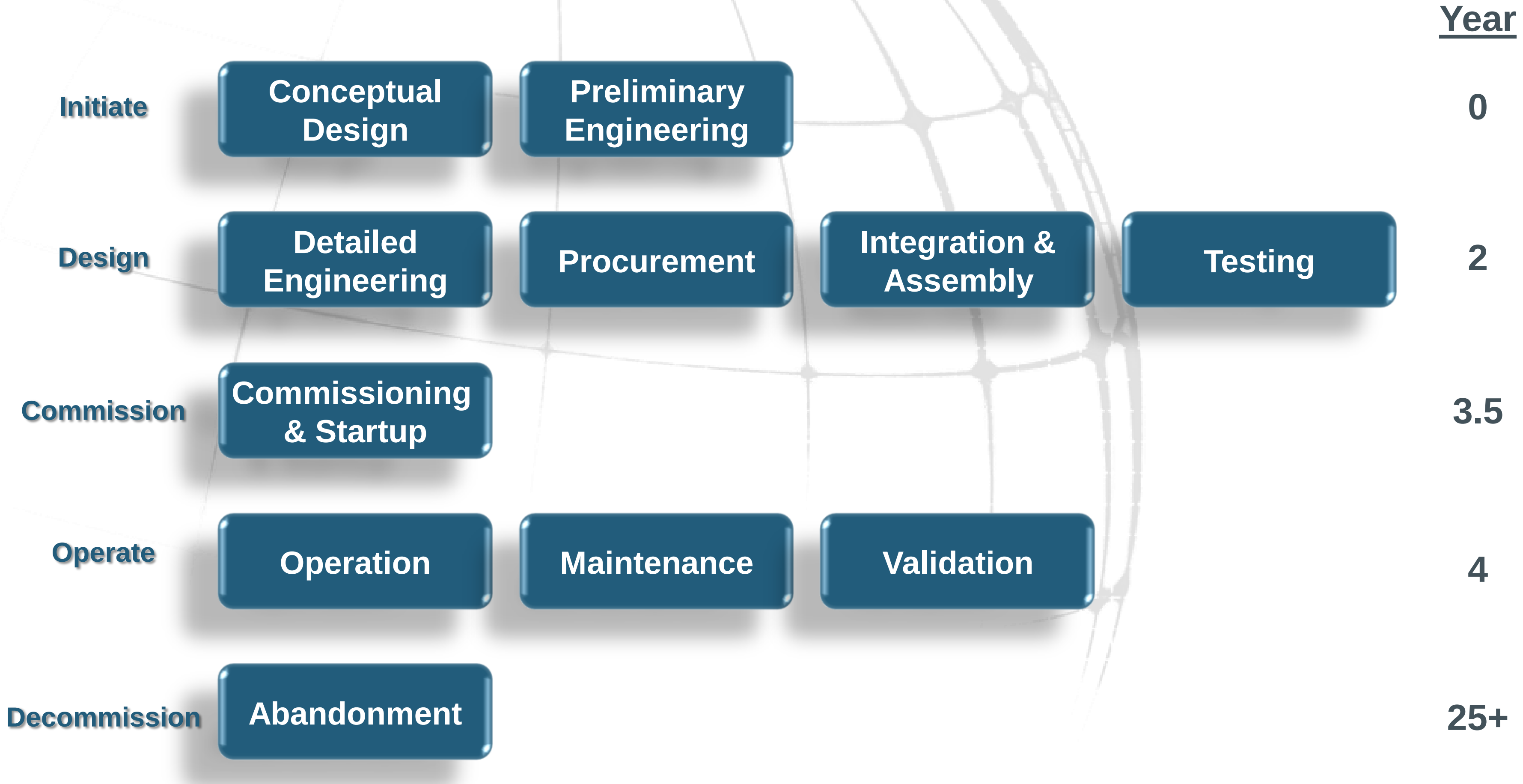
Integrated Control System Threat Vectors



Integrated Control System Threat Vectors



Project Lifecycle



					Year
Initiate	Conceptual Design	Preliminary Engineering			0
Design	Detailed Engineering	Procurement	Integration & Assembly	Testing	2
Commission	Commissioning & Startup				3.5
Operate	Operation	Maintenance	Validation		4
Decommission	Abandonment				25+

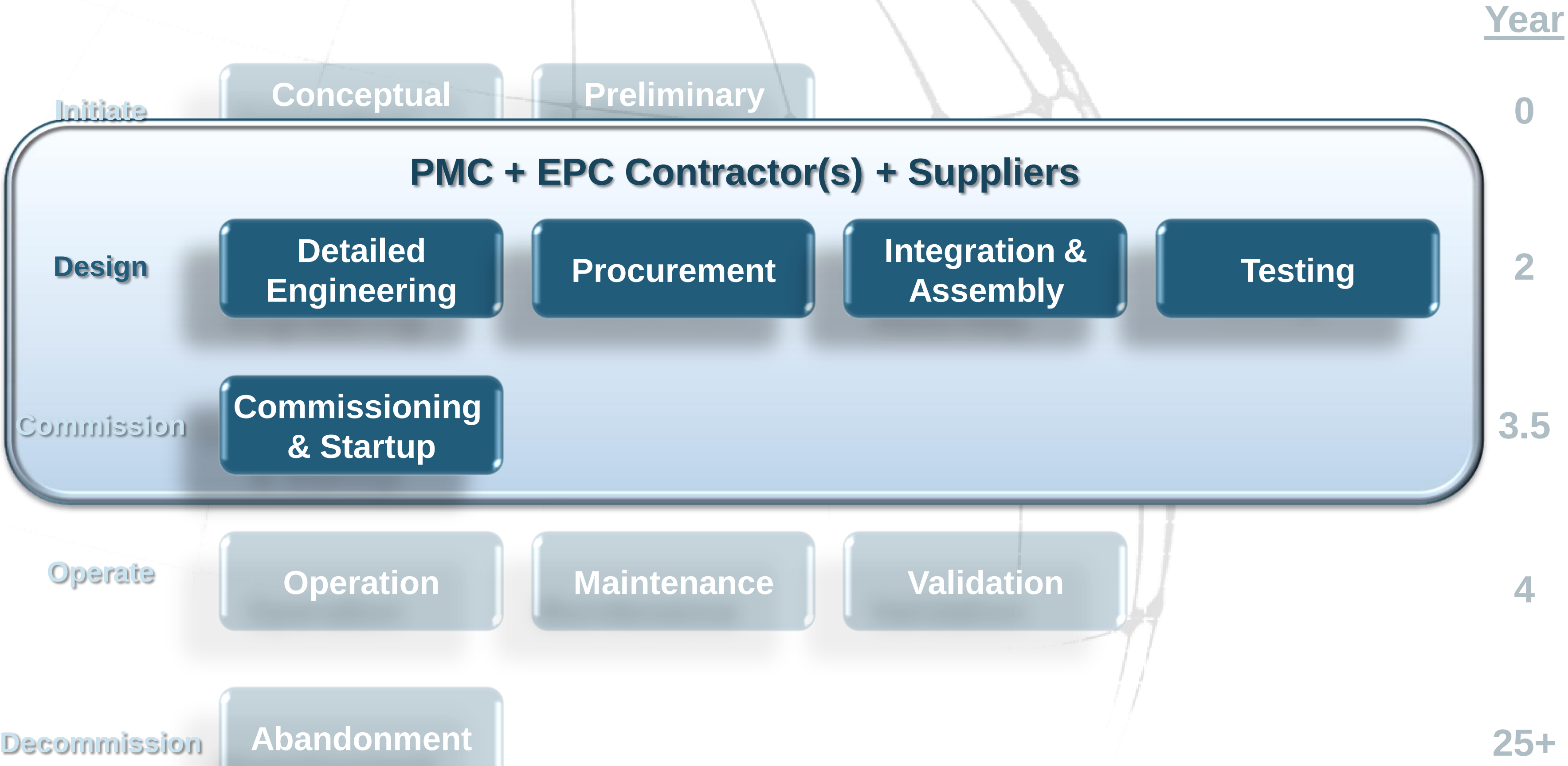
Project Lifecycle

Owner-Operator + FEED Contractor

					Year
Initiate	Conceptual Design	Preliminary Engineering			0
Design	Detailed Engineering	Procurement	Integration & Assembly	Testing	2
Commission	Commissioning & Startup				3.5
Operate	Operation	Maintenance	Validation		4
Decommission	Abandonment				25+

FEED = Front-End Engineering and Design

Project Lifecycle



Year

Initiate — Conceptual — Preliminary — 0

PMC + EPC Contractor(s) + Suppliers

Design — Detailed Engineering — Procurement — Integration & Assembly — Testing — 2

Commission — Commissioning & Startup — 3.5

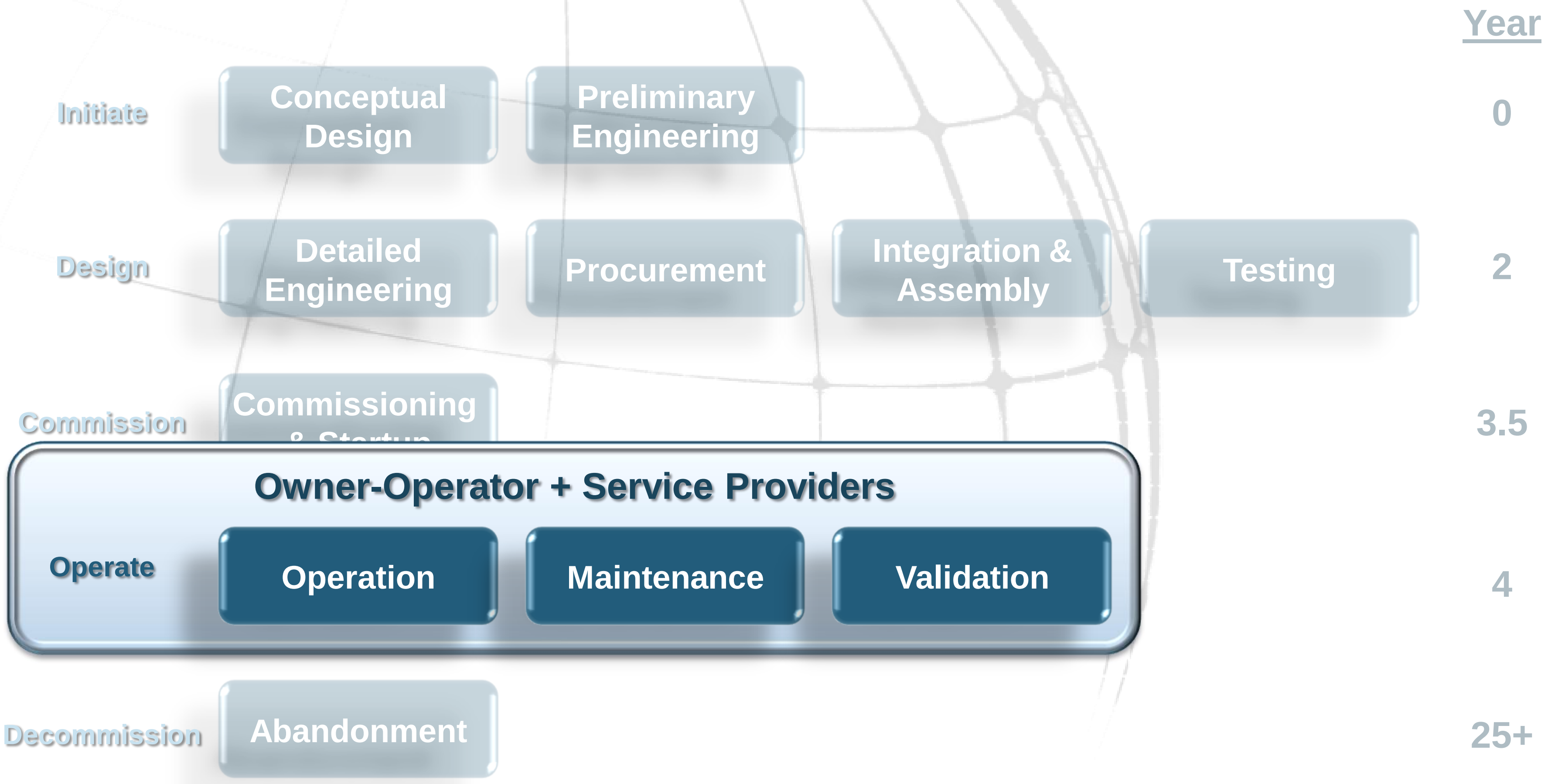
Operate — Operation — Maintenance — Validation — 4

Decommission — Abandonment — 25+

PMC = Project Management Contractor

EPC = Engineering, Procurement & Construction

Project Lifecycle



Year

Initiate
Conceptual Design
Preliminary Engineering
0

Design
Detailed Engineering
Procurement
Integration & Assembly
Testing
2

Commission
Commissioning & Startup
3.5

Owner-Operator + Service Providers

Operate
Operation
Maintenance
Validation
4

Decommission
Abandonment
25+

Project Development Lifecycle

Preliminary Engineering

Technology selection, overall system functionality, preliminary architecture, security strategy, MAC mobilization, approved vendor lists, roles & responsibilities, AFD documentation

Detailed Engineering

HAZOP/PHA, risk assessments, SIL studies, component specifications, network design & segmentation, countermeasure selection, configuration, installation drawings

Procurement

Application development, component selection, inspection, version control, change management, AFC documentation

Integration & Assembly

Assemble systems, application integration, middleware, performance calculations

Testing

Functionality, interoperability, reliability, security, maintainability

Commissioning & Startup

Final integration, training, “as-built” documentation

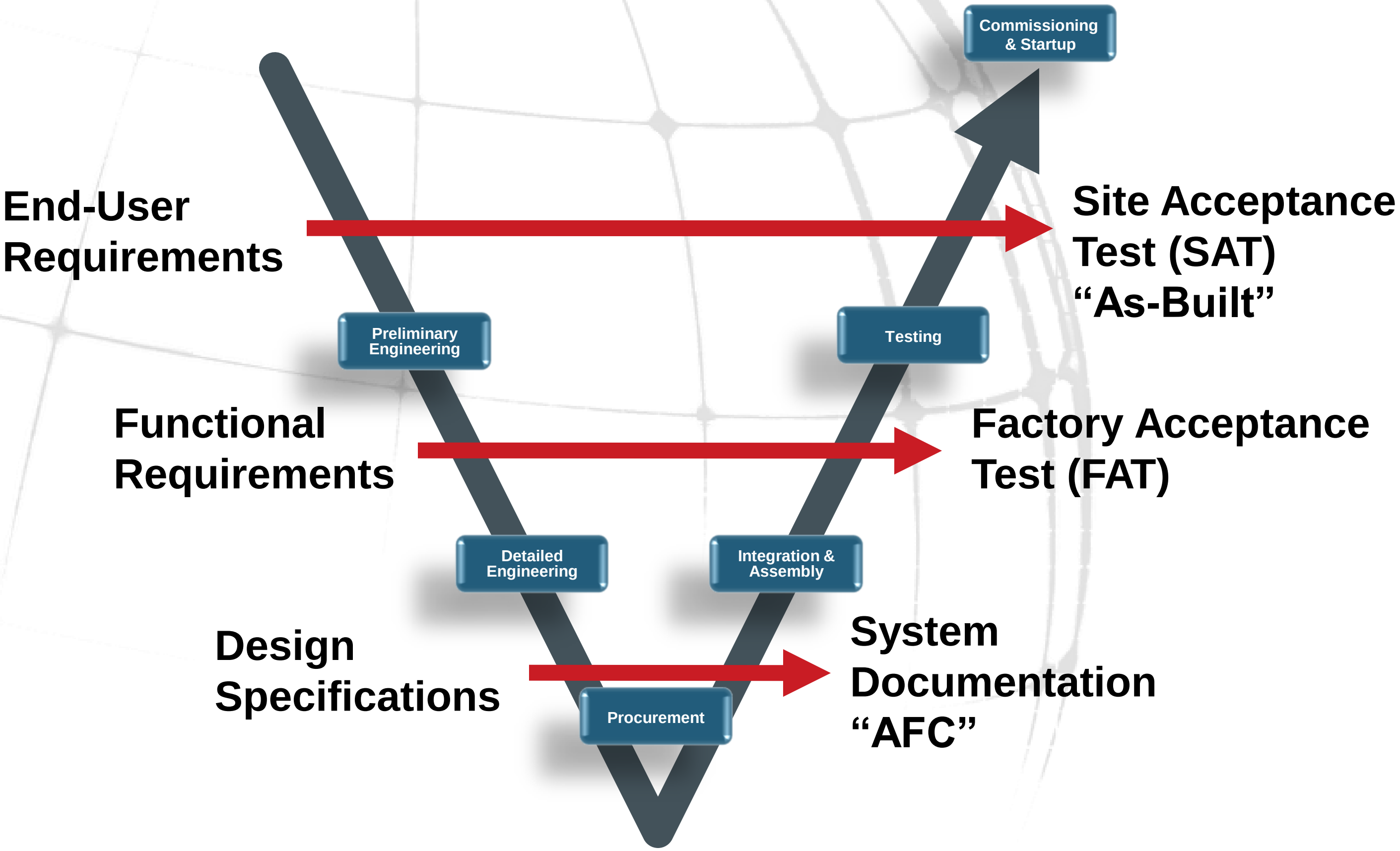
Traditional Project Execution Methodology

1. Early engagement of MAC during FEED to establish project standards for major system components
2. Project organization is typically segmented using a commodity-centric approach
3. Additional segmentation occurs when dealing with multiple EPC contractors
4. Standards are developed, deployed and managed for compliance
5. Functional specifications are developed
6. Configuration activities commonly sent to low-cost organizations
7. Test plans are developed in the later stages of the Detailed Design phase
8. Components are integrated and a pre-test performed prior to any client witnessed test(s)
9. Installation at site is followed by a site test to validate overall operation
10. Commissioning and startup of facility with integrated automation solution
11. Documentation updated to "as-built" and project close-out occurs

Transitioning the MAC Project Execution Methodologies

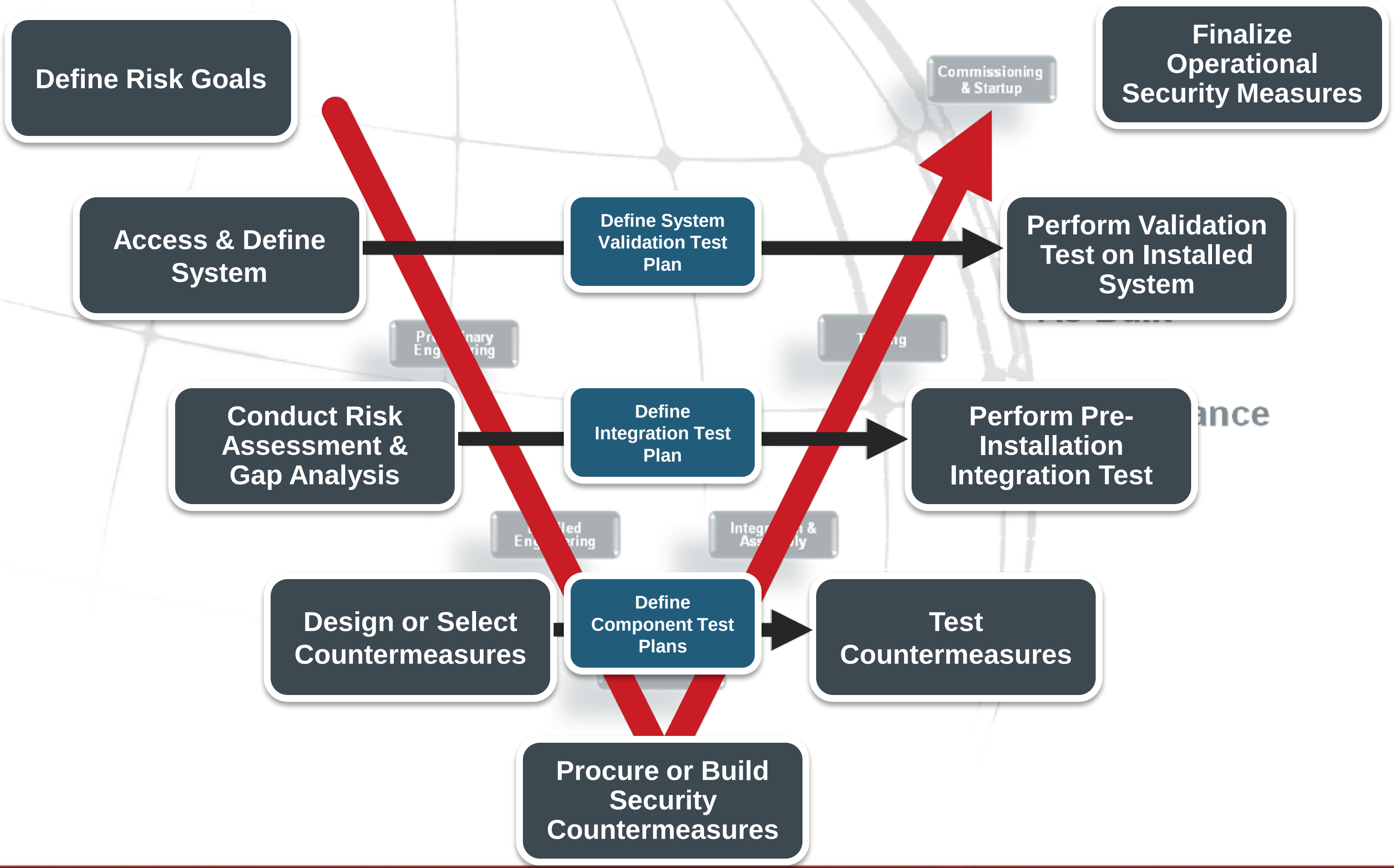
- **As a Main Automation Contractor, they must assure their clients that they can:**
  - Deliver an automation solution using the latest technologies,
  - Work with multiple contractors, suppliers, licensors and in-house resources
  - Find qualified resources for the required scope
  - Maintain the integrated project schedule
  - Design, integrate and test the automation systems prior to commissioning
  - Integrate the automation systems at site with other business components
  - Follow vendor recommendations for security
  - Document the delivered solution
  - Maintain the integrity of the delivered solution over the life of the plant

Project Development Lifecycle



Sources: "Planning Cuts Automation Project Risk", Control Engineering, September, 2009
Good Automated Manufacturing Practice (GAMP) Forum and Best Practices of the Control Systems Integrator Association (CSIA)

Project Development Lifecycle + Security Lifecycle Model



Define Risk Goals

Access & Define System

Conduct Risk Assessment & Gap Analysis

Design or Select Countermeasures

Procure or Build Security Countermeasures

Test Countermeasures

Perform Pre-Installation Integration Test

Perform Validation Test on Installed System

Finalize Operational Security Measures

Define System Validation Test Plan

Define Integration Test Plan

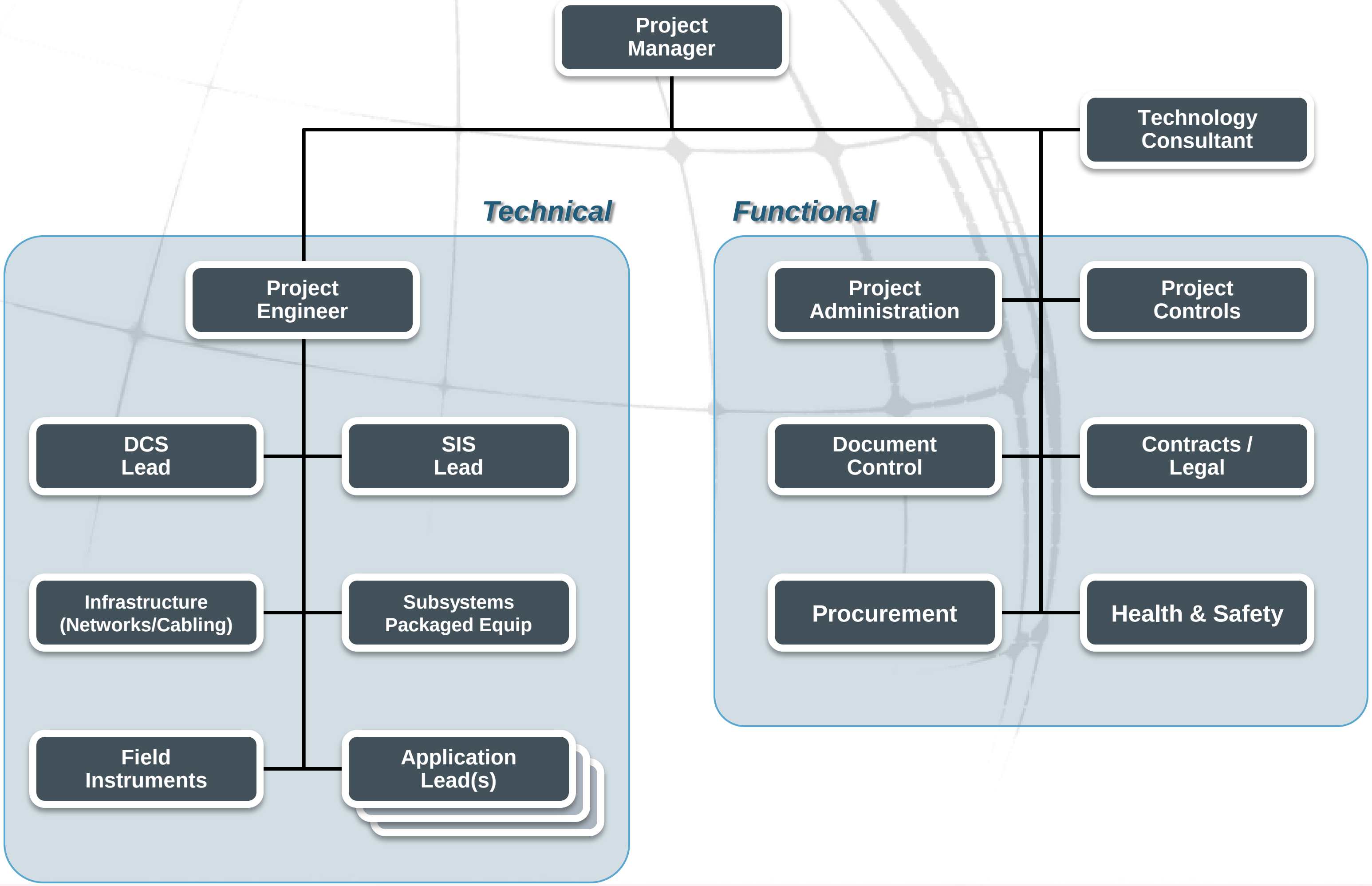
Define Component Test Plans

Source: *"Planning Cuts Automation Project Risk", Control Engineering, September, 2009*
"Integrating Electronic Security into the Manufacturing and Control Systems Environment", ISA-TR99.00.02-2004

Improving the Execution Methodology

- Studies and white papers from analysts, consultants, and end-users alike confirm that maintaining qualified resources is a challenge
- With the vast amount of application and system integration which must be performed, standards are often compromised for the sake of schedule
- DCS and SIS are both considered high profile roles and include dedicated resources from the MAC, EPC and end-user
- Security is typically not a high priority, and is often delegated to the individual/team responsible for "network and infrastructure"
- Concept of "plug-and-play" has led to complacency with respect to ancillary applications and how they impact the integrity of the overall solution
- Initial improvements to the project execution methodology cover
  - Organizational Changes
  - New Class of Engineering Services
  - Improvements to Solution Documentation
  - Solution Integrity Testing

Organizational Changes



Project Manager

Technology Consultant

Technical

Project Engineer

DCS Lead

SIS Lead

Infrastructure (Networks/Cabling)

Subsystems Packaged Equip

Field Instruments

Application Lead(s)

Functional

Project Administration

Project Controls

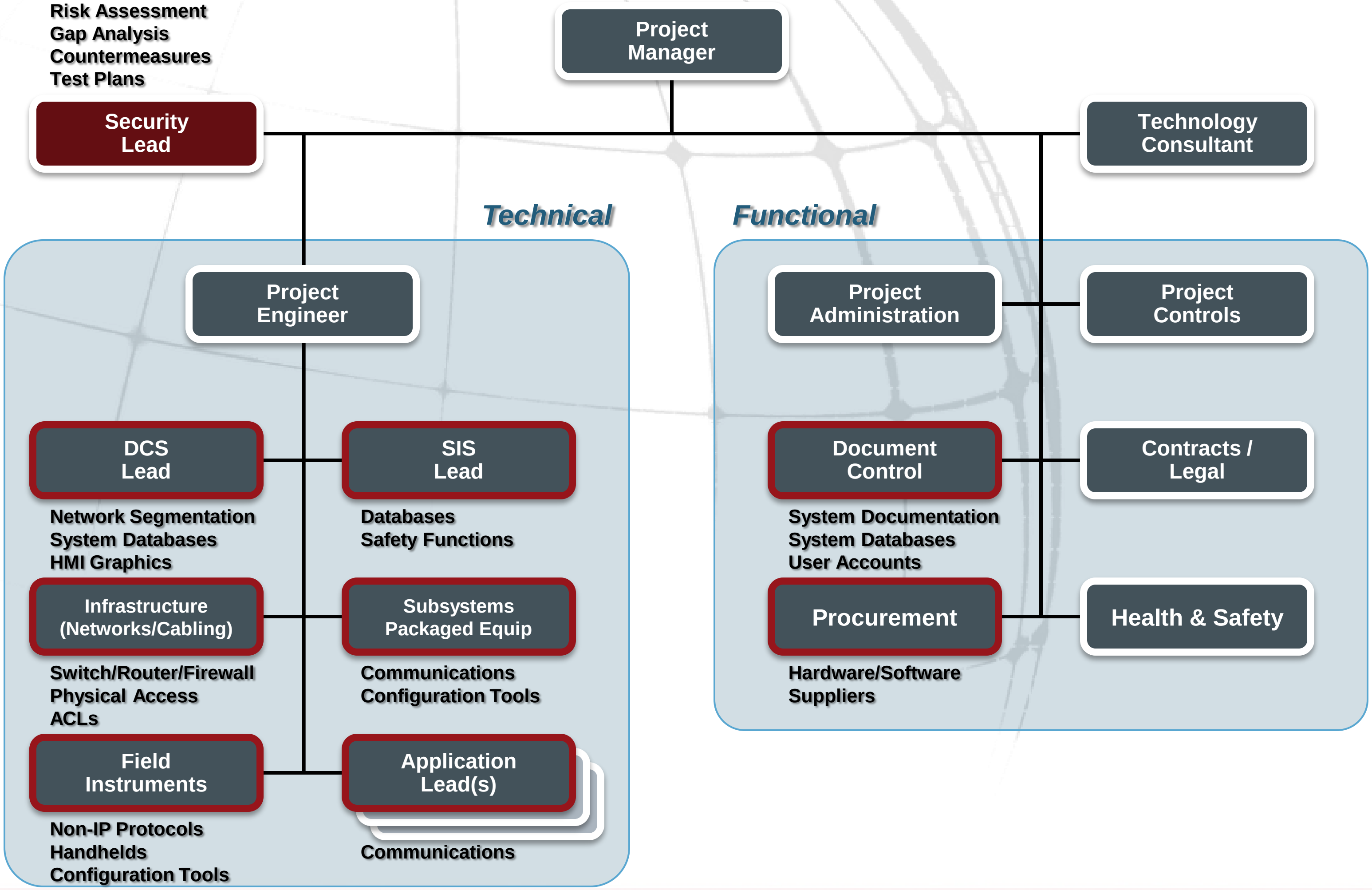
Document Control

Contracts / Legal

Procurement

Health & Safety

Organizational Changes



Project Manager

Security Lead

Risk Assessment
Gap Analysis
Countermeasures
Test Plans

Technology Consultant

Technical

Project Engineer

DCS Lead

Network Segmentation
System Databases
HMI Graphics

SIS Lead

Databases
Safety Functions

Infrastructure (Networks/Cabling)

Switch/Router/Firewall
Physical Access
ACLs

Subsystems Packaged Equip

Communications
Configuration Tools

Field Instruments

Non-IP Protocols
Handhelds
Configuration Tools

Application Lead(s)

Communications

Functional

Project Administration

Project Controls

Document Control

System Documentation
System Databases
User Accounts

Contracts / Legal

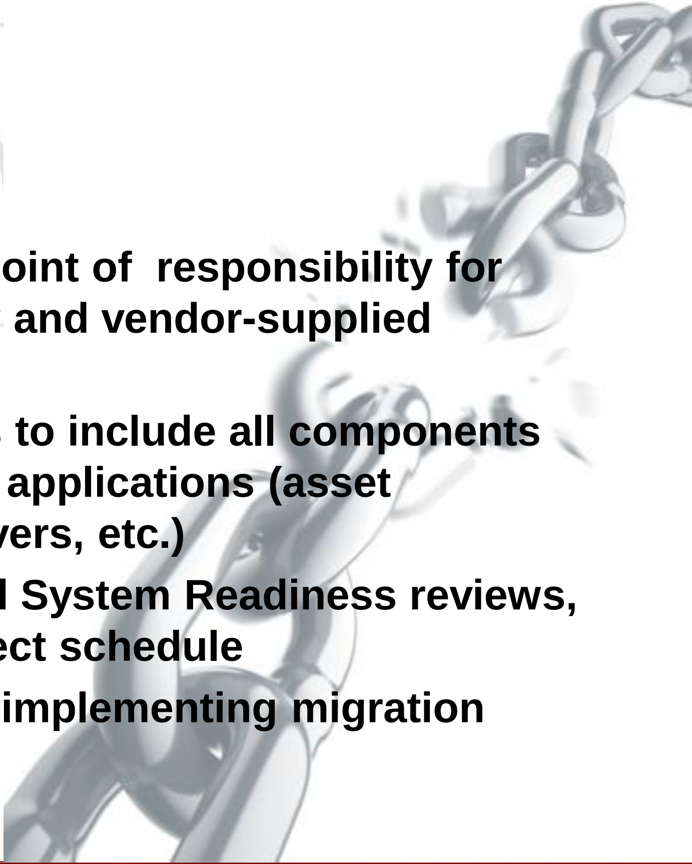
Procurement

Hardware/Software
Suppliers

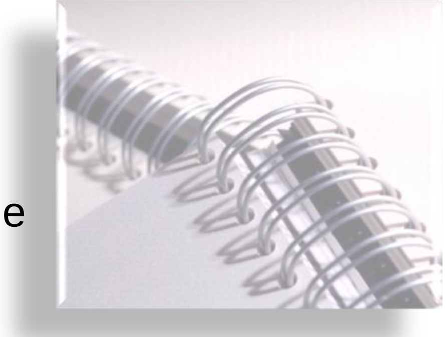
Health & Safety

New Class of Engineering Services

- **Project funding is provided to cover the additional costs required for security related tasks addressed in the development and execution of**
  - Functional Requirements
  - Component Selection
  - Test Planning
  - Commissioning
  - Documentation Deliverables
- **With the MAC scope of supply so broad, a single point of responsibility for security should be assigned to address third-party and vendor-supplied components**
- **Attention is expanded from MAC core components to include all components comprising the overall solution including ancillary applications (asset management, historian, etc.), third-party (OPC servers, etc.)**
- **In addition to standard System Design reviews and System Readiness reviews, specialized Security reviews are added to the project schedule**
- **Incorporate assessments of legacy systems when implementing migration program**



Improvements to Solution Documentation



- **Increase the level of system documentation related to security and long-term security maintenance**
  - Network segmentation
  - Data flow diagram and description of protocols and port usage
  - At the component level, provide details associated with
    - Authentication
    - Encryption
    - Access Control
    - Event and Communication Logging
    - Alarming
  - Switch and Firewall configuration files assigned document numbers and included in MOC procedures
- **System documentation needs to be classified in terms of confidentiality from a security point of view**
- **ANSI/ISA-99.02.01 provides guidance on many of these recommendations, and needs to become standard project practices**

Solution Integrity Testing

- Test not only the “functionality” of the integrated solution, but the “integrity and security” as well
- Automation system must meet both the operational objectives and the security goals of the end-user
- Comprehensive component (subsystem), integration (FAT), and system validation (SAT) test plans need to include security performance testing, as well as operational testing of the final configured system
- In addition to validating that each component complies with the vendor’s recommendations (configuration, policies, DCOM, etc.), vulnerability and active port scanning is included as a part of the standard factory test
  - The factory test provides one of the last opportunities to perform an “aggressive” testing without risk of impact to production
- Test plan should focus equally on core (system server, HMI, etc.) and ancillary components (asset management, history, advanced control, etc.)
- Validation and documentation from all third-party component suppliers
- Important to address non-IP protocols in test plans

Department of Homeland Security: Cyber Security Procurement Language for Control Systems

September 2009

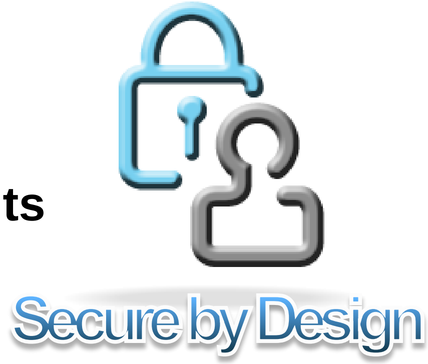
Homeland Security

Control Systems Security Program
National Cyber Security Division

Sources: “Integrating Electronic Security into the Manufacturing and Control Systems Environment”, ISA-TR99.00.02-2004
“Cyber Security Procurement Language for Control Systems”, DHS CSSP, September 2009

Tomorrow’s Automation Contractor

- **“Security by Design” rather than “Security by Default”**
  - Structural reporting changes to address security across the entire project organization
  - Increased awareness of security within all project disciplines
  - Compliments in-house capabilities with experienced, vendor-neutral third-parties to fill critical resource gaps
- **Elevates Industrial Security within the organization in the same manner as Functional Safety**
  - Dedicated resources within EPC and End-User teams
- **Security controls and practices become an influence in buying decisions**
  - DHS Procurement Language for Control Systems
- **Drive towards industry-specific security certifications, registrations, etc. for individuals, as well as components**
  - ICSJWG Work Force Development Subgroup



ENGlobal®

Global Thinking … Global Solutions™

ICSJWG 2010 Spring Conference

San Antonio, Texas

April 6-8, 2010