Siemens Openlab Major Review

October 2011

PLCs Security

Author: Filippo Tilaro

Supervised by: Brice Copy

Background

- **Objective**
  - Improve the Process Control System (PCS) security level
- **More and more discovered vulnerabilities related to PCS**
  - 2010: VxWorks and STUXNET
  - 2011: Sunway ForceControl and pNetPower, Beckhoff TwinCAT 'TCATSysSrv.exe' Network DoS, Rockwell RSLogix Overflow, Measuresoft ScadaPro, Cogent DataHub, AzeoTech DAQFactory Stack Overflow, Progea Movicon, ScadaTEC ModbusTagServer and ScadaPhone Remote Buffer Overflow, Scadatec Procyon 'Coreservice.exe' Stack Buffer Overflow, Siemens WinCC Flexible Runtime Heap Overflow, ActiveX in Advantech Broadwin WebAccess, Sunway ForceControl SCADA SHE, Control Microsystems (Schneider Electric) ClearSCADA Remote Authentication Bypass, Inductive Automation Ignition Disclosure, Siemens SIMATIC S7-300 Hardcoded Credentials, Password Protection Vulnerability in Siemens SIMATIC Controllers (S7-200,300,400,1200), Siemens SIMATIC S7-1200 PLC, Honeywell ScanServer ActiveX Control Use-After-Free
  - **Result:** loss of process control, damage propagation to critical PCSs
- **Strategy**
  - Design of a test-bench to evaluate the PCSs network robustness
  - Determine key cyber security aspects relevant to CERN

Security Standards & Certifications

- ISA-99 standards as reference standard:
  - Lack of pragmatic guidelines to secure PCSs
  - Not finished yet
- ISA-Secure Embedded Device Security Assurance Certification:
  - Based on ISA-99
  - Communication Robustness Testing(CRT): protocol-by-protocol security testing specification
- Fulfilling the ISCI-CRT requirements:
  - Integration of the CRT tests into the TRoIE test-bench developed at CERN
  - Releasing to Siemens a complete test definition set and implementation to be deployed and reproduced in Siemens Labs

PLC I/O Monitoring

- Objective: Detect any delay or anomaly in the device’s process control I/O during the phase of testing

- Precedent solution with the use of another PLC:
  - ✘ The analysis was affected by synchronization issues between the PLC under test and the monitoring one
  - ✘ Low Analysis Time Resolution, not enough to fulfill the ISCI requirements
- Current solution with a Digital Acquisition Card (DAC):
  - No synchronization issues and quite better time resolution than the previous one
  - First version has been released, but further tuning is required

Test-bench User Interface

- Main objectives:
  - Ability to run the tests against specific targets but not to change test definitions
  - Built-in or produced as a part of the TRoIE framework
  - No specific security knowledge is necessary
  - No client-side installation required
  - Client Compatibility with both Windows and Linux
  - Automated Start/Stop of tests
  - Authentication to run a test

- Achievement:
  - First implementation has been released to Siemens, but further developments are required

Next steps

- Expertise knowledge transfer to Siemens
- Custom S7-protocol and PROFINET security testing
- Multi-Protocols (Man-in-the-middle) layer testing support
- Extend the same testing strategy to the supervision level: SCADA system like PVSS, OPC-UA…

Siemens Openlab Major Review

October 2011

SCADA Security

Author: Omer Khalid

Supervised by: Renaud Barillere

Overview

- **Objective**
  - Improve the SCADA security and system robustness

- **Strategy**
  - Identifying vulnerability areas and their associated risks – including test use cases
  - Determine key cyber security aspects from CERN standpoint
  - Document and prepare SCADA security recommendations
  - Taking Siemens/ETM input
  - Evaluate risks and use cases identified, and prototype to investigate vulnerabilities

SCADA Security Analysis I

- Using ISA-99 as reference standard:
  - Taking input from U.S. Homeland Security and Swedish SCADA security guidelines
- Security Areas Analyzed:
  - Access Control
    - Password policy – strength, expiry
    - Regular review of access rights
    - Organization wide access control
  - Data Integrity and Confidentiality
    - Data protection against network attacks
    - Multiple level of data access with in access control

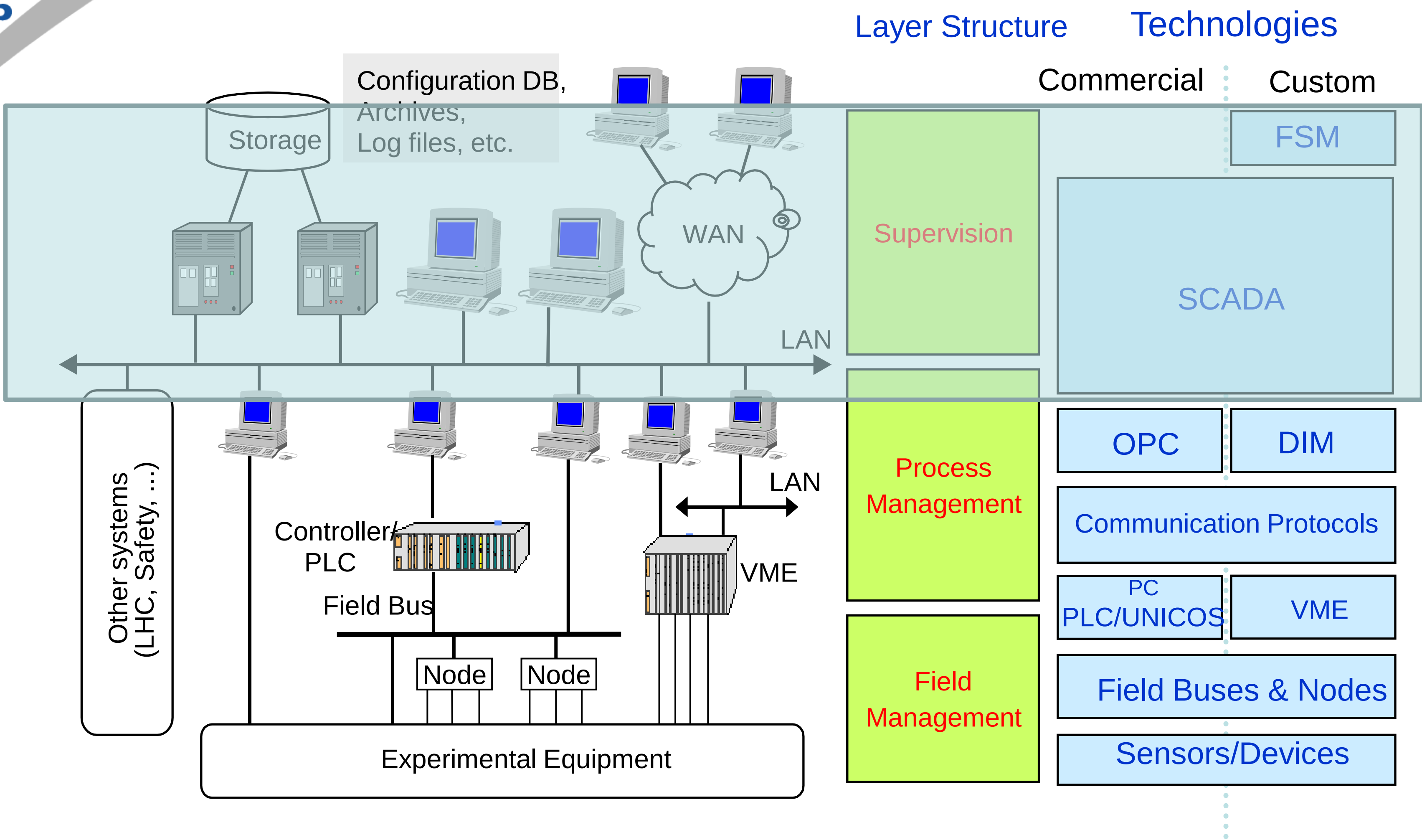
SCADA Security Analysis II

- Continued..:
  - Auditing and Logging
    - Logging all users access and events
    - Logging IP addresses of SCADA software components
  - Updating and Patching
    - Vendor certification of patches
    - Mechanisms to test patches prior to deployment
  - Network Resource Availability
    - Protections against denial of service attacks
    - Protection against data traffic sniffing attacks
- Status: SCADA recommendation document prepared and taking input from SCADA experts

Siemens Openlab Major Review

October 2011

WinCC OA (former PVSS)


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

ARCHIVING

WinCC OA

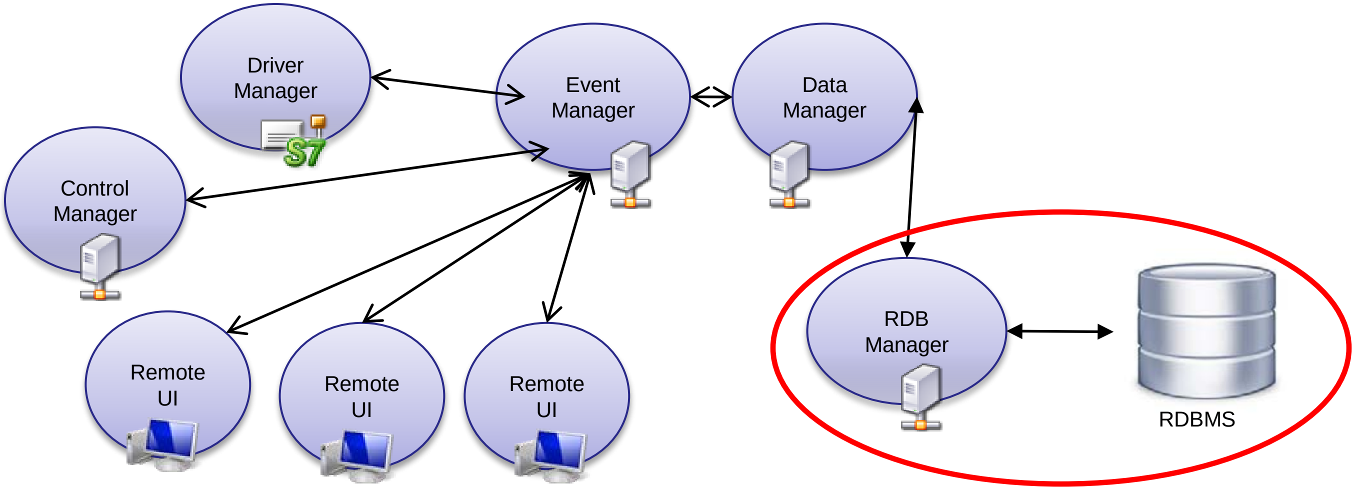
- Topics
  - WinCC OA version 4 archiving
    - Future SCADA system to be released in a few years
    - Work on a storage plug-in for Oracle RDBMS
  - WinCC OA version 3.8 archiving
    - Performance improvements
  - WinCC OA 3.10 archiving
    - Testing/validation of new functionalities

WinCC OA Version 4

- What is WinCC OA version 4
  - Upcoming SCADA system to be released within few years
  - Totally new storage and component architecture
    - Storage architecture designed not only for SCADA but all Siemens products which require archiving
  - CERN is developing an Oracle archiving module. Storage modules for other relational database products developed by ETM
  - Modules are based on the framework provided by ETM ,developed jointly by ETM and Siemens

Status - WinCC OA 4

- Last Major Review Status
  - ✓ Integration in the ETM environment
  - ✓ Most of the basic functionalities implemented and unit tested
- New development
  - 🚫 Functional tests with the WinCC OA database schema
    - New manager component developed for testing



    - Problem with the underlying framework, need to wait for ETM and Siemens
  - Performance tests pending

WinCC OA 4

- Version 4
  - Development of the Oracle storage plug-in has been put on hold until the underlying software framework is ready
  - We have involved users (experiments) and had a couple of meetings on the new architecture to make sure it suits their needs
    - We are not sure how the new archiving service will interface with WinCC OA 4 manager components

WinCC OA 3.8/3.10

- Performance improvements requested by CERN users (pending ETM’s validation)
  - Data buffering after a loss of database connection
  - Trending improvements (grouped queries)
- Planned: scalability performance tests
  - Update of previous round of tests
  - New scenarios
    - High data throughput per client
  - Up-to-date hardware/software
    - Oracle, Servers, WinCC OA, etc
  - Need to get the department IT involved

WinCC OA 3.10

- Validation of the new archive compression (data aggregation) mechanism
  - Possible to precalculate intervals (e.g. Minute, Hour, Day etc.)
  - A function is applied to a data within an interval – min/max/avg/sum...
  - Needed to speed up data retrieval over a long time period (or large data sets)
  - Aggregation handled directly by the RDBMS
    - PL/SQL, DB jobs
  - Cascading – new sets based on existing calculated sets are possible
  - Validation in progress
    - Performance issues have surfaced during tests
    - Managed to optimize database performance, but not enough
      - Tests have shown that performance is too low to calculate compressed values for 250 data point elements within a minute.
      - Even hourly compressions generate a significant CPU load
    - Changes in the implementation might be necessary

ENHANCEMENTS

- Main Activities Since the last review:
  - Testing:
    - ☑ Web Plugin : Finished
    - ☑ New Ultra Thin Client : 1st phase done
  - Development:
    - ☑ CtrlPerformanceMetrics : Delivered
    - ☑ Optimization of Installation Tool : Ongoing
  - Other:
    - ☑ Requirements for Deployment Tool : Delivered
    - ETM User’s Day : Participated
      - 12/ 13 May 2011, Ravenna, Italy
    - PVSS is now rebranded WinCC OA!
      - From version 3.10 onwards.

Testing

- Web Plugin for PVSS version 3.9
  - Previously reported results
    - Visible improvement from previous versions in performance.
    - Pros and Cons for use identified.
  - Current Status
    - Additional tests where performed, namely targeting CPU load.
    - Main conclusions:
      - Installation is easy, making it less complicated than setting up a Remote UI.
      - There are performance limitations, but the solution is suitable for its purpose, a more flexible way to access panels.
    - The full report was delivered and accepted by ETM.
    - The activity is considered to be finished.

Testing

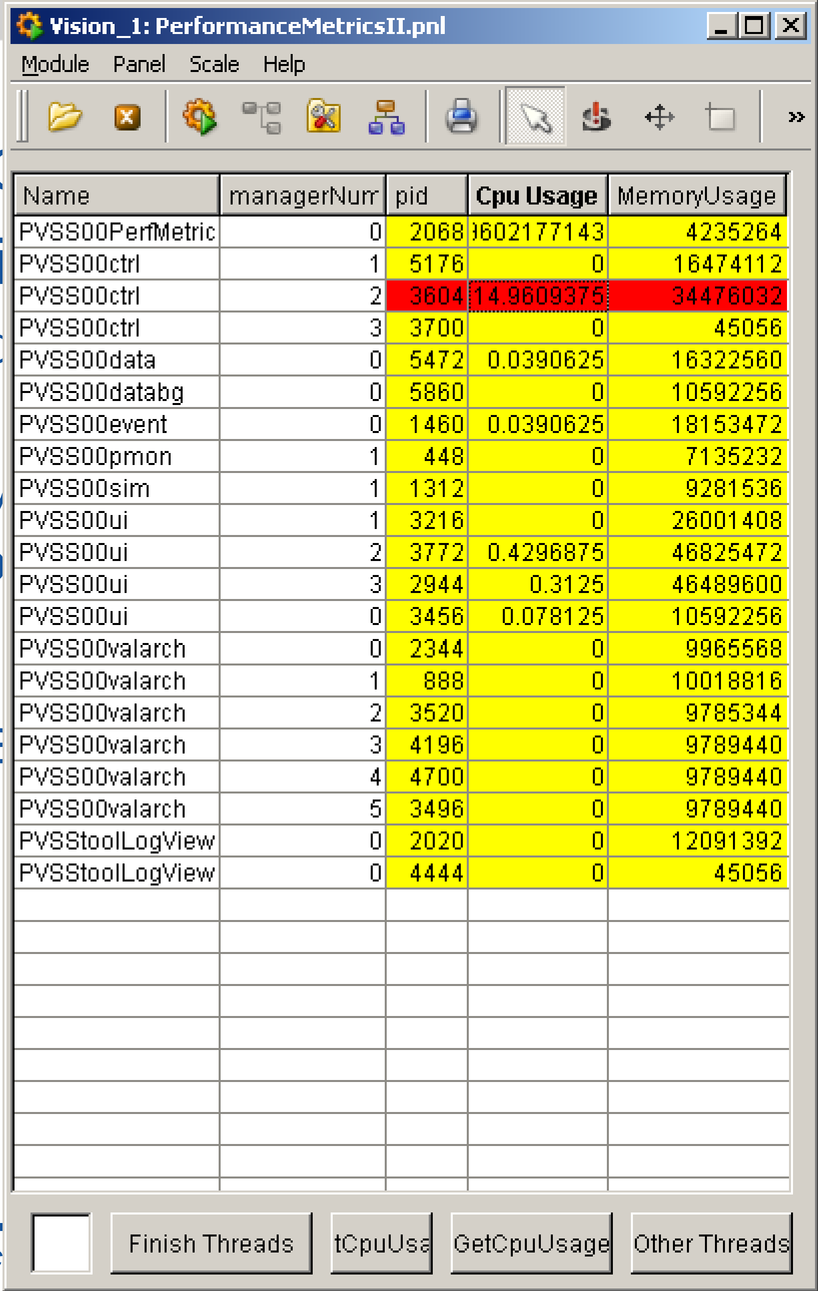
- New Ultra Thin Client
  - Delivered in WinCC OA version 3.10
  - Openlab was requested to test it

- Ultra Thin Client description
  - A "real" Web Solution
    - Based on SVG (Scalabale Vector Graphics) and JavaScript
  - Multiplexing of subscriptions on the Server
  - Offers tools for translating panels into SVG

- Testing
  - 2 phases: 1st focusing on Server performance, 2nd on client
  - First phase results were delivered and are under review:
    - Multiplexing of subscriptions are excellent news
    - Easily portable, as SVG is a Web Standard
    - Translation of panels not yet satisfactory, namely scripting

Development

- CtrlPerformanceMetric
  - Tool developed for aidi
    - Measures CpuLoad and processes
    - Puts information directly
    - Written to PVSS 3.9, po
  - ETM received the code Summer University



Name	managerNum	pid	Cpu Usage	MemoryUsage
PVSS00PerfMetric	0	2068	602177143	4235264
PVSS00ctrl	1	5176	0	16474112
PVSS00ctrl	2	3604	14.9609375	34476032
PVSS00ctrl	3	3700	0	45056
PVSS00data	0	5472	0.0390625	16322560
PVSS00databg	0	5860	0	10592256
PVSS00event	0	1460	0.0390625	18153472
PVSS00pmon	1	448	0	7135232
PVSS00sim	1	1312	0	9281536
PVSS00ui	1	3216	0	26001408
PVSS00ui	2	3772	0.4296875	46825472
PVSS00ui	3	2944	0.3125	46489600
PVSS00ui	0	3456	0.078125	10592256
PVSS00valarch	0	2344	0	9965568
PVSS00valarch	1	888	0	10018816
PVSS00valarch	2	3520	0	9785344
PVSS00valarch	3	4196	0	9789440
PVSS00valarch	4	4700	0	9789440
PVSS00valarch	5	3496	0	9789440
PVSStoolLogView	0	2020	0	12091392
PVSStoolLogView	0	4444	0	45056

Development

- CERN Installation Tool
  - Installation Tool is CERN solution to:
    - manage deployment,
    - upgrade and
    - configure PVSS projects
  - Openlab was asked to help identify possible optimizations
    - This activity is useful for better understanding how deployment is managed at CERN…
    - … and how we can develop a deployment solution at ETM.
  - The tool uses a System Configuration DB
    - Central Database updated by project agents
    - Mechanism bottlenecks were identified
    - A caching mechanism was proposed and developed
  - The optimization solution is under validation and will be applied and deployed on the next technical stop

Other

- New Deployment tool for WinCC OA
  - WinCC OA does not provide a tool for managing large project installations
  - +
  - CERN is used to manage large project installations, and developed its own tool
  - =
- Openlab is participating in the definition of the new Deployment tool for WinCC OA

- Meeting held in Eisendstadt
  - Presentation of CERN current solution
  - Discussion on possible improvements
  - Brainstorm of the requirements and specifications of the future deployment tool

- Initial requirements document provided by ETM
  - Analysis and review of the document delivered

- Openlab will be involved in prototyping components of the future solution

Other

- ETM User’s day
  - Held in Ravenna Italy, 12/13 May 2011
  - An opportunity to interact with other users
  - Highlights
    - PVSS is now Simatic WinCC Open Architecture.
    - Openlab contribution was on display, through the Version Reporting tool.
    - A lot of discussion on the future developments panel, with focus on Web Access and Deployment Mechanisms

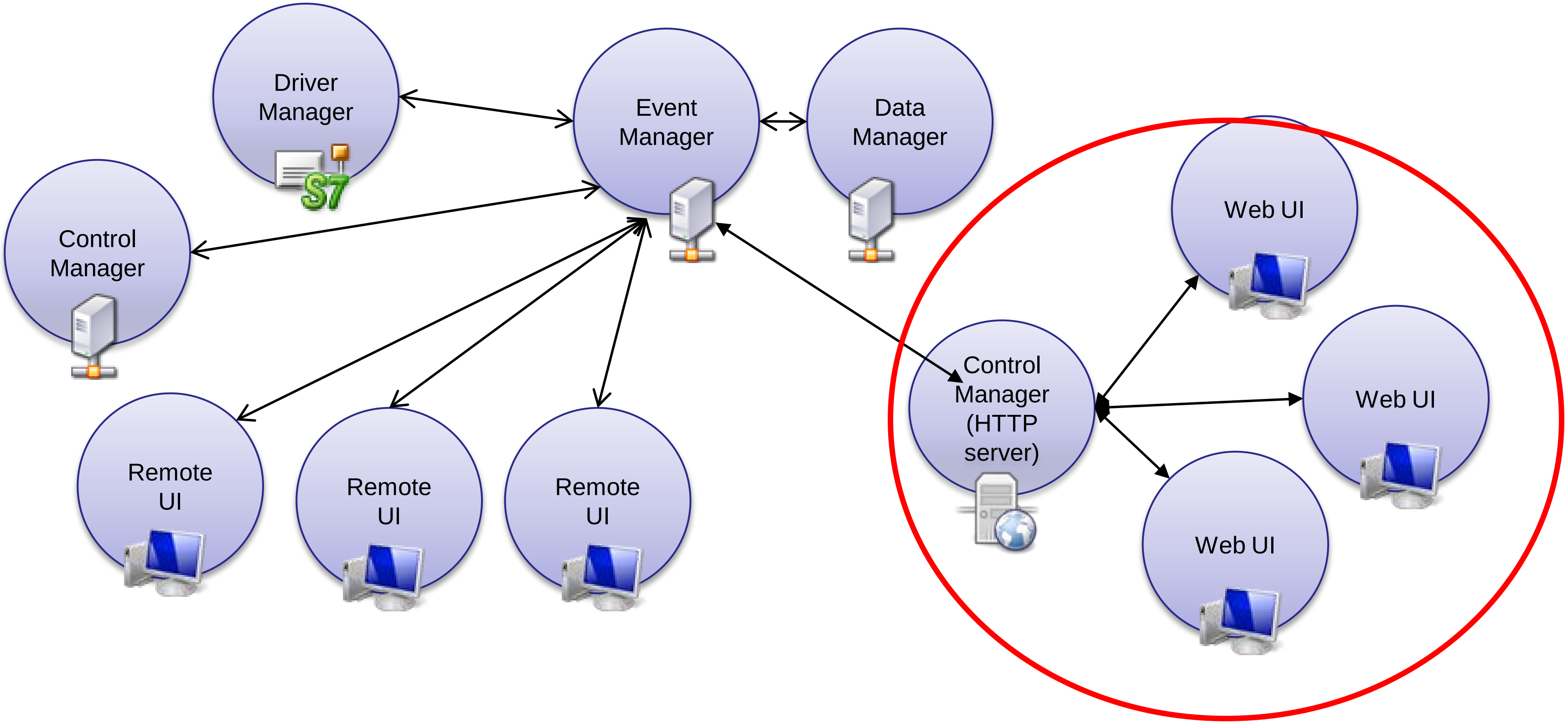
Next Steps

- Testing
  - Ultra Thin Client
    - Execute 2nd phase, focusing on client performance
- Development
  - Installation Tool Optimization
    - Validate and deliver
  - Deployment Tool
    - Participate in the next round of specifications
    - Prototype components

THANK YOU for your attention.

Support Slides

- Example of a PVSS System


Driver Manager
Event Manager
Data Manager
Control Manager
Web UI
Control Manager (HTTP server)
Web UI
Remote UI
Remote UI
Remote UI
Web UI