Automation and Control

CERN openlab

28 January 2010

Outline

- PVSS
  - Openlab staff: D. RODRIGUES
  - Openlab fellow: I. MAGRANS
  - CERN tech. sup.: M. GONZALES
- 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

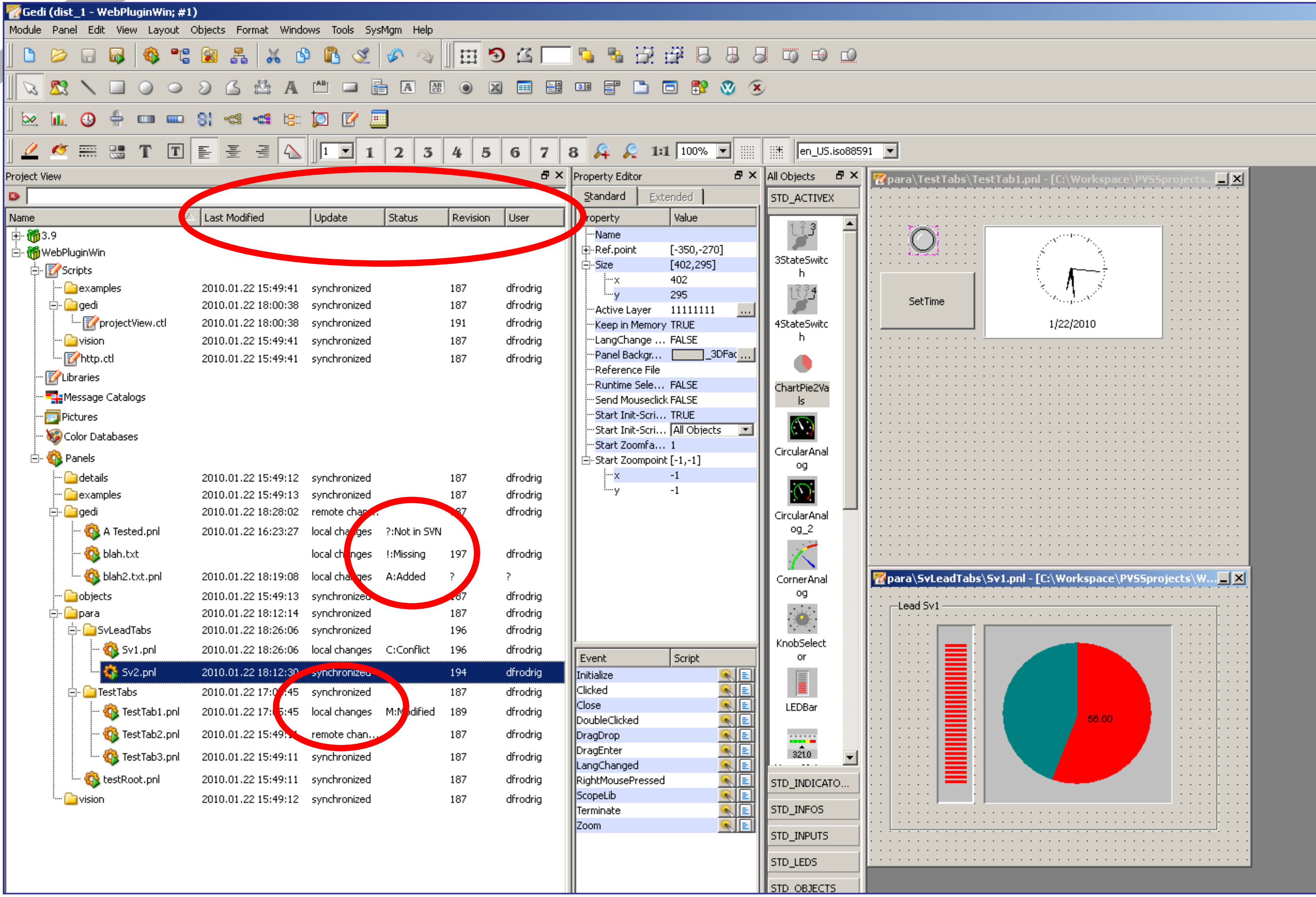
PVSS

- Development Environment
  - SVN plugin
- Installation Tool
  - PVSS Version Reporting Tool
- Web Access
  - Web plugin
- Conclusion

SVN plugin

- Development of a PVSS SVN plugin
  - Goals
    - Provide a gui integrated version control system
    - Improve the development environment and process
    - Based on the previous existing CVS plugin
  - Results
    - A first version is ready to be delivered
    - All information from SVN status available
    - Suitable for ‘standard’ subversion use cycle (add/commit/update/delete)
  - Next Steps
    - Also on the PVSS interface
      - Project wide import/checkout
      - Graphical conflict solving

SVN plugin

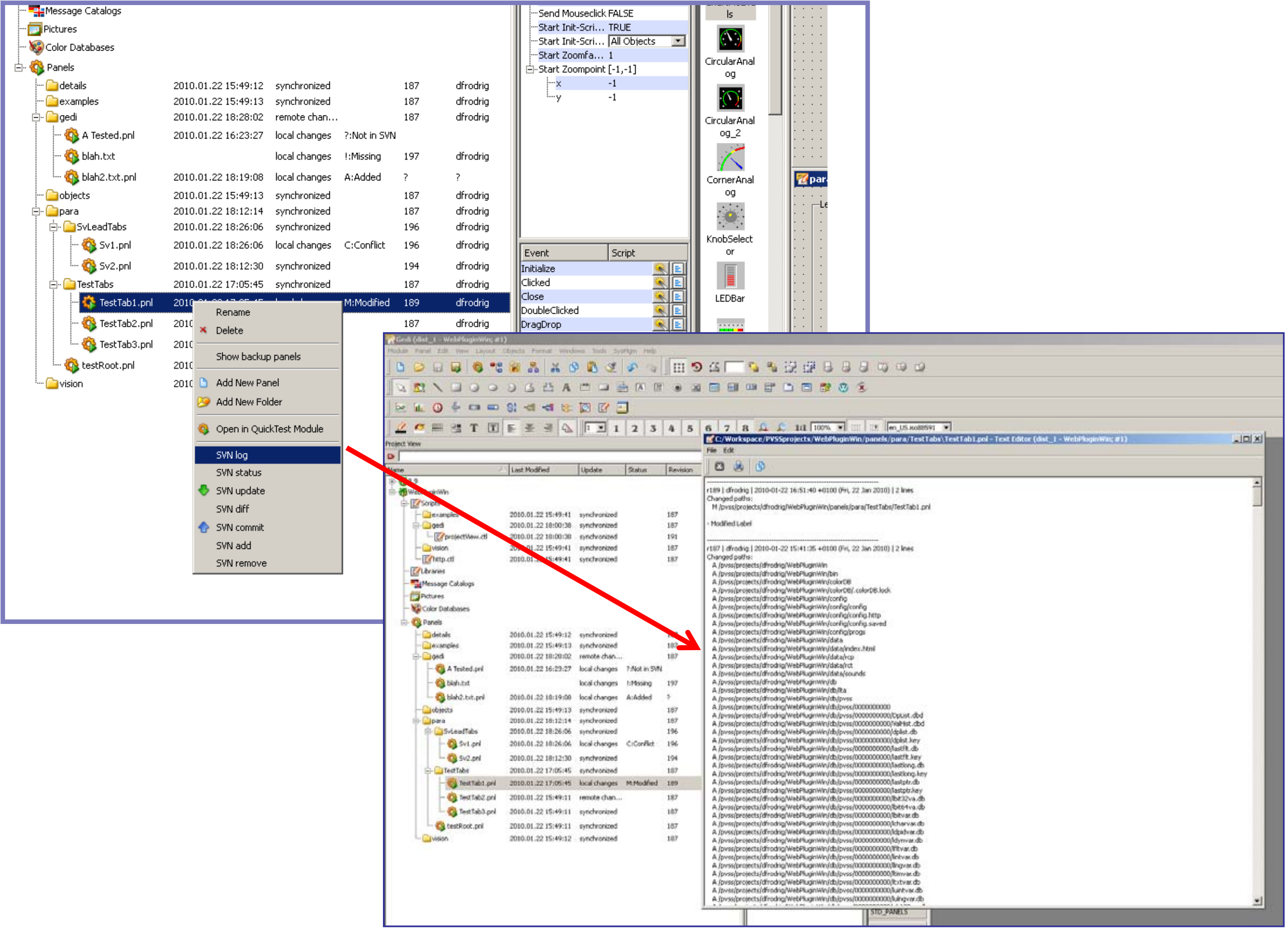


Name	Last Modified	Update	Status	Revision	User
3.9					
WebPluginWin					
Scripts					
examples	2010.01.22 15:49:41	synchronized		187	dfrodrig
gedi	2010.01.22 18:00:38	synchronized		187	dfrodrig
projectView.ctl	2010.01.22 18:00:38	synchronized		191	dfrodrig
vision	2010.01.22 15:49:41	synchronized		187	dfrodrig
http.ctl	2010.01.22 15:49:41	synchronized		187	dfrodrig
Libraries					
Message Catalogs					
Pictures					
Color Databases					
Panels					
details	2010.01.22 15:49:12	synchronized		187	dfrodrig
examples	2010.01.22 15:49:13	synchronized		187	dfrodrig
gedi	2010.01.22 18:28:02	remote chan...		187	dfrodrig
A Tested.pnl	2010.01.22 16:23:27	local changes	?:Not in SVN		
blah.txt		local changes	!:Missing	197	dfrodrig
blah2.txt.pnl	2010.01.22 18:19:08	local changes	A:Added	?	?
objects	2010.01.22 15:49:13	synchronized		187	dfrodrig
para	2010.01.22 18:12:14	synchronized		187	dfrodrig
SvLeadTabs	2010.01.22 18:26:06	synchronized		196	dfrodrig
Sv1.pnl	2010.01.22 18:26:06	local changes	C:Conflict	196	dfrodrig
Sv2.pnl	2010.01.22 18:12:30	synchronized		194	dfrodrig
TestTabs	2010.01.22 17:0[illegible]:45	synchronized		187	dfrodrig
TestTab1.pnl	2010.01.22 17:[illegible]5:45	local changes	M:Modified	189	dfrodrig
TestTab2.pnl	2010.01.22 15:49:[illegible]	remote chan...		187	dfrodrig
TestTab3.pnl	2010.01.22 15:49:11	synchronized		187	dfrodrig
testRoot.pnl	2010.01.22 15:49:11	synchronized		187	dfrodrig
vision	2010.01.22 15:49:12	synchronized		187	dfrodrig

Property	Value
Name	
Ref.point	[-350,-270]
Size	[402,295]
x	402
y	295
Active Layer	11111111
Keep in Memory	TRUE
LangChange ...	FALSE
Panel Backgr...	_3DFac
Reference File	
Runtime Sele...	FALSE
Send Mouseclick	FALSE
Start Init-Scri...	TRUE
Start Init-Scri...	All Objects
Start Zoomfa...	1
Start Zoompoint	[-1,-1]
x	-1
y	-1

Event	Script
Initialize	
Clicked	
Close	
DoubleClicked	
DragDrop	
DragEnter	
LangChanged	
RightMousePressed	
ScopeLib	
Terminate	
Zoom	

SVN plugin



```
Message Catalogs
Pictures
Color Databases
Panels
  details          2010.01.22 15:49:12  synchronized                  187  dfrodrig
  examples         2010.01.22 15:49:13  synchronized                  187  dfrodrig
  gedi             2010.01.22 18:28:02  remote chan...                187  dfrodrig
    A Tested.pnl   2010.01.22 16:23:27  local changes  ?:Not in SVN
    blah.txt                            local changes  !:Missing      197  dfrodrig
    blah2.txt.pnl  2010.01.22 18:19:08  local changes  A:Added        ?    ?
  objects          2010.01.22 15:49:13  synchronized                  187  dfrodrig
  para             2010.01.22 18:12:14  synchronized                  187  dfrodrig
    SvLeadTabs     2010.01.22 18:26:06  synchronized                  196  dfrodrig
      Sv1.pnl      2010.01.22 18:26:06  local changes  C:Conflict     196  dfrodrig
      Sv2.pnl      2010.01.22 18:12:30  synchronized                  194  dfrodrig
    TestTabs       2010.01.22 17:05:45  synchronized                  187  dfrodrig
      TestTab1.pnl 2010                                M:Modified     189  dfrodrig
      TestTab2.pnl 2010                                               187  dfrodrig
      TestTab3.pnl 2010
    testRoot.pnl   2010
  vision           2010
```

```
Send Mouseclick FALSE
Start Init-Scri... TRUE
Start Init-Scri... All Objects
Start Zoomfa... 1
Start Zoompoint [-1,-1]
  x  -1
  y  -1
```

Event	Script
Initialize	
Clicked	
Close	
DoubleClicked	
DragDrop	

```
Name                  Last Modified        Update          Status        Revision
2.9
WebPluginWin
  Scripts
    examples          2010.01.22 15:49:41  synchronized                  187
    gedi              2010.01.22 18:00:38  synchronized                  187
      projectView.ctl 2010.01.22 18:00:38  synchronized                  191
    vision            2010.01.22 15:49:41  synchronized                  187
    http.ctl          2010.01.22 15:49:41  synchronized                  187
  Libraries
  Message Catalogs
  Pictures
  Color Databases
  Panels
    details           2010.01.22 15:49:12  synchronized
    examples          2010.01.22 15:49:13  synchronized                  187
    gedi              2010.01.22 18:28:02  remote chan...                187
      A Tested.pnl    2010.01.22 16:23:27  local changes   ?:Not in SVN
      blah.txt                             local changes   !:Missing     197
      blah2.txt.pnl   2010.01.22 18:19:08  local changes   A:Added       ?
    objects           2010.01.22 15:49:13  synchronized                  187
    para              2010.01.22 18:12:14  synchronized                  187
      SvLeadTabs      2010.01.22 18:26:06  synchronized                  196
        Sv1.pnl       2010.01.22 18:26:06  local changes   C:Conflict    196
        Sv2.pnl       2010.01.22 18:12:30  synchronized                  194
      TestTabs        2010.01.22 17:05:45  synchronized                  187
        TestTab1.pnl  2010.01.22 17:05:45  local changes   M:Modified    189
        TestTab2.pnl  2010.01.22 15:49:11  remote chan...                187
        TestTab3.pnl  2010.01.22 15:49:11  synchronized                  187
      testRoot.pnl    2010.01.22 15:49:11  synchronized                  187
    vision            2010.01.22 15:49:12  synchronized                  187
```

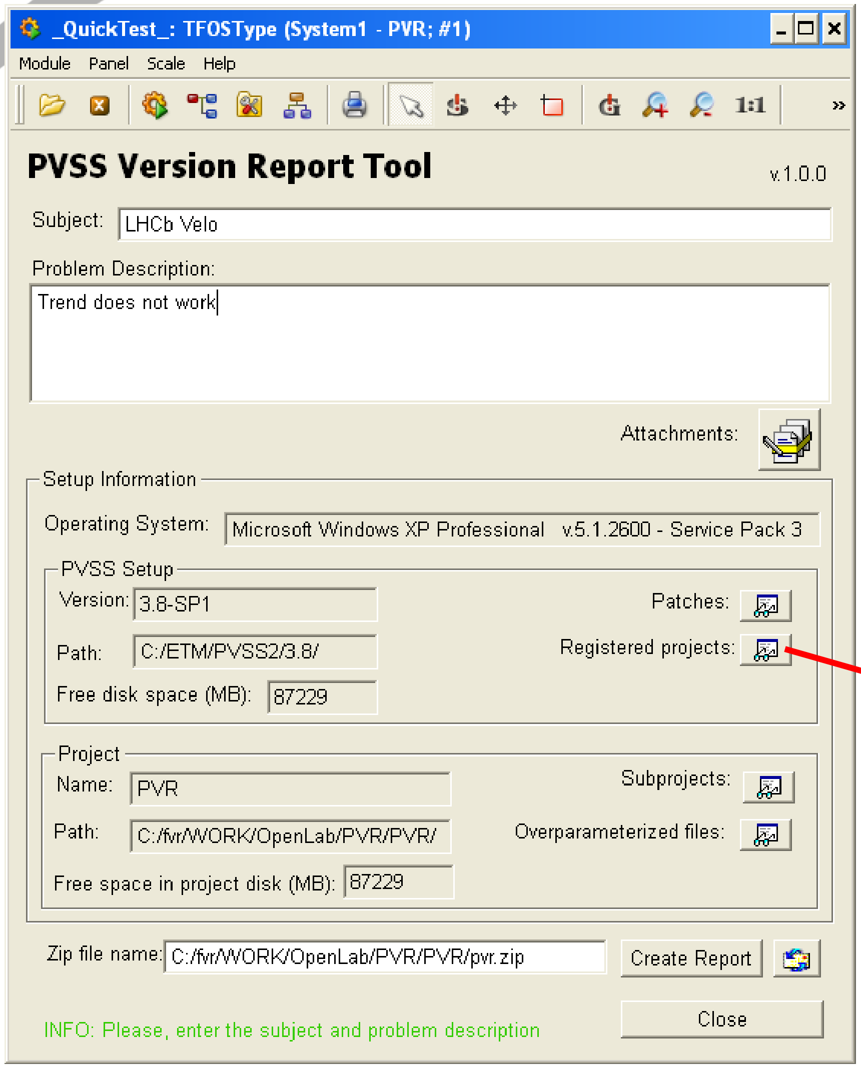
C:/Workspace/PVSSprojects/WebPluginWin/panels/para/TestTabs\TestTab1.pnl - Text Editor (dist_1 - WebPluginWin; #1)

```
------------------------------------------------------------------------
r189 | dfrodrig | 2010-01-22 16:51:40 +0100 (Fri, 22 Jan 2010) | 2 lines
Changed paths:
   M /pvss/projects/dfrodrig/WebPluginWin/panels/para/TestTabs/TestTab1.pnl

- Modified Label

------------------------------------------------------------------------
r187 | dfrodrig | 2010-01-22 15:41:35 +0100 (Fri, 22 Jan 2010) | 2 lines
Changed paths:
   A /pvss/projects/dfrodrig/WebPluginWin
   A /pvss/projects/dfrodrig/WebPluginWin/bin
   A /pvss/projects/dfrodrig/WebPluginWin/colorDB
   A /pvss/projects/dfrodrig/WebPluginWin/colorDB/.colorDB.lock
   A /pvss/projects/dfrodrig/WebPluginWin/config
   A /pvss/projects/dfrodrig/WebPluginWin/config/config
   A /pvss/projects/dfrodrig/WebPluginWin/config/config.http
   A /pvss/projects/dfrodrig/WebPluginWin/config/config.saved
   A /pvss/projects/dfrodrig/WebPluginWin/config/progs
   A /pvss/projects/dfrodrig/WebPluginWin/data
   A /pvss/projects/dfrodrig/WebPluginWin/data/index.html
   A /pvss/projects/dfrodrig/WebPluginWin/data/rcp
   A /pvss/projects/dfrodrig/WebPluginWin/data/rct
   A /pvss/projects/dfrodrig/WebPluginWin/data/sounds
   A /pvss/projects/dfrodrig/WebPluginWin/db
   A /pvss/projects/dfrodrig/WebPluginWin/db/lta
   A /pvss/projects/dfrodrig/WebPluginWin/db/pvss
   A /pvss/projects/dfrodrig/WebPluginWin/db/pvss/0000000000
   A /pvss/projects/dfrodrig/WebPluginWin/db/pvss/0000000000/DpList.dbd
   A /pvss/projects/dfrodrig/WebPluginWin/db/pvss/0000000000/ValHist.dbd
   A /pvss/projects/dfrodrig/WebPluginWin/db/pvss/0000000000/dplist.db
   A /pvss/projects/dfrodrig/WebPluginWin/db/pvss/0000000000/dplist.key
   A /pvss/projects/dfrodrig/WebPluginWin/db/pvss/0000000000/lastflt.db
   A /pvss/projects/dfrodrig/WebPluginWin/db/pvss/0000000000/lastflt.key
   A /pvss/projects/dfrodrig/WebPluginWin/db/pvss/0000000000/lastlong.db
   A /pvss/projects/dfrodrig/WebPluginWin/db/pvss/0000000000/lastlong.key
   A /pvss/projects/dfrodrig/WebPluginWin/db/pvss/0000000000/lastptr.db
   A /pvss/projects/dfrodrig/WebPluginWin/db/pvss/0000000000/lastptr.key
   A /pvss/projects/dfrodrig/WebPluginWin/db/pvss/0000000000/lbit32va.db
   A /pvss/projects/dfrodrig/WebPluginWin/db/pvss/0000000000/lbit64va.db
   A /pvss/projects/dfrodrig/WebPluginWin/db/pvss/0000000000/lbitvar.db
   A /pvss/projects/dfrodrig/WebPluginWin/db/pvss/0000000000/lcharvar.db
   A /pvss/projects/dfrodrig/WebPluginWin/db/pvss/0000000000/ldpidvar.db
   A /pvss/projects/dfrodrig/WebPluginWin/db/pvss/0000000000/ldynvar.db
   A /pvss/projects/dfrodrig/WebPluginWin/db/pvss/0000000000/lfltvar.db
   A /pvss/projects/dfrodrig/WebPluginWin/db/pvss/0000000000/lintvar.db
   A /pvss/projects/dfrodrig/WebPluginWin/db/pvss/0000000000/llngvar.db
   A /pvss/projects/dfrodrig/WebPluginWin/db/pvss/0000000000/ltimvar.db
   A /pvss/projects/dfrodrig/WebPluginWin/db/pvss/0000000000/ltxtvar.db
   A /pvss/projects/dfrodrig/WebPluginWin/db/pvss/0000000000/luintvar.db
   A /pvss/projects/dfrodrig/WebPluginWin/db/pvss/0000000000/lulngvar.db
```

Installation Tool

- PVSS version reporting tool
  - Goals
    - Improve support request response time by reducing question/answer interactions between user and support team
    - How
      - Automate the process to gather and send relevant information to solve a given support request
      - What is relevant:
        - » Host/platform (OS, service pack, Free disk space)
        - » PVSS installation (Version, AddOns, config files)
        - » PVSS project (Subprojects, config files, components)
  - Results
    - A first release was made available
    - Supports Windows and Linux
    - Compressing and e-mail sending available
    - States information on over parameterized components
  - Next Steps
    - Redundant system report
    - Work on the stability and bug fixing
    - Release a production version

PVSS Version Reporting Tool



PVSS Version Report Tool

v.1.0.0

Subject: LHCb Velo

Problem Description:
Trend does not work

Setup Information

Operating System: Microsoft Windows XP Professional v.5.1.2600 - Service Pack 3

PVSS Setup

Version: 3.8-SP1

Path: C:/ETM/PVSS2/3.8/

Free disk space (MB): 87229

Project

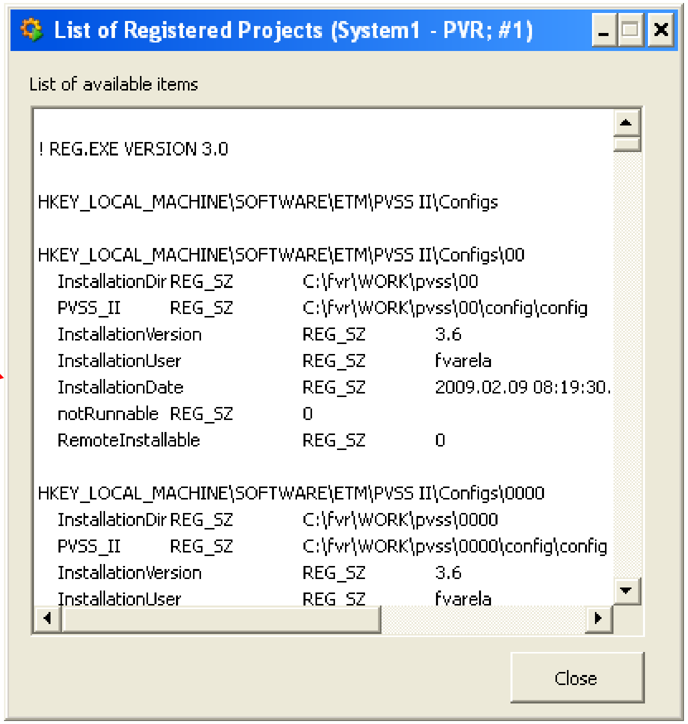
Name: PVR

Path: C:/fvr/WORK/OpenLab/PVR/PVR/

Free space in project disk (MB): 87229

Zip file name: C:/fvr/WORK/OpenLab/PVR/PVR/pvr.zip

INFO: Please, enter the subject and problem description



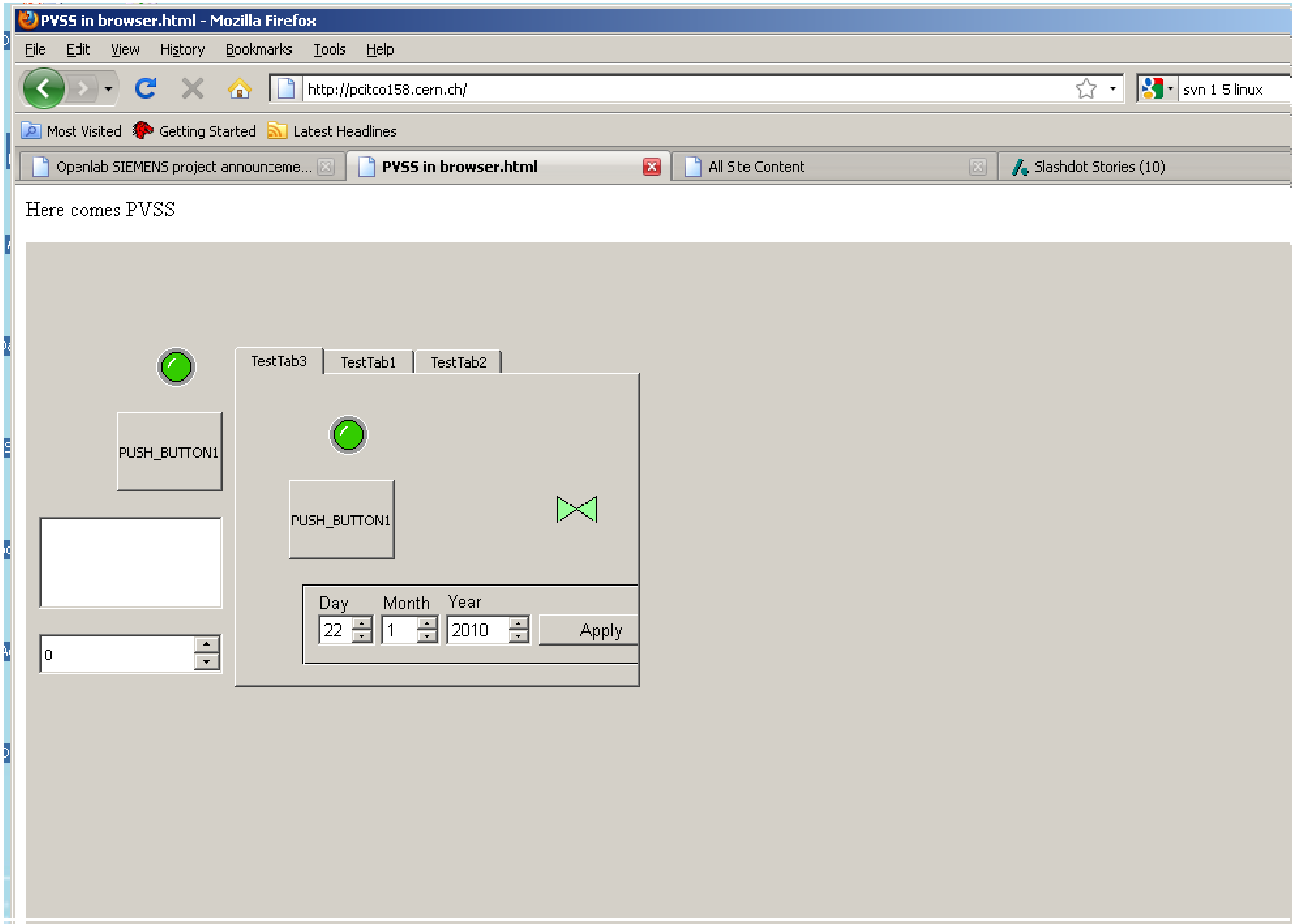
List of available items

```
! REG.EXE VERSION 3.0

HKEY_LOCAL_MACHINE\SOFTWARE\ETM\PVSS II\Configs

HKEY_LOCAL_MACHINE\SOFTWARE\ETM\PVSS II\Configs\00
    InstallationDir REG_SZ        C:\fvr\WORK\pvss\00
    PVSS_II         REG_SZ        C:\fvr\WORK\pvss\00\config\config
    InstallationVersion           REG_SZ      3.6
    InstallationUser              REG_SZ      fvarela
    InstallationDate              REG_SZ      2009.02.09 08:19:30.
    notRunnable     REG_SZ        0
    RemoteInstallable             REG_SZ      0

HKEY_LOCAL_MACHINE\SOFTWARE\ETM\PVSS II\Configs\0000
    InstallationDir REG_SZ        C:\fvr\WORK\pvss\0000
    PVSS_II         REG_SZ        C:\fvr\WORK\pvss\0000\config\config
    InstallationVersion           REG_SZ      3.6
    InstallationUser              REG_SZ      fvarela
```

Web Plugin

- ETM released a new WebPlugin
  - Goals
    - Testing the preview release on 3.9
    - Evaluate if it is adequate to CERN environment
  - Results
    - Install and Basic functionality Testing - Ok (80%)
    - Network Setup Testing - Ok (50%)
    - High Load Testing - OK (50%)
    - Plugin did well in testing
      - minor configuration issues reported back to ETM
  - Evaluation
    - WebPlugin at CERN
      - Considering the security constraints the intended use is foreseen as not possible
      - However, other uses are under evaluation

Web Plugin



Here comes PVSS

Day 22 Month 1 Year 2010

0

Conclusion

- Current project/tasks status
  - RDB Archive Manager upgrading still on hold
  - Tasks for the previous quarter focused on testing and improvements

- Achievements
  - Web Plugin
    - Testing permitted to gather information concerning usefulness to CERN
    - Some feedback to ETM
  - Subversion Plugin
    - The prototype was enhanced, debugged and documented.
  - Installation Tool
    - The PVSS Version Report Tool has been released
  - Documentation
    - An active PVSS wiki is now updated regularly

- Next steps
  - RDB Archive Manager redesign
  - Development Environment Tools
  - Web Access Enhancement

PLCs Security

Background

- **Technological Evolution**:
  - Growing interconnectivity between fabric and management
  - Introduction of IT functionalities into control devices
  - lack of security standards and guidelines
  - Effects:
    - recovery from attacks could be expensive (time, cost, effort)
- **Objectives**
  - Improve the Distributed Control System (DCS) security level
  - Discover and Classify vulnerabilities
- **Strategy**
  - Investigate cyber security standards
  - Determine key cyber security aspects relevant to CERN
  - Assess the robustness of Siemens PLCs products
  - Establish a test bench
    - To discover vulnerabilities
    - To develop sophisticated attacks
  - Defining metrics for security evaluation

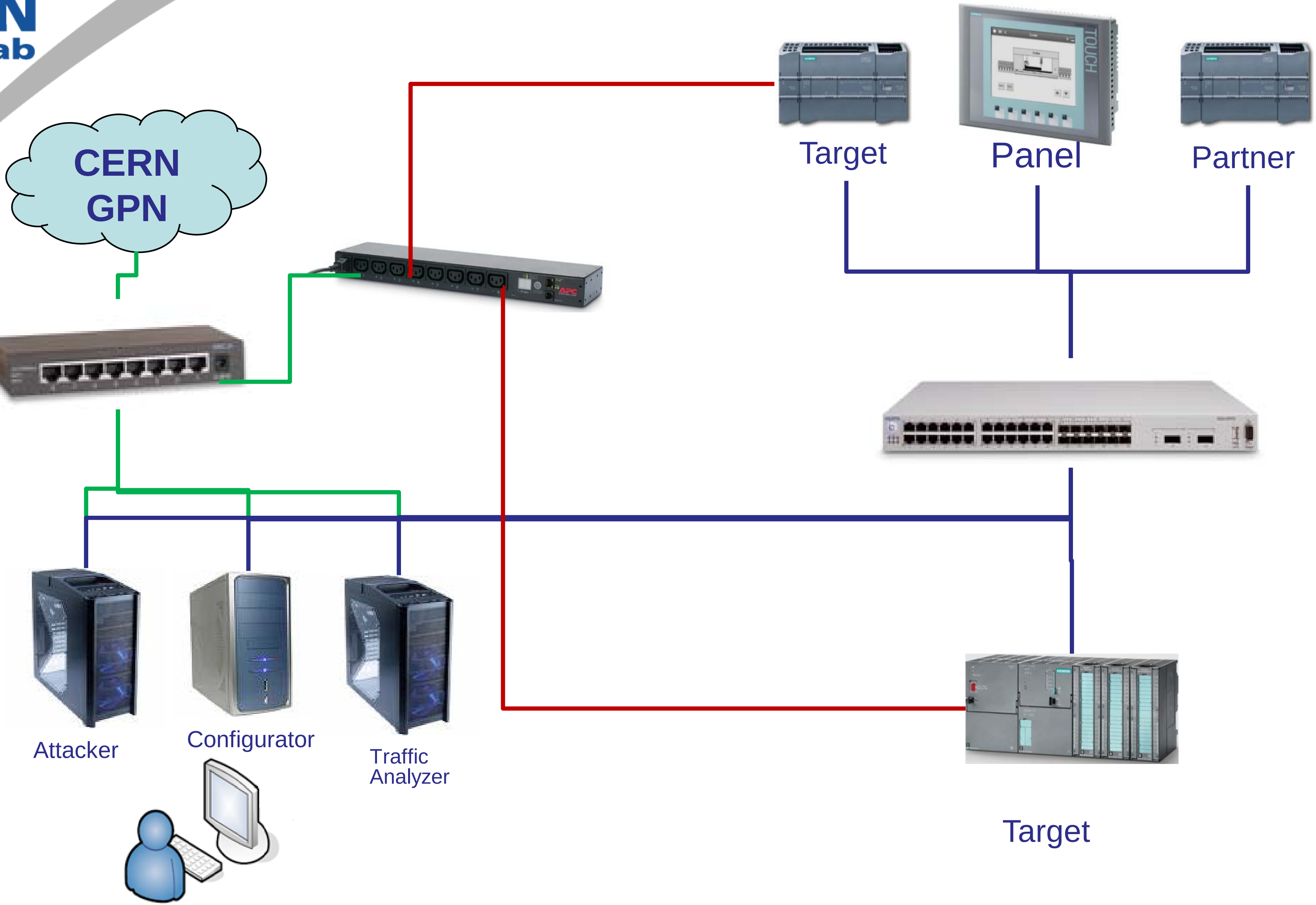
Achievements I

- **WP 3: Security evaluation**
  - SIEMENS S7-1200 ,S7-400 and S7-300 Product hardening tests
    - We identified four families of critical vulnerabilities
    - We fully documented vulnerabilities and possible cyber-security improvements
    - We developed the necessary software and procedures to reproduce the attacks in SIEMENS labs
  - Analysis of the S7-1200 authentication system
  - Siemens direct training on S7-1200 PLC and technical issues resolution

Achievements II

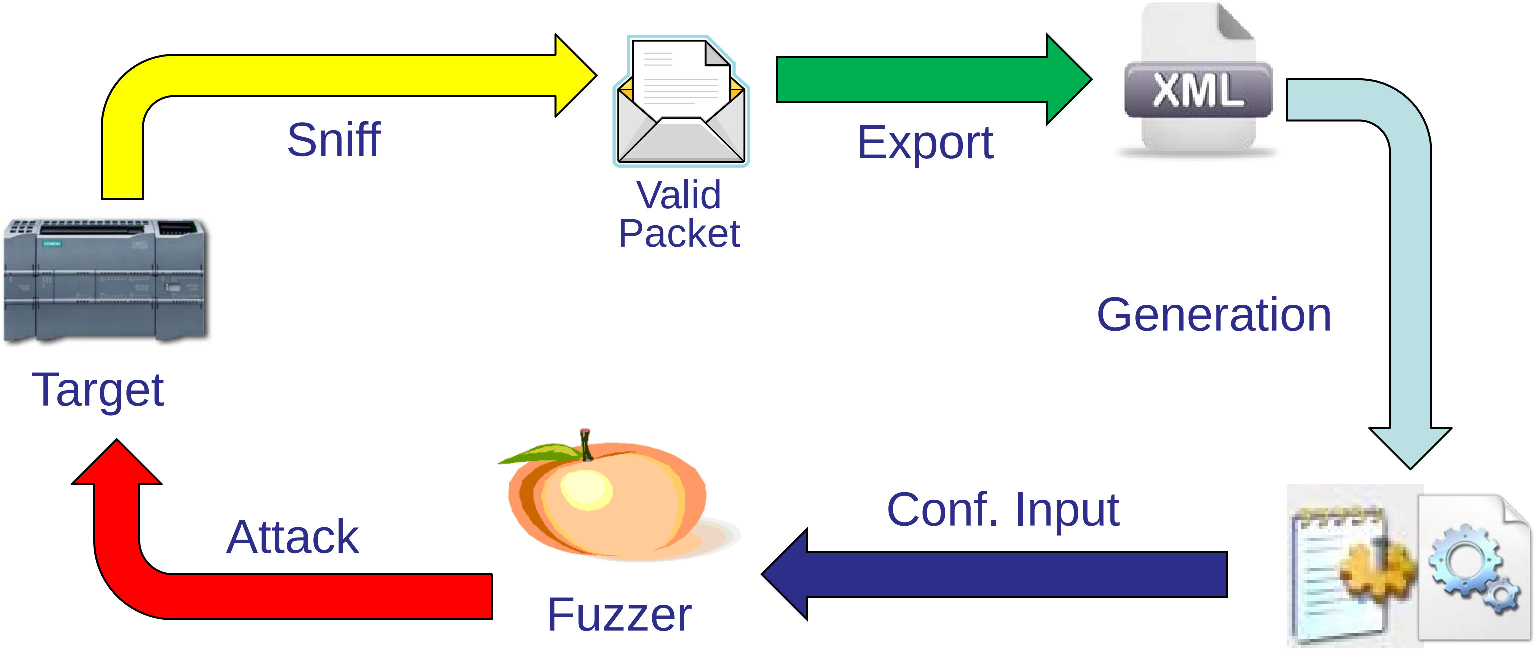
- **WP 4: Test-bench improvements**
  - Upgrade test bench architecture components
    - “Development-oriented” network architecture
  - More flexible and generic network architecture support by the introduction of new hardware components in the test-bench:
    - Physical separation between CERN and test network
    - Segmentation into VLANs
    - Concurrent tests without interferences
    - Dynamicity to add new components and create new scenarios of testing
  - Improving the PLC monitoring framework in order to detect a finer granularity of vulnerabilities:
    - Port mirroring for traffic analysis

TRoIE Network topology



Achievements III

- **WP 4: Test-bench improvements**
  - Adding a fuzzing framework to the test-bench architecture
    - Integration of the PEACH Fuzzer Framework into the test-bench architecture



Achievements IV

- **WP 5: Achilles Satellite security tests and related benefits**
  - Wurldtech Achilles Satellite Evaluation and Analysis
    - Analysis of the implemented attack techniques and their efficiency against Siemens PLCs
  - Comparison with other general vulnerability assessment tools
  - Effectiveness against Siemens PLCs
  - Extract the maximum knowledge and benefits from Achilles analysis

Overview

- WP 1: Review existing standards — Completed

  Expected End Date: October 2009

- WP 2: Test bench Implementation — Completed

  Expected End Date: November 2009

- WP 3: Security Evaluation — Completed

  Expected End Date: December 2009

- WP 4: Test bench Improvements — Completed

  Expected End Date: January 2010

- WP 5: Future milestones — Not Started

  Expected End Date: (waiting for S7-1500)

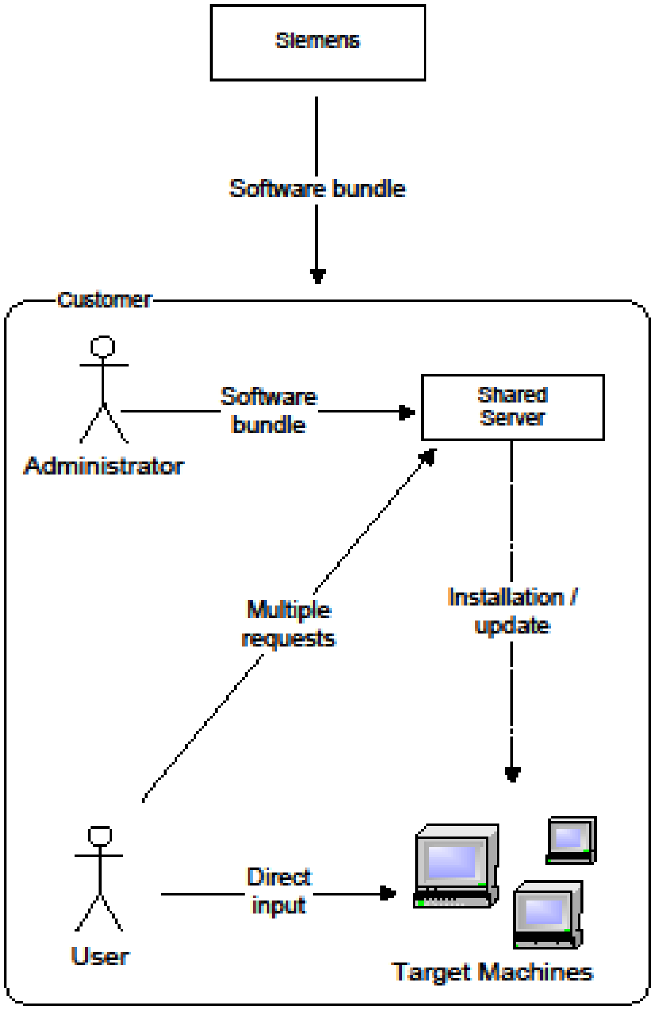
- WP 5(added): Achilles Satellite security tests and related benefits for the projects — Completed

On going activities

- WP6 – Definition of a Security Concept
- WP7 – Definition of a benchmark
- WP8 – Fuzzing support
- WP9 – Benchmark upgrades and extension
- WP10 – Testing and Reporting System
- WP11 – CERN Risk analysis

STEP7

Background



Siemens

Software bundle

Customer

Administrator

Software bundle

Shared Server

Multiple requests

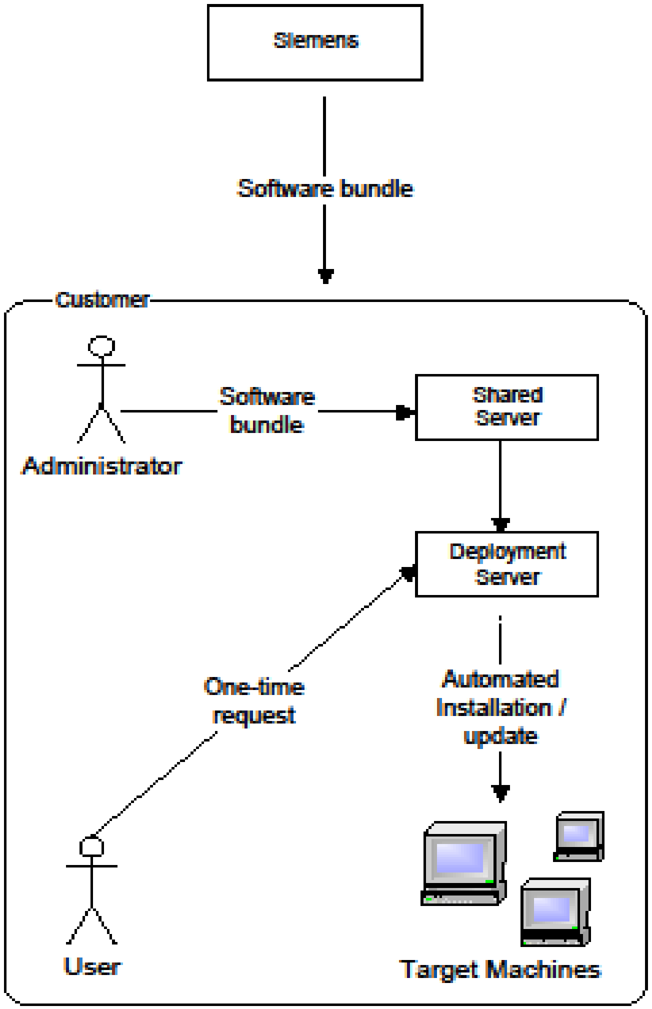
Installation / update

User

Direct input

Target Machines

No Deployment Tools



Siemens

Software bundle

Customer

Administrator

Software bundle

Shared Server

Deployment Server

One-time request

Automated Installation / update

User

Target Machines

With Deployment Tools

Overview

- WP1: Review current status

  Completed

  Completion Date: June 2009

- WP2: Market Survey

  Completed

  Completion Date: May 2009

- WP3: SW Design: Use cases

  Completed

  Completion Date: Nov 2009

- WP4: SW Design: Architecture

  Completed

  Completion Date: Nov 2009

- WP5: Feasibility Study

  Completed

  Completion Date: Nov 2009

- WP6: SIA Engine Approach

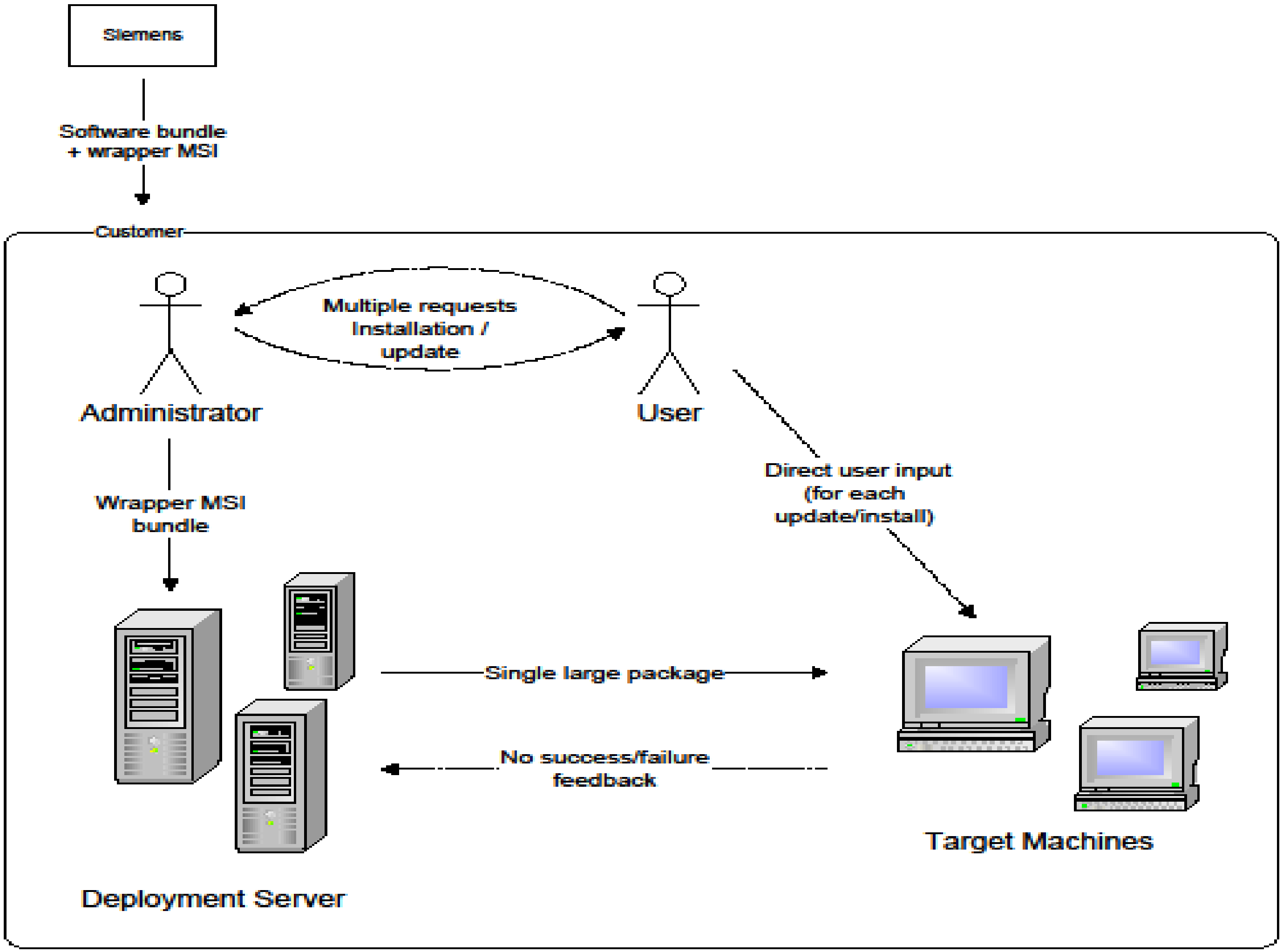
  Finalizing

  Completion date: Mar 2010

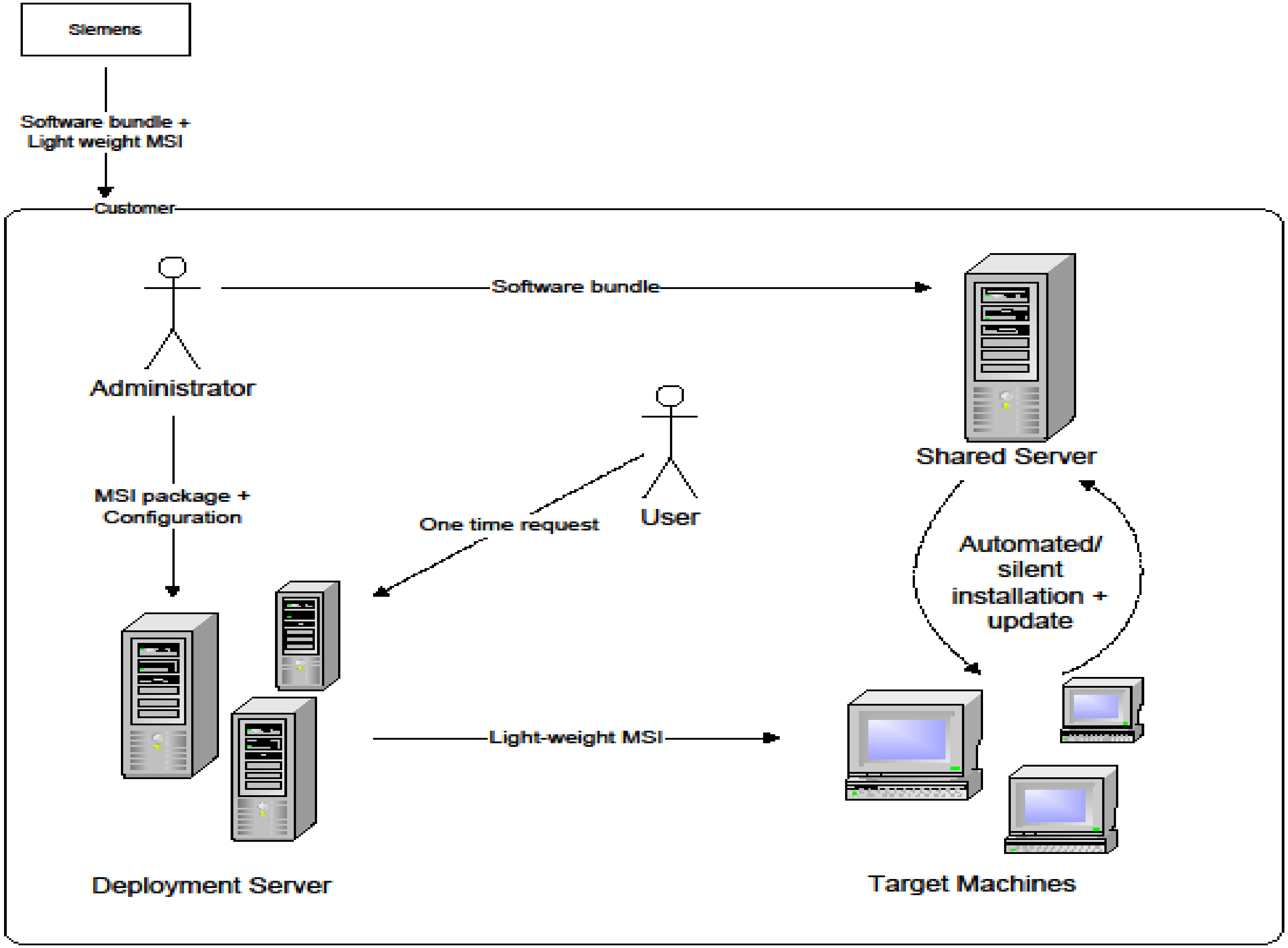
Achievements

- 3 deployment strategies developed
  - Short-term, medium-term, long-term
    - To support older and upcoming versions of Step7
  - Methodology:
    - Identify key requirements and target Step7 version
    - Develop a prototype, test and evaluate at CERN
      - Interfacing with Siemens developers
    - Document and presented results to Siemens team
  - Major evaluation metrics:
    - Diverse sets of deployment scenarios
    - Initial development cost required for Siemens
    - Flexibility and ease of integration in to various deployment tools

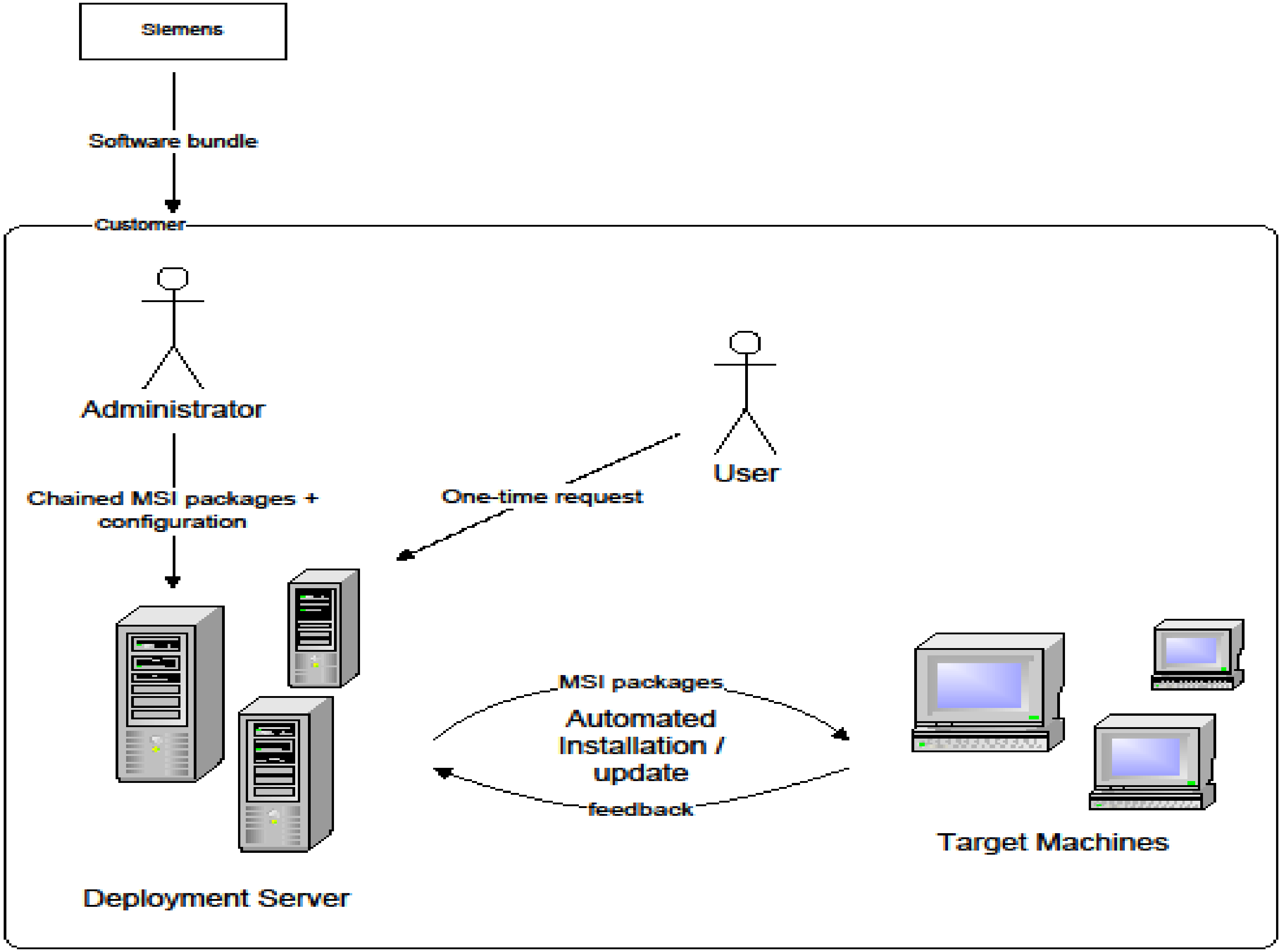
Short Term Strategy


Siemens
Software bundle + wrapper MSI
Customer
Multiple requests Installation / update
Administrator
User
Wrapper MSI bundle
Direct user input (for each update/install)
Single large package
No success/failure feedback
Deployment Server
Target Machines

Medium Term Strategy



Long Term Strategy



Conclusion

- Various approaches evaluated
  - MSI wrappers, SIA Engine, chained MSI’s
- 3 strategies identified spanning short, medium and long term
    - With clear set of goals and requirements
- Recommended:
  - Medium term approach
    - Fits very well with in Siemens existing product suite
    - Sustaining existing developments efforts in this direction
    - Strategy report already delivered to Siemens

Siemens is implementing it for v12 of Step7

Conclusion II

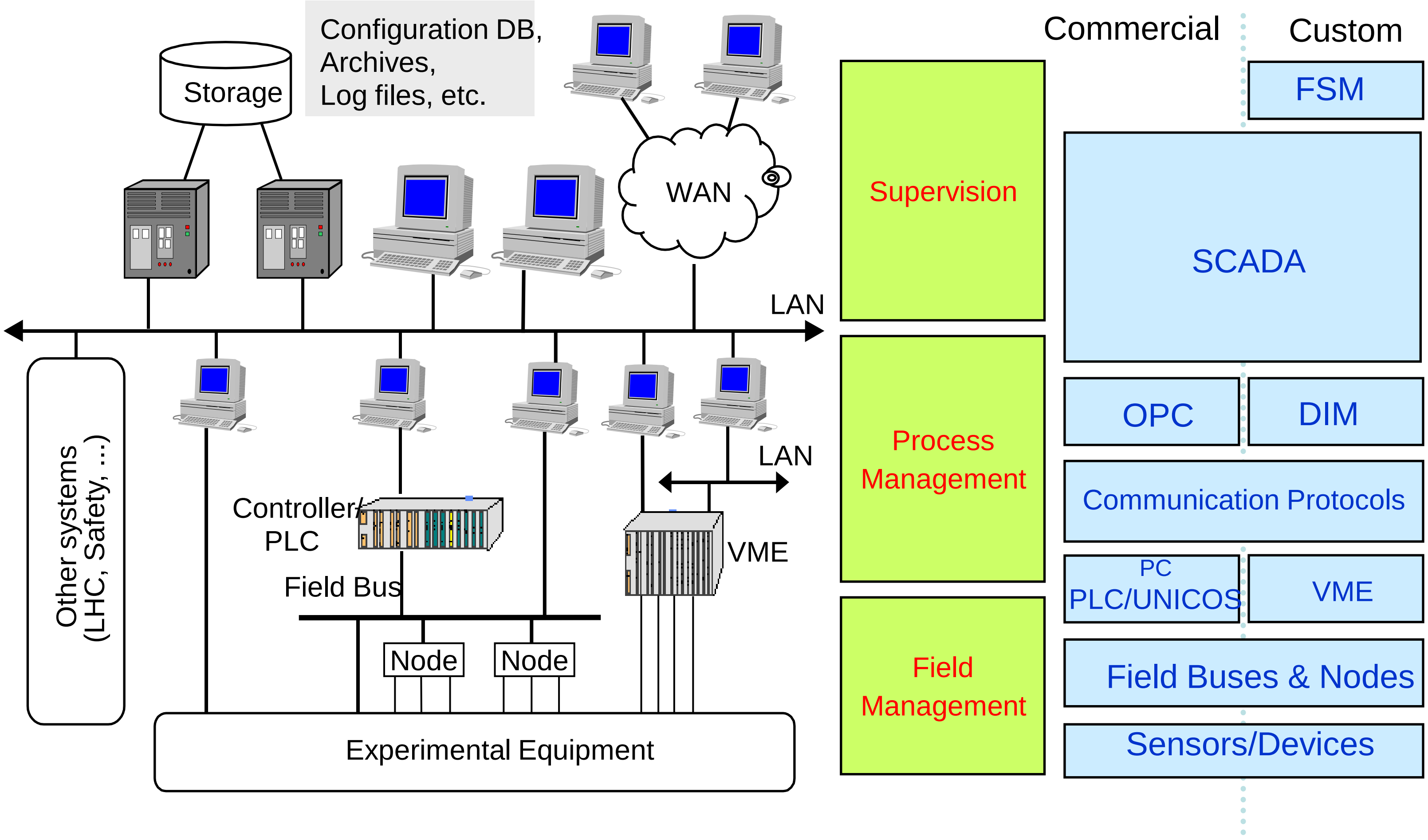
- What’s next:
  - Final evaluation of medium term strategy
    - With real SIA Engine in coming weeks
  - Starting up on “Openness” sub-project
    - Identifying new Siemens technical contact
    - Brainstorming and identifying key requirements
      - With Siemens and CERN PLC Section
    - Defining new work packages

Thank you for listening

QUESTIONS!

Support Slides

Controls architecture



Configuration DB,
Archives,
Log files, etc.
Storage
WAN
LAN
LAN
Other systems
(LHC, Safety, ...)
Controller/
PLC
Field Bus
Node
Node
VME
Experimental Equipment
Layer Structure
Technologies
Commercial
Custom
Supervision
Process
Management
Field
Management
FSM
SCADA
OPC
DIM
Communication Protocols
PC
PLC/UNICOS
VME
Field Buses & Nodes
Sensors/Devices