Automation and Control

CERN openlab

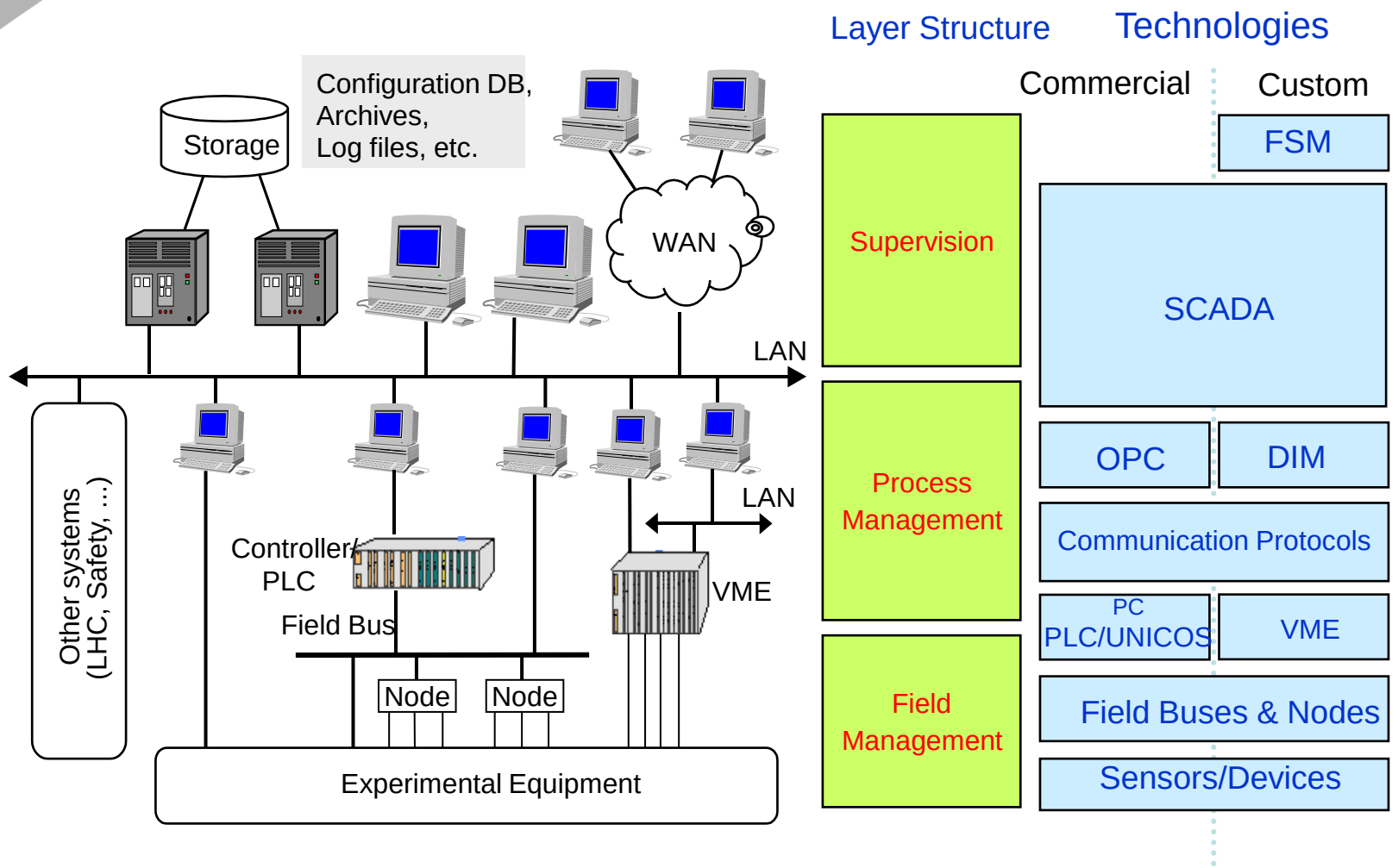
29 September 2009

Renaud BARILLERE

Outline

- Introduction
- Security and control devices
  - Openlab fellow: F. TILARO
  - CERN tech. sup.: B. COPY
- PLC IDE evolution
  - Openlab fellow:O. KHALID
  - CERN tech. sup.: M. DUTOUR
- PVSS
  - Openlab staff: D. RODRIGUES
  - Openlab fellow: I. MAGRANS
  - CERN tech. sup.: M. GONZALES

Controls architecture



Security - Background

- **Technological Evolution**:
  - Growing interconnectivity between the fabric level and the management one.
  - IT functionalities with inherent vulnerabilities into control devices.
  - No widely accepted security standard nor guidelines.
  - Effect:
    - Control Systems are exposed: recovery from attacks is expensive (time, cost, effort).
- **Objectives**
  - To improve the level of control system security.
  - Discover and Classify vulnerabilities of control system devices.

Security - Approach

- Investigate cyber security standards
- Determine key cyber security aspects relevant to CERN
- Re-assess the robustness of Siemens PLCs products
- Define and produce a test bench
  - To discover vulnerabilities
  - To develop sophisticated attacks
- Defining metrics for security evaluation

Security - Achievements I

- **WP1: Reviewing Existing Standards**
  - Analyzed industrial security standards
    - ISA-99, NERC-CIP, IEC-62
  - Identified the most relevant
    - ISA-99 is suitable for any kind of control system
- **WP2: Test bench Implementation**
  - Key requirements definition
    - Extensible, deterministic, first list of vulnerabilities
  - Tools evaluation and selection to perform attacks
    - OpenVas, Netwox & Netwag, NMap
  - Test bench implementation and validation against:
    - S7-300, S7-400, S7-1200 PLCs
    - Non-Siemens third party control devices

Security - Achievements II

- WP3: Security Evaluation
  - Design of an advanced PLCs Monitoring Service
    - Configuration of the open-source “Cacti” SNMP server
    - Implementation of a traffic monitor using open source library
  - Usage of available libraries:
    - To monitor and discover vulnerabilities
    - JMatic Library used to control and circumvent security features
  - Preliminary results found on new S7-1200 and old S7-300
    - Return to Siemens as inputs to new qualification tests
- WP4: Test bench improvements
  - Sophisticated attacks search findings:
    - “Fuzzing” is a technique used to discover weaknesses in protocol implementations
    - Selected “Peach Fuzzer” for next phase

Security - On going activities

- WP2: Test bench Implementation
  - Perform further S7-1200 PLC security evaluations
- WP3: Security Evaluation
  - Upgrade test bench architecture components
  - Improving the PLC monitoring framework in order to detect a finer granularity of vulnerabilities
  - Monitor the CPU activity for loss of control
  - Perform CERN risk analysis
- WP4: Test bench Improvements
  - Testing and Analysis of Wurldtech Achilles Satellite
  - Comparison with other general vulnerability Assessment tools
  - Effectiveness against S7-400 (not only S7-300 and S7-1200)

Extract the maximum knowledge and benefits from Achilles

Security - Project Plan Overview

- WP 1: Review existing standards

  Expected End Date: October 2009

- WP 2: Test bench Implementation

Expected End Date: November 2009

- WP 3: Security Evaluation

Expected End Date: December 2009

- WP 4: Test bench Improvements

Expected End Date: on-going

- WP 5: Future milestones

Expected End Date: (waiting for S7-1500)

Step7 - Background

- Aim: To bring-in modern software engineering capabilities to Step7 product line. Divided in to 2 phases:
  - Step7 “Automated Deployment”
    - To automate the deploy Siemens software (Step7 initially) on a group of machines
    - Scalability: from small (10’s of machines) to large (100’s of machines)
    - Easy and flexible to deploy, fast refresh rate
  - Step7 “Openness”
    - Source code versioning control
    - Syntax highlighting
    - Automatic code generators

Step7 - Approach

- Siemens decided to focus on “Deployment” only in the first phase of the project.
- Work packages (WP) and deliverables
  - in Mar 09 when the project started in consultations with Siemens
- Steps:
  - To evaluate available deployment tools in the market
  - Understanding PLC user practices and Step7 deployment use cases at CERN
  - Analysis of Siemens installation framework (SIA)
  - Design, Implementation and Feasibility study of the proposal
  - Validation at CERN and handing over to Siemens

Step7 - Achievements

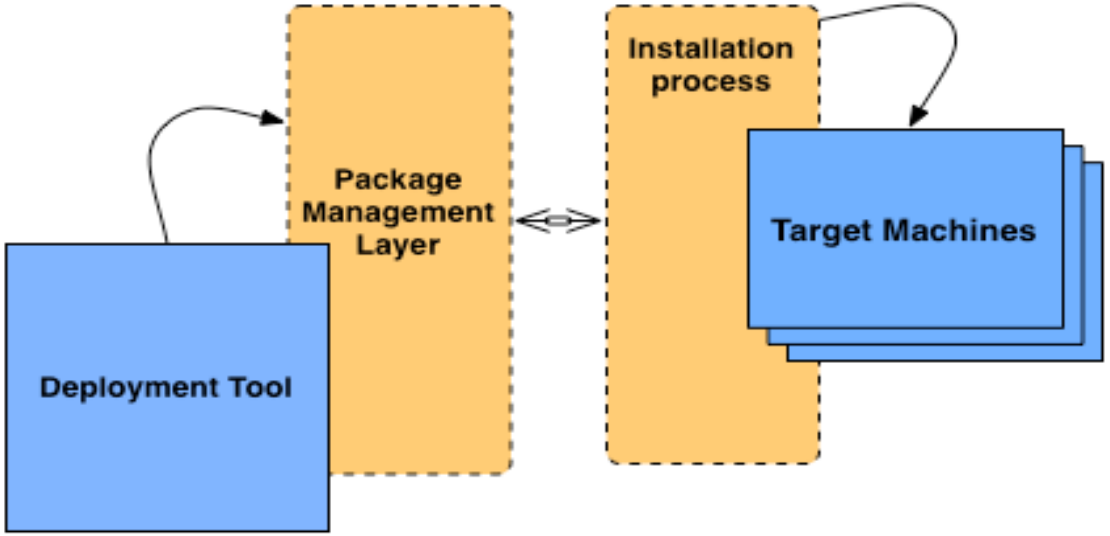
- Market Survey — Completed (May09)
  - Extensive survey of the off the shelf deployment tools
    - More than 15, including CERN CMF.
  - Tools evaluated, shortlisted and selected
    - Selection metrics:
      - » scalability, deployment refresh rate, licensing
      - » MSI based packaging and deployment was selected for evaluation for Siemens Installer Framework.
  - License purchased for CFEngine for feasibility study
- PLC/Step7 Survey — Completed (Jun09)
  - Focusing only on installation and deployment
    - Targeting PLC and Step7 users and developers
  - Results / User wish list:
    - Silent installation, automation of deployment, client-server model, possible use of virtualization technology

Step7 - Quarterly Review

- Siemens – Step7 Workshop
  - Held in July 09 at CERN
  - Existing work packages results were reported, and feedback gathered
  - Intensive brainstorming sessions on:
    - Possible new ideas based on user feedback and broader trends in software development
    - Analysis of Siemens installer architecture
    - Different MSI based deployment model were proposed
      - To separate installation mechanisms from deployment on target machines
    - Agreement on two MSI approaches:
      - Using MSI wrappers for legacy application
        - » since stability is a key requirement
      - Migrating most of installer capabilities to MSI packages

Step7 - Proposed Architecture

- Currently:
  - Installation is done through stand-alone executable
- Proposal:
  - Separation of installation from deployment process to migrate towards MSI based packaging model for the software

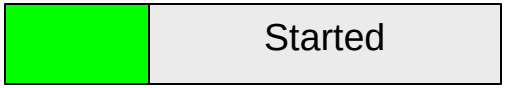


Step7 - On going activities

- **WP 3: SW Design – Use cases**

  - Use cases identified and documented
    - e.g. clean installation, repair and update existing packages

- **WP 4: SW Design – Architecture**



  - Completed first draft of design document
  - Continuing expanding towards MSI model
  - Interfacing directly with Siemens developers

- **WP 5: Feasibility Study**

  - Developing prototype MSI packages for SIA installer to validate design ideas:
    - Separate set of packages for legacy versions of Step7
    - Management of migratory path future installer packages
      - To be compliant for large number of software deployment tools

Step7 - Bird's Eyeview

- WP1: Review current status — Completed
  Completion Date: June 2009
- WP2: Market Survey — Completed
  Completion Date: May 2009
- WP3: SW Design: Use cases — Started
  Expected End Date: Sep 2009
- WP4: SW Design: Architecture — Started
  Expected End Date: Oct 2009
- WP5: Feasibility Study — Started
  Expected End Date: on-going

PVSS - Overview

- First defined activities
  - SVN plugin
  - Installation Tool
  - Oracle Archiver
  - Web Plugin
- Training
  - PVSS course
  - Technical meetings on Oracle Archiver (Eisenstadt)
  - Hands on with source code

PVSS - SVN plugin

- Served as introductory task to PVSS environment
- Provides source versioning to PVSS users
  - Enhancing project management
  - Supporting concurrent development
- Based on existing CVS plugin, using Ctrl
- Prototype was made available
- Several improvements already identified
  - Under development
- On hold (task reprioritized)

PVSS - Installation Tool

- To facilitate the management of large PVSS Distributed Control Systems
  - More than 150 PVSS applications in a large LHC experiment DCS
- Work done:
  - Requirements and use cases document sent to ETM for discussion
  - Survey of related technologies
    - Analysis of constraint based technologies
    - Survey of existing configuration management tools able to manage PVSS control systems
- Training and hands on activities:
  - Helping to support the CERN Installation Tool

PVSS - Oracle Archiver 1/2

- Improvement of reliability and stability
  - Major issues were identified by users affecting the Oracle Archiver
  - Openlab permitted to closely follow the issues directly on a production environment
  - Patch 41 released with major contributions and input from Openlab
  - Several critical bugs affecting both CERN and other ETM clients were fixed within this activity scope
- Additional objectives
  - Getting introduced to ETM workspace
  - first look into the oracle archiver potentially permitting identification of redesign needs
- Tasks completed

PVSS - Oracle Archiver 2/2

- Redesign of the Oracle Archiver
  - Code redesign is necessary
    - Current code built around a specific request
    - Not easy to add features/extensions
    - Difficulties in tracing issues
  - Working on reliability and stability permitted understanding of the current limitations on Oracle Archiver
  - Task on hold, waiting Siemens input.

PVSS – Conclusion

- Focus on training
  - As PVSS Users
  - As PVSS developers
  - Conditions for the development at CERN.
- Results for users
  - While learning
  - Benefit not limited to CERN users
- SVN and ORACLER WPs are well advanced
- Web Plug-in WP is just started.