Patch Management Program for Control Systems

Challenges, Perspectives and Responses

ISA99 Committee on Control Systems Security

ICSJWG 2010 Spring Conference

Abstract

Industrial Control Systems are built upon open systems platforms with security updates and other patches issued regularly from the various suppliers. Vendors of control systems regularly issue operational patches and occasionally security patches that must be assessed for the impact to control systems and installed, if necessary, onto those control systems.

The ISA99 committee is developing international standards and associated technical reports and recommended practices on this subject, including a recommended approach for managing and sharing patch compatibility information. This presentation will describe what is available, how it can be used and the longer term plans to address other areas of a comprehensive patch management system. Topics of particular interest include the difference between patch management programs for business systems and those for control systems and how to work with system vendors as part of the patch management program.

Topics

- What is patch management?
- Why is patch management important?
- The need for a Control Systems focus
- Elements of a patch management program
- The ISA99 contribution

What is Patch Management?

- A “formal” definition:
  - *Patch management is the process of using a strategy and plan of what patches should be applied to which systems at a specified time.* [1]
- Patches include problem fixes and security fixes
- Patches come from:
  - Operating system vendors
  - Infrastructure vendors
  - Control System vendors
  - Other software vendors

[1] – Source: Wikipedia

Patch Management is Change Management

The case for change must be understood by **all** stakeholders:

- Manufacturing asset owners
- IT leadership
- Engineering
- Plant Operations
- Support teams

Topics

- What is patch management?
- Why is patch management important?
- The need for a Control Systems focus
- Elements of a patch management program
- The ISA99 contribution

Patch Management is Risk Management

Managing the risk of change:

- Change introduces risk.
- Unplanned change risks are greater than planned change.
- Allows shifting of change into a planned event.
- Ensure appropriate resources are available and impact to plant are understood.

Addressing a Range of Needs

New environment

- New systems
- New functionality
- New infrastructure
- Major user changes
- Years between release

Emergency change

- Virus and vulnerability patches
- Critical application problems
- Critical infrastructure problems
- 3-14 days for delivery

Steady State change

- Change to standard systems
- Steady state patches
- New Server implementation
- 90 day for delivery

Engaging Operations

Plants Personnel need to understand and agree to changes:

- When a change will occur (i.e., date, time ,length of change)
- Why changes are happening.
- Impact of changes.
- Where to call if something not work

Working with control system vendors

- Documentation of software used by vendors products
  - Microsoft Windows
  - SQL Server
  - Adobe Acrobat
- Documentation of ports and protocols used
- Documentation of services used
- Accreditation of software patches by vendors
  - Accreditation in a timely fashion
  - Notification system for accreditation of patches

Topics

- What is patch management?
- Why is patch management important?
- The need for a Control Systems focus
- Elements of a patch management program
- The ISA99 contribution

An Assertion…

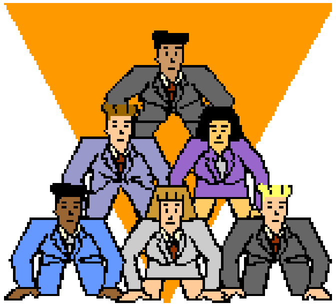
Improper patch management **CAN** compromise system availability

Not “Typical” Business Systems

- Difficulty in finding a “service window” for updates
- Unintended consequences (examples):
  - Interference with software license information
  - Incompatibility between patches and control system software
  - Virus and anti-malware “false positives”

More Stakeholder Groups

Cross-functional team with skills and authority to asses, understand impact and communicate changes



- Technical Infrastructure
  - Internal or outsourced
- Control system Application support
- Manufacturing operations application support
- Security expertise
- Vendor
  - Certification of patches and provided associated changes if needed
- IT Change Management
- Support staff
  - Help define impact and implementation approach

Topics

- What is patch management?
- Why is patch management important?
- The need for a Control Systems focus
- Elements of a patch management program
- The ISA99 contribution

Creating a Patch Management Program

- Start with an IT patch management program
  - Similar to process for critical IT servers
- Integrate into security management program
- Incorporate elements that are required for control systems
- Compliant with regulatory or sector requirements (e.g., NERC-CIP)

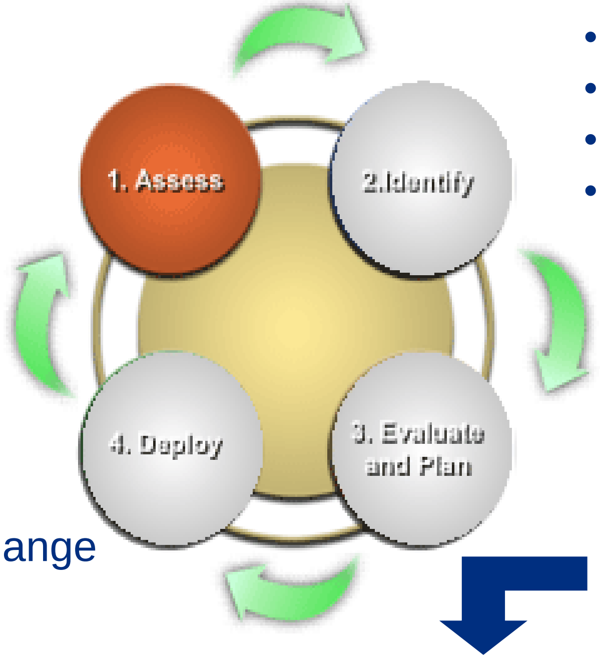
A Change Management Process

Assessment

- Need for change
- Magnitude of change
- Impact to users
- Support resources

Identification

- Group Changes
- Application
- Platform
- Network
- Firewall
- Security Bulletins



Deployment

- Early communications with plant
  - Scope and duration of change
- Deploy
  - Test environment
- Stage with Plant (time and date)
  - Plant approval
- Implementation
  - Plant approval

Evaluation

- Impact to users
- Risk of delaying
- Benefits to user
- Vendor certification

Emergency Changes

- Low risk of negative impact
- High risk if not applied

Quarterly Changes

- Functional enhancement
- High Risk

Program Elements

- Configuration Management
  - Inventory of all hardware and software including versions
  - List of ports and services used by system (attack surface)
- Backup/Archive
  - Process to backup prior to patching
- Incident Response
- Disaster Recovery Plan
  - Recovery plan if patch fails
- Unit Patching Operations
- Patch Management Plan

Patch Management Plan - Workflow

- Vulnerability Monitoring
- Vendor Patch Monitoring
- Risk Assessment
- Vulnerability Mitigation Planning
- Mitigation Deployment
- Patch Testing
- Patch Release for Deployment
- Patch Scheduling
- Patch Deployment
- Patch Validation and Monitoring
- Patch Removal
- Patch Program Tracking and Auditing

Risk Assessment and Mitigation

- Catalog vulnerabilities
- Determine risk to system of vulnerability
  - Include analysis of defenses already in place
- Determine risk of patch to system
- Prioritize risks and identify mitigations
  - Should only be required for high risk items
- Deploy mitigations

Patch Testing and Deployment

- Test all patches prior to deploying on production systems
  - Many vendors test their vendors patches
    - Microsoft security updates qualified by most vendors
  - Use a test system if one is available
  - Use a system not currently being used for production
  - If no test system available deploy to engineering portion of system
- Determine impact to system
  - Identify and resolve issues
- Prepare patch for deployment if steps are necessary

Patch Scheduling and Deployment

- Schedule patch for deployment
  - Inform production system managers of patch requirement
- Deploy patch through patch servers
  - Patch servers located in Process DMZ
  - Patch servers should not be internet accessible
- Monitor deployment progress
  - Audit installation of patches onto all systems

Patch Removal

- Process in place to deal with patches that impact system performance
- Uninstall process for patch should be part of patch testing
  - Uninstall may mean system restore

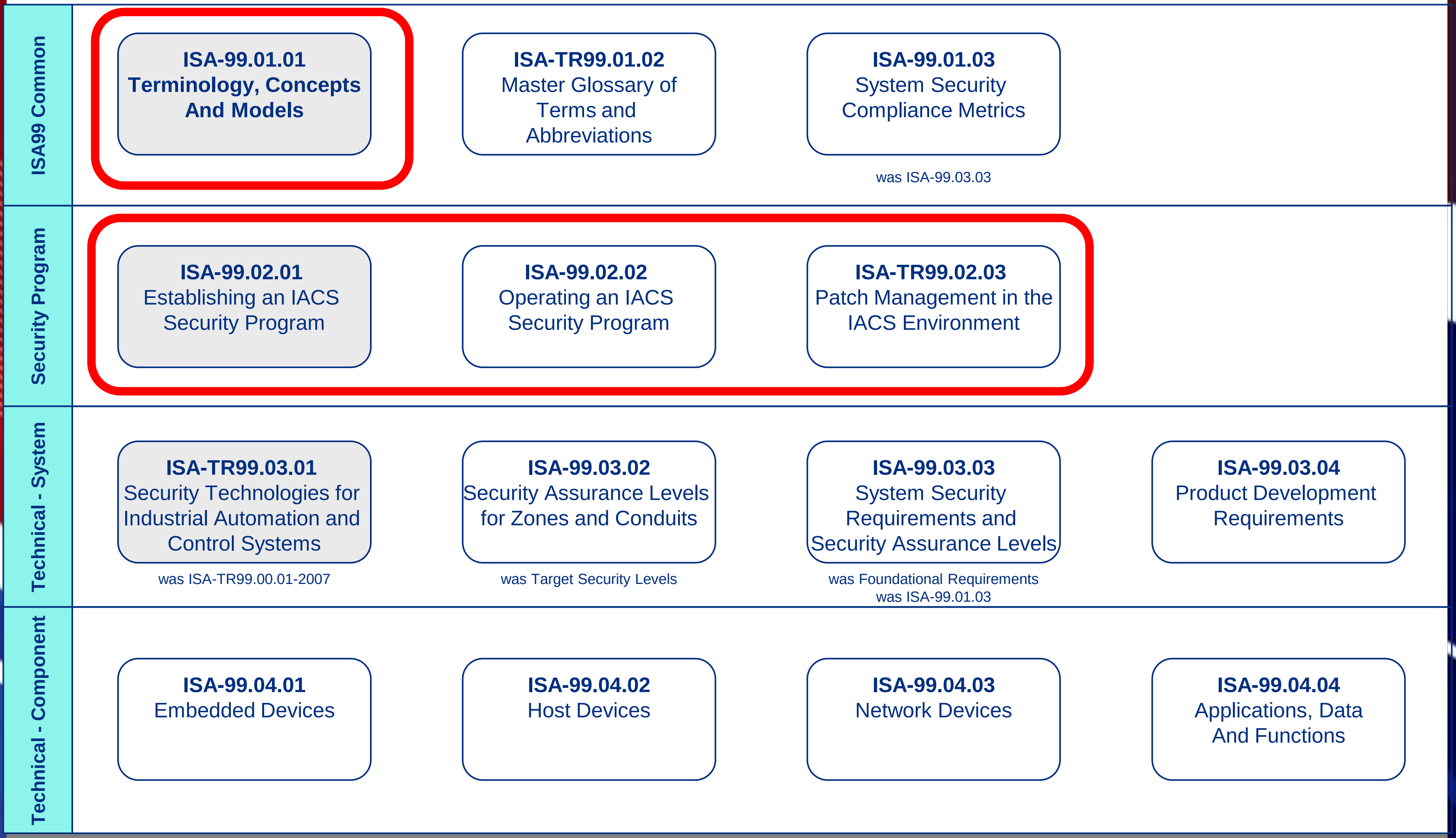
Patch Program Tracking and Auditing

- Patch compliance monitoring
  - Assure patches are installed on all systems in a timely manner
- Use patch tools that provide audit capability
  - e.g., Microsoft WSUS

Topics

- What is patch management?
- Why is patch management important?
- The need for a Control Systems focus
- Elements of a patch management program
- The ISA99 contribution

The ISA99 Perspective



ISA99 Common	**ISA-99.01.01** **Terminology, Concepts And Models**	**ISA-TR99.01.02** Master Glossary of Terms and Abbreviations	**ISA-99.01.03** System Security Compliance Metrics was ISA-99.03.03	
Security Program	**ISA-99.02.01** Establishing an IACS Security Program	**ISA-99.02.02** Operating an IACS Security Program	**ISA-TR99.02.03** Patch Management in the IACS Environment	
Technical - System	**ISA-TR99.03.01** Security Technologies for Industrial Automation and Control Systems was ISA-TR99.00.01-2007	**ISA-99.03.02** Security Assurance Levels for Zones and Conduits was Target Security Levels	**ISA-99.03.03** System Security Requirements and Security Assurance Levels was Foundational Requirements was ISA-99.01.03	**ISA-99.03.04** Product Development Requirements
Technical - Component	**ISA-99.04.01** Embedded Devices	**ISA-99.04.02** Host Devices	**ISA-99.04.03** Network Devices	**ISA-99.04.04** Applications, Data And Functions

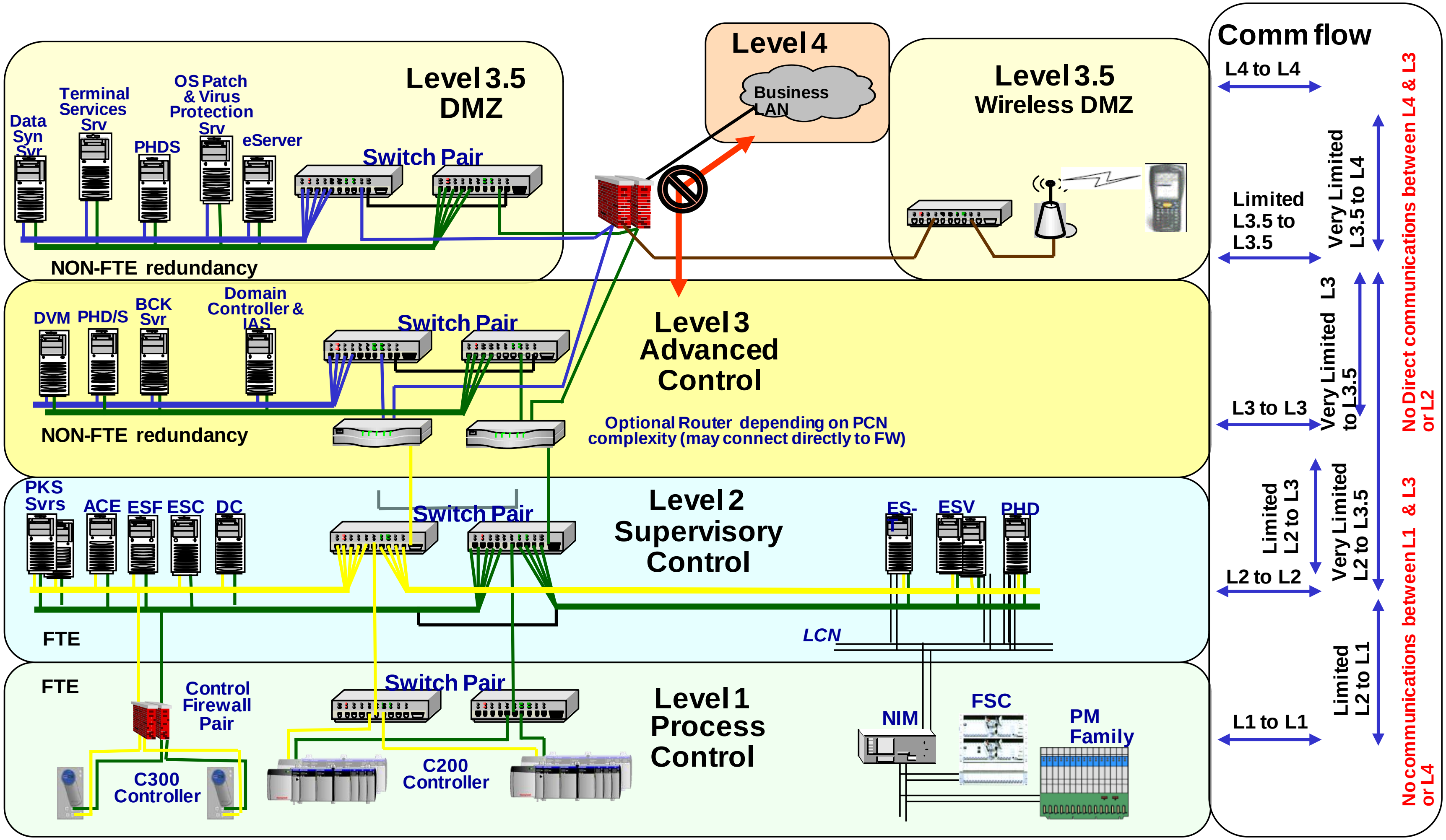
The ISA99 Perspective

- Understand and characterize your architecture using zones (See ISA-99.01.01)
- Anchor patch management as part of a broader management system (See ISA-99.02.01)
- Integrate the program with that used for business systems, but acknowledge the special needs
- Consider a consistent approach to communicating path compatibility information (Recommended practice as part of ISA-TR99.02.03)

Patch Deployment Architecture

- Architecture considerations
  - Is the control system networked?
  - Will networking add significant vulnerabilities?
  - Do non-networked systems require patching?
  - How are non-networked systems patched?
- For networked control systems
  - Locate patch servers in an isolated security zone
    - Not connected directly to the internet
      - May daisy chain from corporate patch servers
      - May communicate with vendor servers through external connection

Example Architecture Model



Summary

- Patch management is necessary for any control system
- A control system patch management plan builds on an IT patch management plan
- Work with control system vendors to assist with patch management
  - The may include a patch management service
- Good summary in the DHS *"Recommended Practice for Patch Management of Control Systems"*
- http://csrp.inl.gov/Documents/PatchManagementRecommendedPractice_Final.pdf

Questions

Eric C. Cosman

Co-Chair
ISA99 committee on control systems security
eric.cosman@gmail.com