Siemens Openlab Major Review

September 2012

CERN openlab

Contents

- Organization
- Data Analytics
- PLCs Security
- WinCC Open Architecture
  - Database Archiver
  - Deployment Tool

Organization

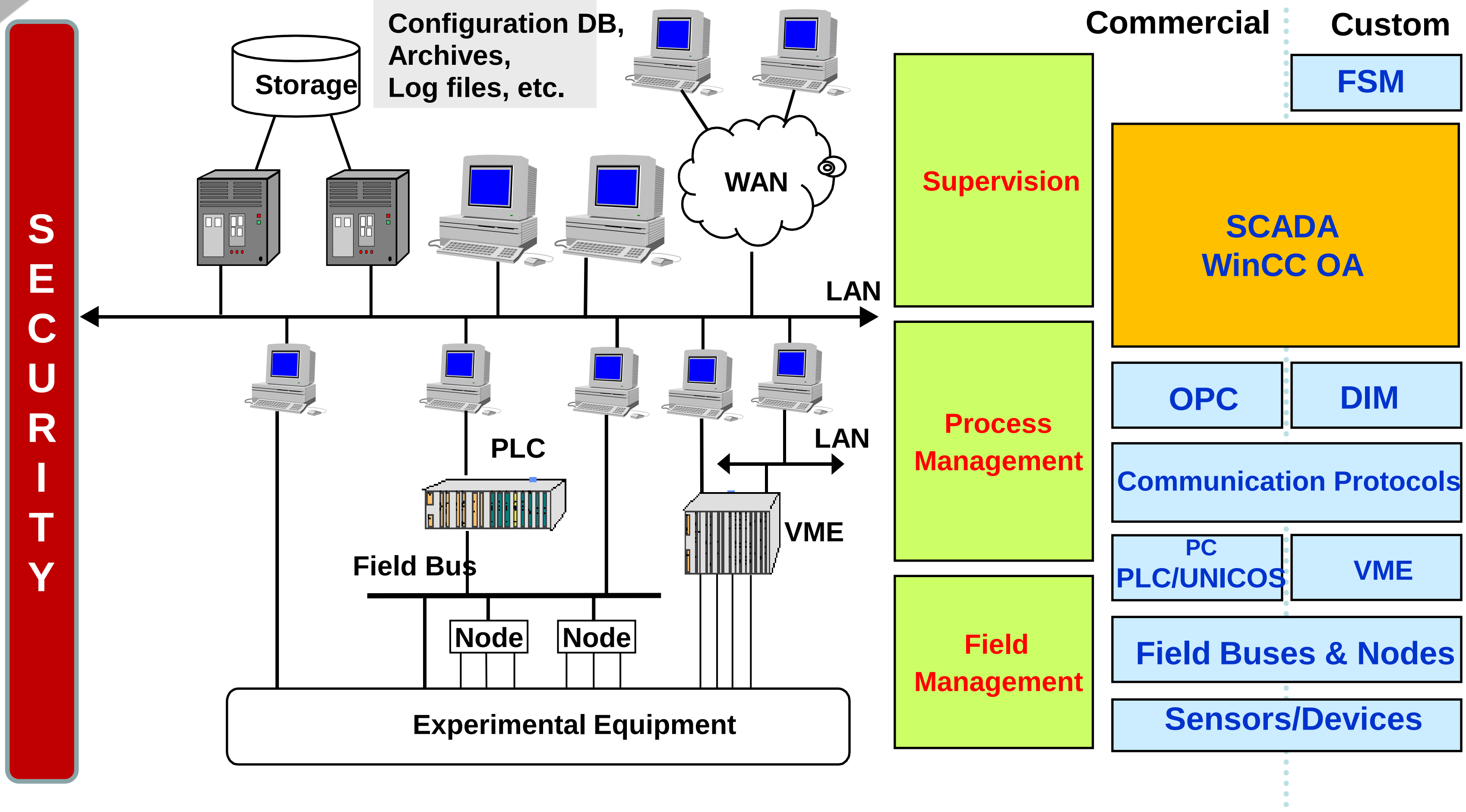
Management

Siemens - Thomas Hahn
ETM - Guenther Zoffmann

CERN - Manuel Gonzalez

	Database Archiver	Deployment Tool	Security	Data Analytics
openlab Researcher	Marcin Bogusz	Pavel Fiala	Filippo Tilaro	TBD
CERN Supervisor	Piotr Golonka	Fernando Varela	Brice Copy	TBD
Siemens/ETM Supervisor	Ewald Sperrer	Rainer Glocknitzer	Hans-Walter Hirsch Jan Kaestner	TBD

Typical Control System Architecture



Data Analytics

- New activity in Phase IV
  - Focus on data gathered/produced in Controls
  - Currently being defined
- Prepared initial list of Use Cases
  - Infrastructure (e.g. electrical network)
  - Control System “health”
  - Analysis of alarms
- Joint Workshop Siemens-Oracle
  - Identify possible synergies
  - Aim to have it in November

Siemens Openlab Major Review

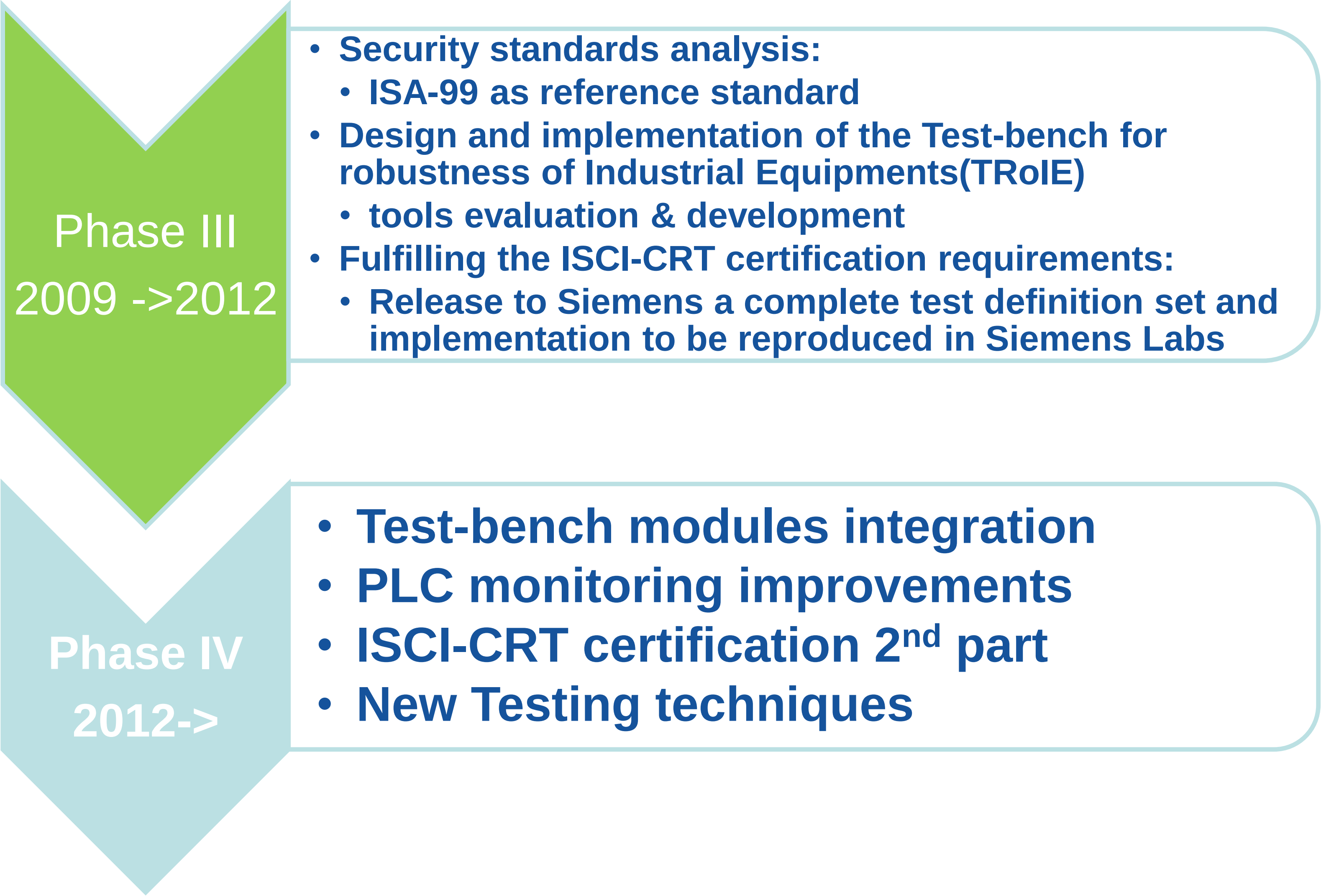
September 2012

PLCs Security

Author: Filippo Tilaro

Supervised by: Brice Copy

PLC Security project phases



Phase III

2009 ->2012

- Security standards analysis:
  - ISA-99 as reference standard
- Design and implementation of the Test-bench for robustness of Industrial Equipments(TRoIE)
  - tools evaluation & development
- Fulfilling the ISCI-CRT certification requirements:
  - Release to Siemens a complete test definition set and implementation to be reproduced in Siemens Labs

Phase IV

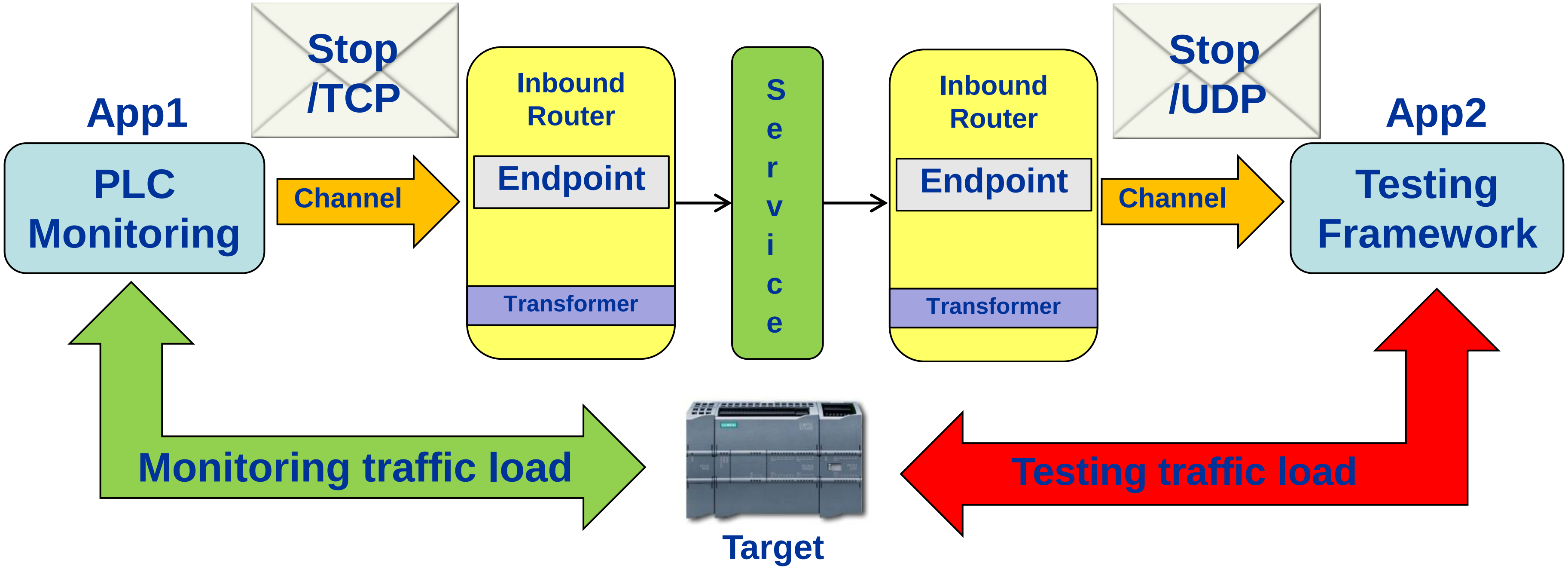
2012->

- **Test-bench modules integration**
- **PLC monitoring improvements**
- **ISCI-CRT certification 2nd part**
- **New Testing techniques**

Achievements I

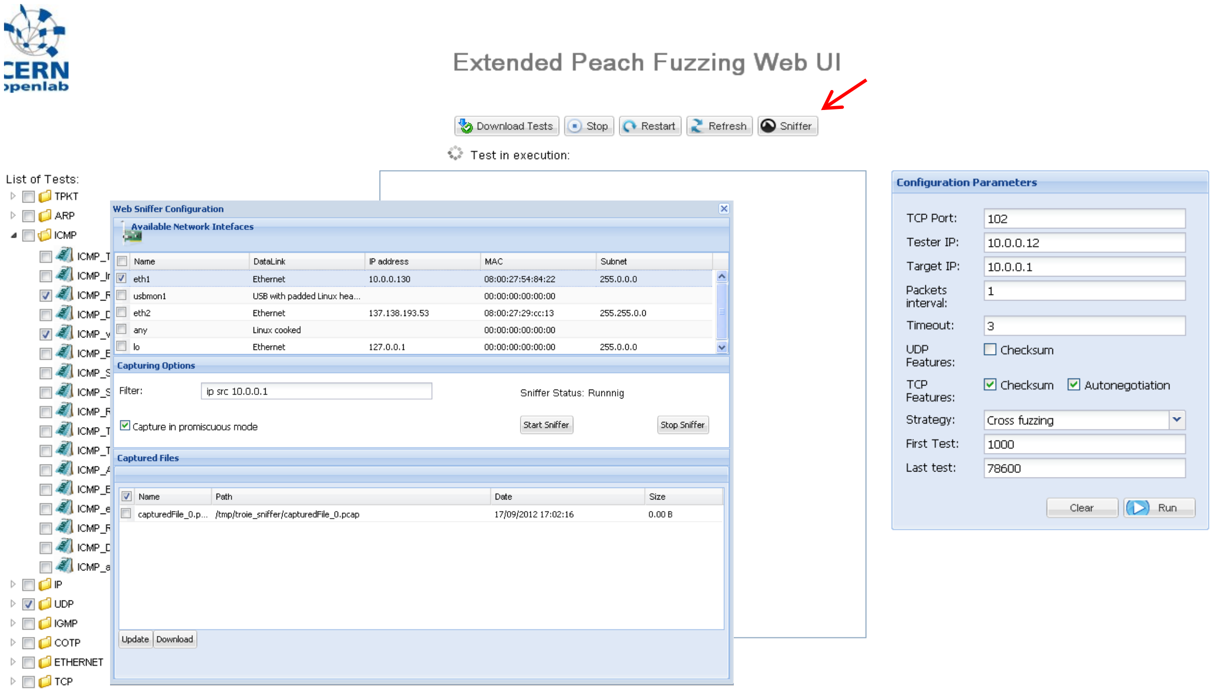
Integration of the test-bench modules:

- Through the use of Enterprise Service Bus (ESB)
  - Orchestrate application modules
  - Message routing and transformation
  - Wide range of connectors: REST, SOAP, LDAP, JDBC, JMS, HTTP/S, FTP/s, Email/SMTP, Facebook, Twitter…



Achievements II

- Communication Monitoring System
  - Development of a web driven sniffer
  - Internal module of the TRoIE test-bench and communicating with other internal modules



Extended Peach Fuzzing Web UI

Test in execution:

List of Tests:

- ▷ □ TPKT
- ▷ □ ARP
- ◢ □ ICMP
  - □ ICMP_T
  - □ ICMP_Ir
  - ☑ ICMP_R
  - □ ICMP_D
  - ☑ ICMP_v
  - □ ICMP_E
  - □ ICMP_S
  - □ ICMP_S
  - □ ICMP_R
  - □ ICMP_T
  - □ ICMP_T
  - □ ICMP_A
  - □ ICMP_E
  - □ ICMP_e
  - □ ICMP_R
  - □ ICMP_D
  - □ ICMP_a
- ▷ □ IP
- ▷ ☑ UDP
- ▷ □ IGMP
- ▷ □ COTP
- ▷ □ ETHERNET
- ▷ □ TCP

Web Sniffer Configuration

Available Network Intefaces

□	Name	DataLink	IP address	MAC	Subnet
☑	eth1	Ethernet	10.0.0.130	08:00:27:54:84:22	255.0.0.0
□	usbmon1	USB with padded Linux hea...		00:00:00:00:00:00	
□	eth2	Ethernet	137.138.193.53	08:00:27:29:cc:13	255.255.0.0
□	any	Linux cooked		00:00:00:00:00:00	
□	lo	Ethernet	127.0.0.1	00:00:00:00:00:00	255.0.0.0

Capturing Options

Filter: ip src 10.0.0.1

Sniffer Status: Runnnig

☑ Capture in promiscuous mode

Captured Files

☑	Name	Path	Date	Size
□	capturedFile_0.p...	/tmp/troie_sniffer/capturedFile_0.pcap	17/09/2012 17:02:16	0.00 B

Configuration Parameters

TCP Port: 102

Tester IP: 10.0.0.12

Target IP: 10.0.0.1

Packets interval: 1

Timeout: 3

UDP Features: □ Checksum

TCP Features: ☑ Checksum ☑ Autonegotiation

Strategy: Cross fuzzing

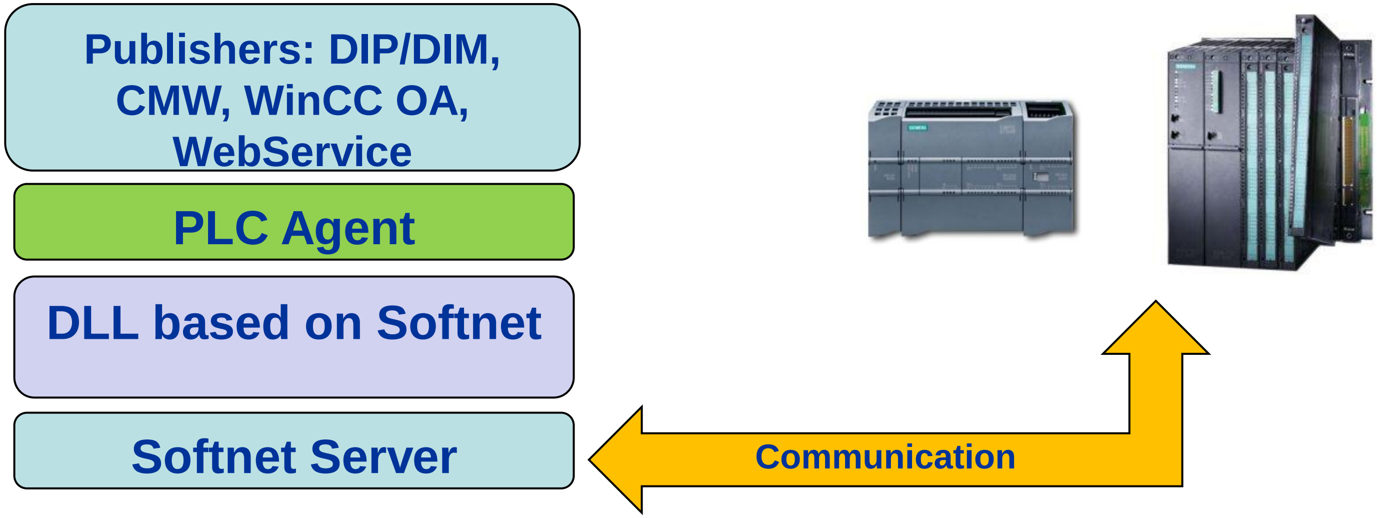
First Test: 1000

Last test: 78600

Undergoing activities

PLC Status monitoring:

- Previous existing CERN system:
  - PLC DIAMON with ‘libnodave’ (open-source library)
- Siemens Softnet library
  - Development of a server-side monitoring system able to question the Siemens PLCs
  - Integration with the GWT client application within the TRoIE test-bench



Publishers: DIP/DIM, CMW, WinCC OA, WebService

PLC Agent

DLL based on Softnet

Softnet Server

Communication

ISCI CRT certification Phase 2

- Extension of the CRT for not covered protocols:
  - S7, Profinet, OPC, DNS, HTTP, FTP, IPv6,Modbus / TCP, SNMP
  - List of tests:
    - Storms and Maximum Load Tests
    - Single Field Injection
    - Combinatorial Fields Injection
    - Cross State Fuzzing (for stateful protocols)

SIEMENS

Recognized CRT Tool
ISASecure

Conclusions and Next Steps

Current and finished activities:

- PLC communication monitoring
- Improve the PLC internal status monitoring

Design of new testing techniques:

- Multi-Protocols (Man-in-the-middle) layer testing
  - Able to test any kind of communication protocols
  - Scalable and user-friendly to define new grammars
  - Overcome the current testing framework limitations
    - Traffic generation, multi-layer fuzzing

Extending to the supervision level: SCADA system like WinCC OA, OPC OA ...

Siemens openlab Projects

September 2012

WinCC OA

Marcin Bogusz

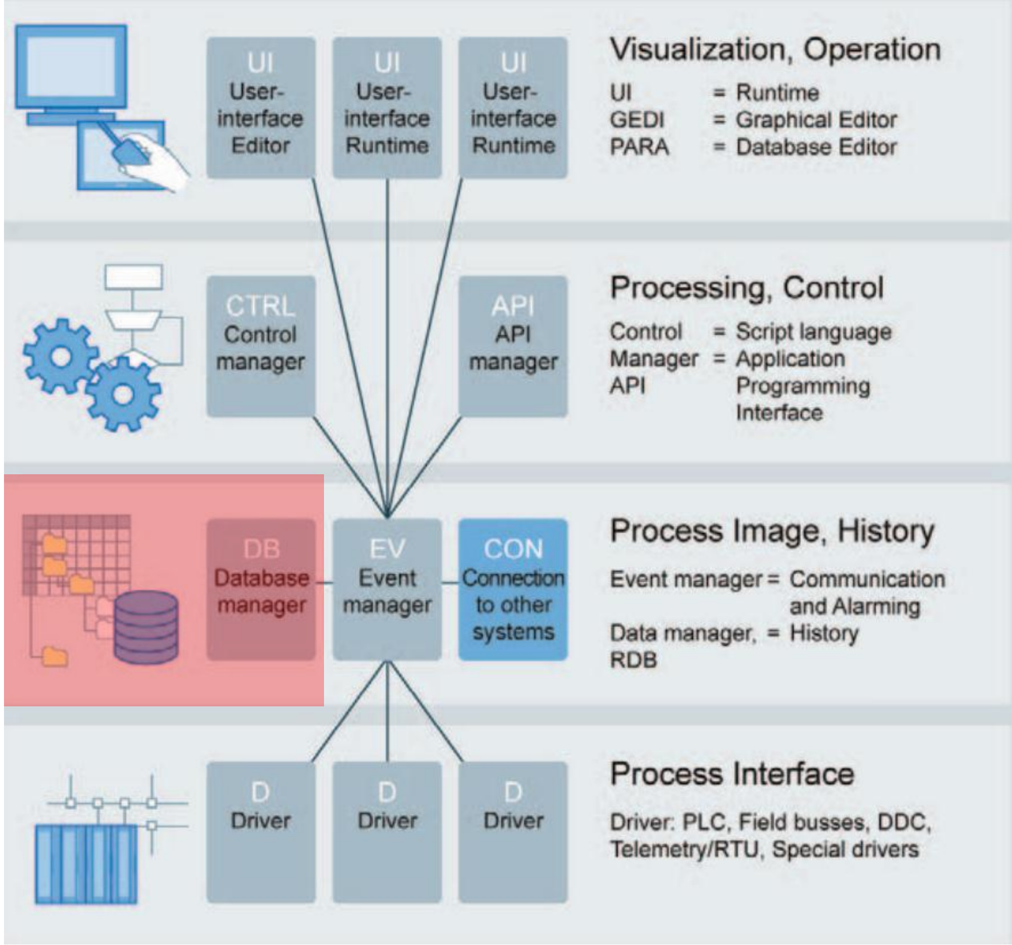
Pavel Fiala

WinCC OA

- RDB archiving
  - WinCC OA version 4 archiving
    - Future SCADA system
    - Work on a storage plug-in for Oracle RDBMS
  - WinCC OA 3.11 archiving
    - New Features Validation
    - Large Scale Performance tests

- Centralized Deployment Tool
    - New Fellow Pavel Fiala
    - Started with the ASCII Manager

RDB ARCHIVING

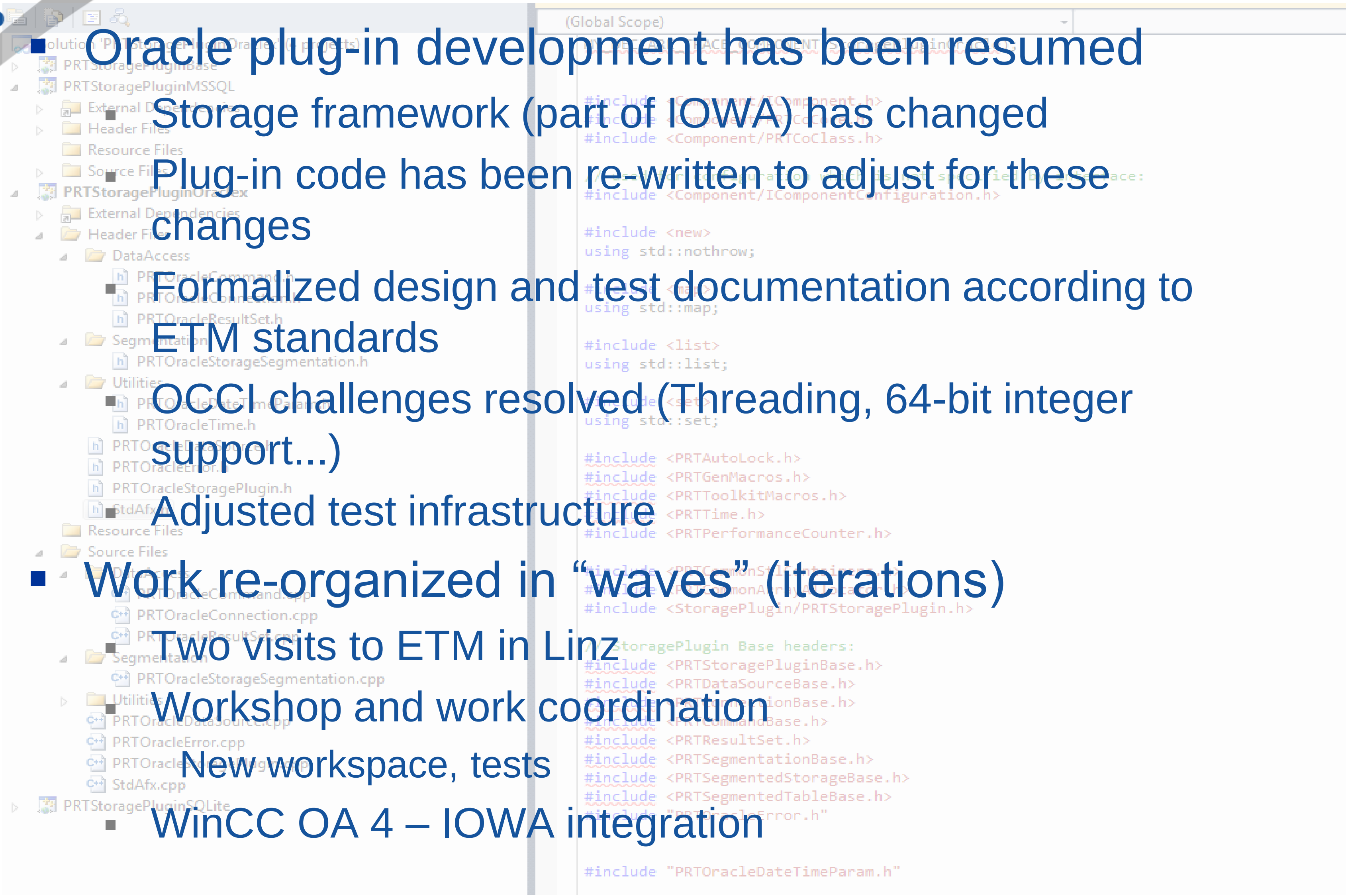


WinCC OA Version 4

SIEMENS SIMATIC WinCC Open Architecture

- Upcoming SCADA system to be released in the next years
- New storage and component architecture
  - Storage architecture designed not only for WinCC OA but other Siemens products which require archiving
- CERN is developing an Oracle archiving module (Oracle plug-in).
- Other relational database plug-ins developed by ETM (SQLite, MS SQL Server)
- Modules are based on the framework provided by ETM, developed jointly by ETM and Siemens

WinCC OA 4



```
Solution 'PRTStoragePluginOracle' (4 projects)
  PRTStoragePluginBase
  PRTStoragePluginMSSQL
    External Dependencies
    Header Files
    Resource Files
    Source Files
  PRTStoragePluginOracle
    External Dependencies
    Header Files
      DataAccess
        PRTOracleCommand.h
        PRTOracleConnection.h
        PRTOracleResultSet.h
      Segmentation
        PRTOracleStorageSegmentation.h
      Utilities
        PRTOracleDateTimeParam.h
        PRTOracleTime.h
      PRTOracleDataSource.h
      PRTOracleError.h
      PRTOracleStoragePlugin.h
      StdAfx.h
    Resource Files
    Source Files
      DataAccess
        PRTOracleCommand.cpp
        PRTOracleConnection.cpp
        PRTOracleResultSet.cpp
      Segmentation
        PRTOracleStorageSegmentation.cpp
      Utilities
      PRTOracleDataSource.cpp
      PRTOracleError.cpp
      PRTOracleStoragePlugin.cpp
      StdAfx.cpp
  PRTStoragePluginSQLite
```

(Global Scope)

```
#include <Component/IComponent.h>
#include <Component/PRTCoClass.h>
#include <Component/PRTCoClass.h>

#include <Component/IComponentConfiguration.h>

#include <new>
using std::nothrow;

#include <map>
using std::map;

#include <list>
using std::list;

#include <set>
using std::set;

#include <PRTAutoLock.h>
#include <PRTGenMacros.h>
#include <PRTToolkitMacros.h>
#include <PRTTime.h>
#include <PRTPerformanceCounter.h>

#include <StoragePlugin/PRTStoragePlugin.h>

// StoragePlugin Base headers:
#include <PRTStoragePluginBase.h>
#include <PRTDataSourceBase.h>
#include <PRTCommandBase.h>
#include <PRTResultSet.h>
#include <PRTSegmentationBase.h>
#include <PRTSegmentedStorageBase.h>
#include <PRTSegmentedTableBase.h>
#include "PRTOracleError.h"

#include "PRTOracleDateTimeParam.h"
```

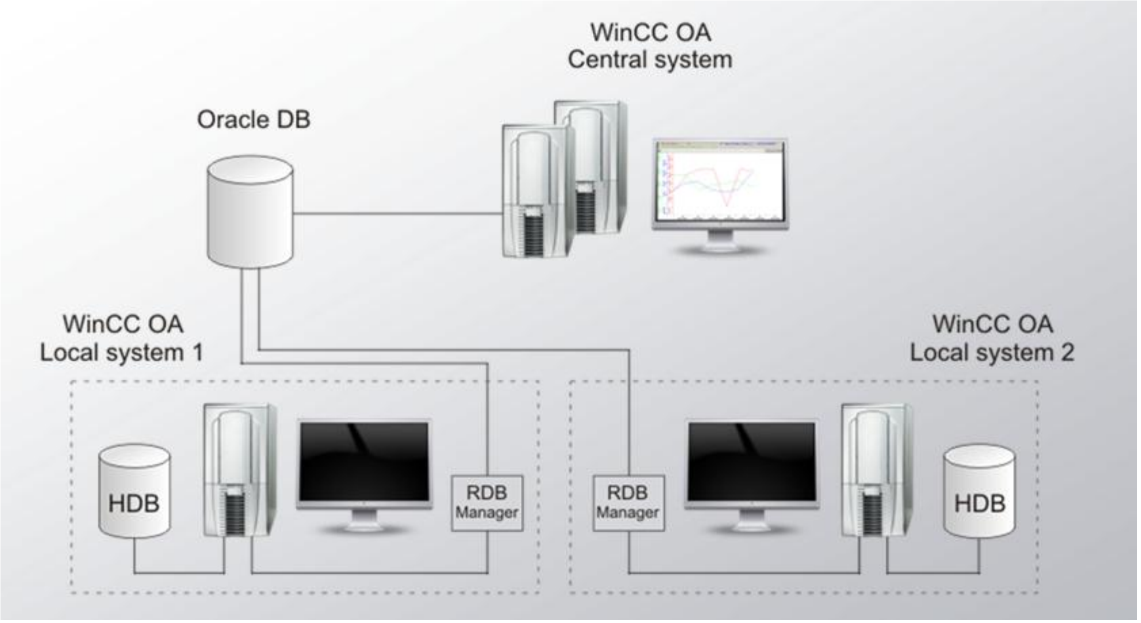
- Oracle plug-in development has been resumed
  - Storage framework (part of IOWA) has changed
  - Plug-in code has been re-written to adjust for these changes
  - Formalized design and test documentation according to ETM standards
  - OCCI challenges resolved (Threading, 64-bit integer support...)
  - Adjusted test infrastructure
- Work re-organized in “waves” (iterations)
  - Two visits to ETM in Linz
  - Workshop and work coordination
    - New workspace, tests
  - WinCC OA 4 – IOWA integration

WinCC OA 4

- Achievements
  - Milestone : Wave 1 completed
    - Plugin code passes all the ETM unit tests
- Next Steps (Wave 2)
  - Planning phase started
  - Missing Functionality – storage segmentation
  - Changed interface adjustments
  - Database schema (re)design
    - Survey of other products (at CERN, open source)

WinCC OA 3.11

- WinCC OA 3.11 is being validated at CERN
  - Successor to 3.8 SP2 for the long shutdown 1
- New Features Validation
  - Parallel archiving feature tested
    - Local file archiver (HDB) & Oracle DB



  - RDB Compression mechanism
    - Follow-up of 3.10 validation

WinCC OA 3.11

- Scalability performance tests
  - Update of previous round of tests (~7 years ago)
    - New hardware and software versions
    - Scalability reassessment
      - New up-to-date performance figures
  - Test machines have been set up
    - 50 WinCC OA servers (up to 200 projects)
    - Oracle server – 2 node RAC
  - Collaborating with IT-DB experts
    - Setup
    - Optimization
      - Use of IOT
      - Index compression...

DEPLOYMENT TOOL

ASCII Manager

- Key component of the Centralized Deployment Tool
  - Will allow pushing new versions of WinCC OA-based components onto sets of remote projects
- Imports/exports the run-time database of a project from/to files
- Initial tasks
  - Benchmark the current performance
  - Introduce XML format for files
  - Extend the functionality of the manager by:
    - Pre-validating the file contents prior to imports
    - Deletion of database entries
    - Coherent exports to ensure the completeness of parameterization
  - Performance optimization
  - GUI usability improvement

Any Questions

Thank you for attending!