IST-2001-37652

Hard Real-time CORBA

Title

PCT Design

Authors

Santos Galán (UPM)
Manuel Rodríguez (UPM)
Ricardo Sanz (UPM)

Reference IST37652/038 Deliverable D4.2
Date 2002-12-27
Release 0.3
Status Draft
Clearance Consortium

Partners

Universidad Politécnica de Madrid
Lunds Tekniska Högskola
Technische Universität Wien
SCILabs Ingenieros

Summary Sheet

IST Project 2001-37652
HRTC
Hard Real-time CORBA

PCT Design

Santos Galán (UPM), Manuel Rodríguez (UPM), Ricardo Sanz (UPM)

Abstract:

The present document defines the design of the Process Control Testbed (PCT) based on the requirement s specification (D4.1).

This document has been issued in accordance with the document *IST-2001-37652 Annex 1 – "Description of Work"*. The identification of this deliverable is D4.2.

HRTC Partners:

Universidad Politécnica de Madrid
Lunds Tekniska Högskola
Technische Universität Wien
SCILabs Ingenieros.

Release Sheet (1)

Release:	**0.1 Draft**
Date:	2002/10/20
Scope	Initial version
Sheets	All

Release:	**0.2 Draft**
Date:	2002/11/29
Scope	Added contents
Sheets	All

Release:	**0.3 Draft**
Date:	2002-12-27
Scope	Added contents
Sheets	All

Table of Contents

1 Introduction

1.1. Purpose of the document

This document defines the design of the PCT based on the available equipments and the requirements expressed in D4.1.

1.2. Definitions, acronyms and abbreviations

Definitions

Acronyms

AI	Analog Input
AO	Analog Output
CCS	CORBA Control System
CORBA	Common Object Request Broker Architecture
DCS	Distributed Control System
DI	Digital Input
DO	Digital Output
GPS	Global Positioning System
GR	General Requirement
GUS	Global User Station
HLA	High Level Architecture
HM	History Module
HMI	Human Machine Interface
HPM	High-Performance Process Manager
HRTP	Hard Real-Time Protocol
IIOP	Internet Inter-ORB Protocol
I/O	Input / Output
LCN	Local Control Network
MBPC	Model Based Process Control
NIM	Network Interface Module
ORB	Object Request Broker

PCT	Process Control Tested
PLC	Programmable Logic Controller
SI	Serial Interface
SOE	Sequence Of Events
SR	Specific Requirement
TCP/IP	Transmission Control Protocol / Internet Protocol
TPS	Total Plant Solution
TT	Time Triggered
TTP	Time Triggered Protocol
UCN	Universal Control Network

Abbreviations

1.3. References to Project documents

HRTC Project Annex 1 "Description of Work"
D1.1 "CCS Domain Analysis"
D4.1 "PCT Requirements Specification"

2 PCT Overview

2.1. Purpose of the PCT

The main objective of the distributed process control testbed is to identify (mainly hard real time) requirements for distributed control systems and perform experiments in conditions of systems heterogeneity and legacy integration. Experiments will be done using conventional IIOP and the new real-time protocol.

One of the general requirements of the PCT is (GR1 in D4.1) to be representative of a process plant control system. A short summary of the description in D1.1 is included here for convenience.

2.2. Process Control Overview

Most present-day plant-wide control systems are very complex, constituted by diverse hardware and software components which interact with each other. With the incorporation of intelligent sensors, the computers reach even the lower level of the control hierarchy. They are also distributed systems, different tasks run on different processors (computers, networks interfaces, PLC's...) and common resources are shared between processors. Distributed systems are designed to improve performance and increase system reliability in order to meet timing, resources and concurrency constraints on each node. The control system have been traditionally separated into several levels:

1. Field level. This level is dedicated to the instruments (sensors and actuators) and basic regulatory control. It is communicated via fieldbus.

2. Process control level. This level takes over the advanced and supervisory control (advanced controller, multivariable controller,

model predictive control,…). This level also computes a local optimization. It is communicated via an Ethernet based protocol

3. Business level. The upper level is dedicated to global optimization, scheduling and planning. It is communicated via Ethernet.

Although these levels have been always present in the process industry the control implementation has been evolving along the years. From the first direct digital control where all the devices were connected separately to the control room where the control was centralized to a single computer; to the traditional Distributed Control System implementation where several devices are linked to a controller and there are several distributed controllers that are connected to the DCS console; to the future where the control is totally distributed to field with the loops in individual devices. Nowadays we are mostly in the traditional DCS but migrating slowly to the future.

2.3. Conceptual Design of PCT

The design basis for the PCT are the requirements included in document D4.1 *PCT Requirements Specification*.

The PCT mimics a plant control system, what can be seen (D1.1) as a (possibly hybrid) redundant network where the nodes are monitoring and control elements. Therefore, PCT is essentially a redundant network where components are connected. The hybrid characteristic of current industrial control systems, with distinct networks at different levels, is intentionally eliminated to test the viability of a flat network in control environments. On the other hand, since a conventional (non HRTP, TCP/IP) and a specialized (HRTP, TTP/C) networks are going to be compared, the heterogeneous feature is recovered joining both networks in a final test.

The designed PCT should be able to comprehend the functionality of both present and future process plant control systems. The idea is to try to build such a control system using CORBA components and check whether it is possible to:

1. Perform the tasks that current systems usually do.
2. Accomplish the tasks that future systems are expected to achieve.

The results of the experiments (mainly the negative ones) will identify the features needed in HRTC to be used in control systems.

Since we know current CORBA actually lacks hard real-time attributes and it may happen that some of the experiments could even not be tried, a progressive approach to the construction of the PCT is devised. This progression is concretized in a series of *scenarios* (different network configurations) where a set of experiments are performed.

The experiments, based on the use cases of D4.1 are:

1. Single control loop
2. Legacy system integration
3. Simulation components integration
4. Sequence of events generation
5. Traffic capacity test
6. Concurrent access
7. Response to faults

These experiments are to be run on the conventional and specialized networks. The final experiment will try to combine both through a bridge.

An important issue is the implementation of monitoring tools for the measurement of the relevant variables in tests. For distributed real-time systems it is necessary to observe inputs and outputs, but also the timing and order of the executing and communicating. Thus, a global synchronized time base with known precision is needed.

In the tests, the behavior of the system is monitored to judge whether the system comply with the requirements. Notice that in monitoring, testing is used for finding failures or their absence. Debugging (finding the error that cause the failures) is out of the scope of this project.

The monitoring tools (also called observers), observe the system behavior at different levels:

- Dedicated nodes eavesdropping on the network
- Local tasks in the nodes
- Programming language statements inside tasks that output information

3 PCT description

3.1. Topology

The following figure shows the complete topology of the proposed testbed. This final structure should hopefully be reached in several stages of increasing difficulty where different experiments shall be tried. The detailed description of the building blocks can be found in the following subsections. The set of partial structures for the test stages is included in the next section.

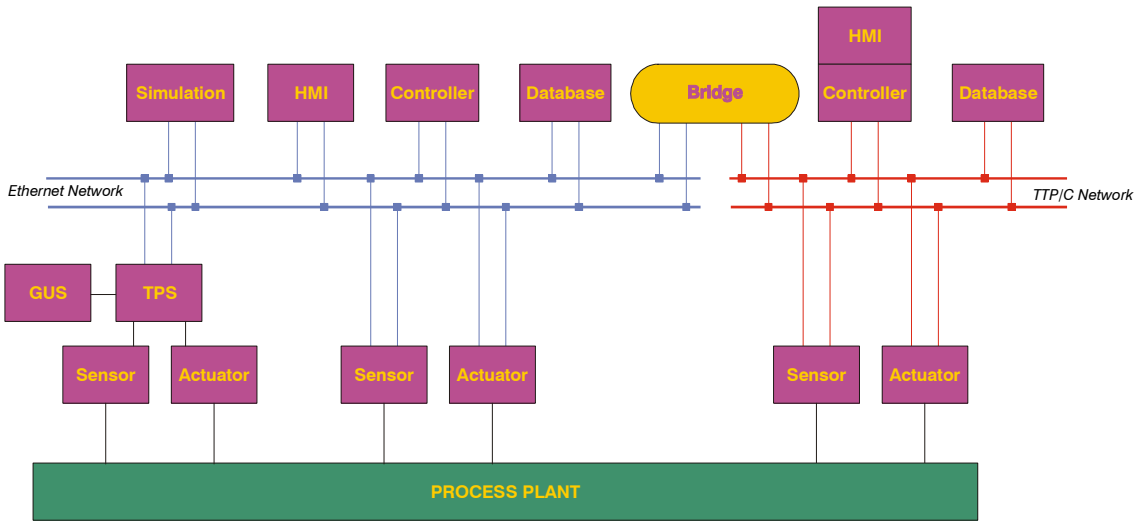

Figure 1:Process Control Testbed elements

The testbed tries to represent the basic characteristics of a process plant control system network with advanced features not found in current designs, like the two flat control networks (Ethernet and TTP/C) where all the elements are linked. Several instruments (sensors and actuators) are connected to a (actual or simulated) process plant in three different ways:

1. Trough a typical industrial distributed control system (DCS), in this case the TPS from Honeywell that constitutes a legacy system in this context, with its own controller and user interface. The TPS communicates with the Ethernet control network.
2. Directly connected to an Ethernet control network.
3. Directly connected to a time-triggered network (TTP/C).

Apart from the TPS monitoring and controlling devices, both networks include controllers, human-machine interfaces (HMI) and history databases. This is not the typical configuration in industrial practice, where separate networks are used. Finally, one or several simulation nodes are included in the Ethernet network.

The Ethernet and time-triggered networks communicate through a bridge.

3.2. Components

Ethernet network

A 100BASE-TX Ethernet with a maximum of 8 nodes with (redundant) connection to 2 switches.

Time-triggered network

The time-triggered network will have 4 TTTech Monitoring Nodes with (redundant) connection to 2 switches.

Instruments

Sensors

Sensors measure physical values of the process variables. There are different types in a process plant: temperature sensors, pressure sensors, flowmeters, etc.

Sensors are usually connected to conventional (4-20 mA) or 'smart' (digital bus) transmitters, that transport the measurement to the control system. In the commercial DCS they enter through the I/O cards.

For connecting the sensors to the Ethernet network in the PCT it is necessary to have a wrapper node that, ideally, could be integrated in the instrument.

Two kind of sensors shall be used:

1. Actual (physical) instruments with a transmitter and an input card in the DCS (analog signal or serial interface) or the wrapper node (serial interface).
2. Simulated sensors instantiated on the wrapper node. They will allow to test the effect of a large number (a more realistic scenario at a reasonable cost) of sensor on the system performance.

Actuators

Actuators are the final elements of a control loop, modifying the process conditions as the result of the controller command. They include control valves, frequency variators, etc.

As it happened in the case of the sensors, a wrapper node (or the DCS) with I/O cards is necessary to connect them to the network (or the HPM controller, see TPS subsection below). Also two kind of actuators shall be used:

1. Actual actuators
2. Simulated actuators

Controllers

The controller receive the signal of the sensors and as a function of their setpoints and control algorithms calculate the output signal to be sent to the actuator. There will be two controller types:

1. The controller integrated in the DCS (HPM) that receives and sends signals (initially) internally without entering the Ethernet network.
2. The controller nodes built for this project that implement the CORBA Control algorithms, and that communicate with the sensors and actuators through the Ethernet or TT networks.

Human-Machine Interface

The Human-Machine Interface in modern Plant Control Systems is usually a graphical interface, with or without windows. The HMI allows the monitoring function carried by human operators, as well as their interaction with the process by means or control actions, such as starting up/stopping units, changing setpoints, etc.

In the PCT, preferentially graphical HMI nodes shall be built in order to access and interact with the data and agents on the network.

Database

Historical databases record selected data from the control system configuration and/or operation. Also, they usually contain the sistem software files. Operators can access to them through HMIs.

Commercial DCS (TPS)

An already available commercial DCS, the Honeywell TPS (TDC 3000), will be used. The system is composed by:

1. A High-Performance Process Manager (HPM) controller
2. A Global User Station (GUS)
3. A History Module (HM)
4. A Network Interface Module (NIM)
5. A redundant Local Control Network (LCN)
6. A redundant Universal Control Network (UCN)
7. Several I/O cards:
    a. Analog Input (AI)
    b. Analog Output (AO)
    c. Digital Input (DI)
    d. Digital Output (DO)
    e. Serial (Modbus) Interface (SI)

With the available hardware, to integrate the TPS in the Ethernet network the system could be wrapped (with a PC) via the serial bus or via the GUS. The serial bus has the advantage of directly accessing the controller (HPM) like sensors or actuators do.

A temperature sensor and transmitter enter the system through the AI card. The heating module is controlled by an AO output signal.

Simulation

An increasing number of control and monitoring functions utilize models in on-line and off-line applications as:

1. Model based process control (MBPC)
2. Hardware in the loop
3. Data reconciliation
4. Operator training

In such context, the availability of plugable simulation nodes accessible by the other components in a transparent way will constitute and advance from the current state. Besides, the use of distributed simulation architectures (like HLA) that facilitate real time applications, should be easily integrated over the network.

Bridge

A bridge handles the communication between two networks. The bridge hardware is constituted by an additional monitoring node, with both Ethernet and TTP/C connections.

3.3. Monitoring tools

Each node of PCT is a self sufficient computing element with CPU, memory, network access, a local clock and, possibly, I/O units for sampling and actuation of an external process. In order to monitor a network composed of such nodes, synchronization and observers which register the system behavior at different levels have to be considered.

Synchronization

For distributed real-time systems it is necessary to observe inputs, outputs and their timing. Thus, a global synchronized time base with known precision δ (no two nodes in the system have local clocks differing by more than δ) is needed. Actually, this issue should be elucidated in the

project, but at least provision has to be made for external measuring of times in different nodes. The use of GPS clocks is initially planned.

Monitoring tasks and monitoring statements in applications

Monitoring objects included in the software of the nodes have to be developed at the same time. The actual act of monitoring a real-time system can change its behavior (*probe-effect* or *Heisenberg uncertainty in software*). In that case their effect should be calculated and compensated for.

The minimum functions for monitoring on every node shall be logging of data exchange and time-stamping.

Eavesdropping node

A node that eavesdrop on the network is a desirable tool, but it likely falls beyond the scope of this project . At least one that stores monitoring information from other nodes would greatly simplify the analysis of results. The historical databases could include that function.

4 PCT experiments

The PCT should be built progressively, executing the programmed test and recording integration and development incidences that identify the CCS requirements. The stages in PCT construction represent increasingly complex process control scenarios that eventually could not be reached.

4.1. CCS loops

Purpose

To demonstrate the use of CORBA components for the implementation of control loops. From this experiment, the basic requirements for CCS should be elucidated.

Description of the experiment

A simple regulatory control loop with three components:

1. Sensor
2. Actuator
3. Controller

built as independent nodes connected through the Ethernet and the TTP/C networks shall be tested. Also there should be two additional nodes:

1. HMI
2. Historical Database

For the TT network the HMI and the controller are in the same node.

In the experiment, an operating elemental process plant, such as a neutralization tank with a pH sensor will be controlled by the addition of a reactant with a volumetric pump. The time series of values of the process

variables shall be recorded on the historic database and shown on real time on the HMI. The operator shall be able to change the set point through this HMI node.

PCT configuration

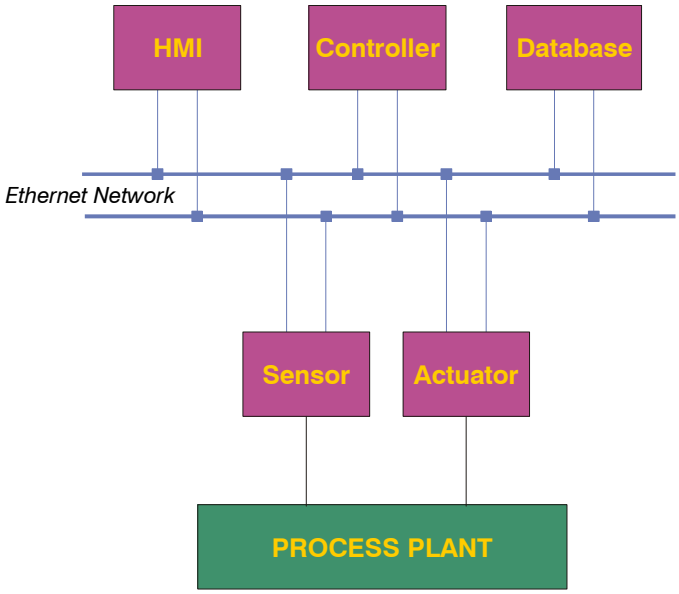

Figure 2: Ethernet control loop

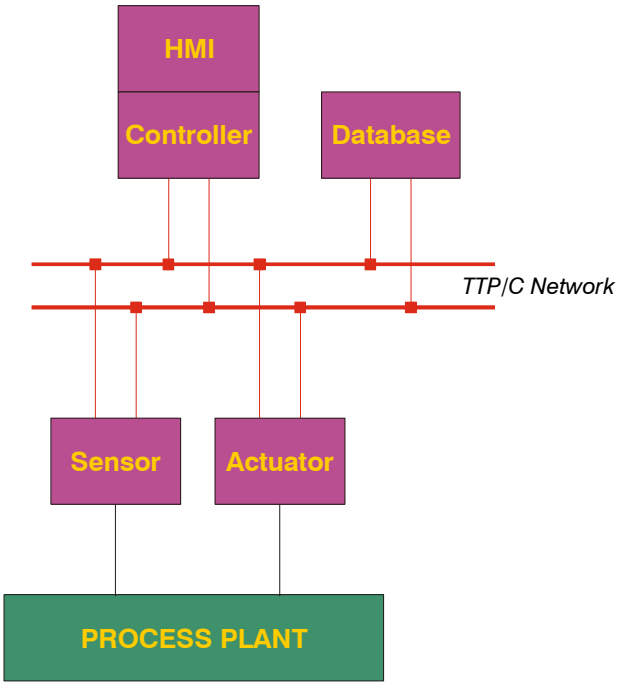

Figure 3: TTP/C control loop

Tests and measurements

1. Performance comparison with a conventional control loop
2. Performance comparison on the Ethernet and TTP/C networks
3. Error handling

4.2. Integration of legacy systems

Purpose

To demonstrate the integration of legacy systems in a CCS.

Description of the experiment

A commercial Honeywell TPS distributed control system shall be wrapped to become a node on a CCS network. Based on the available hardware and the time scope of this project, only a limited set of the TPS functionality shall be reachable through the network.

PCT configuration

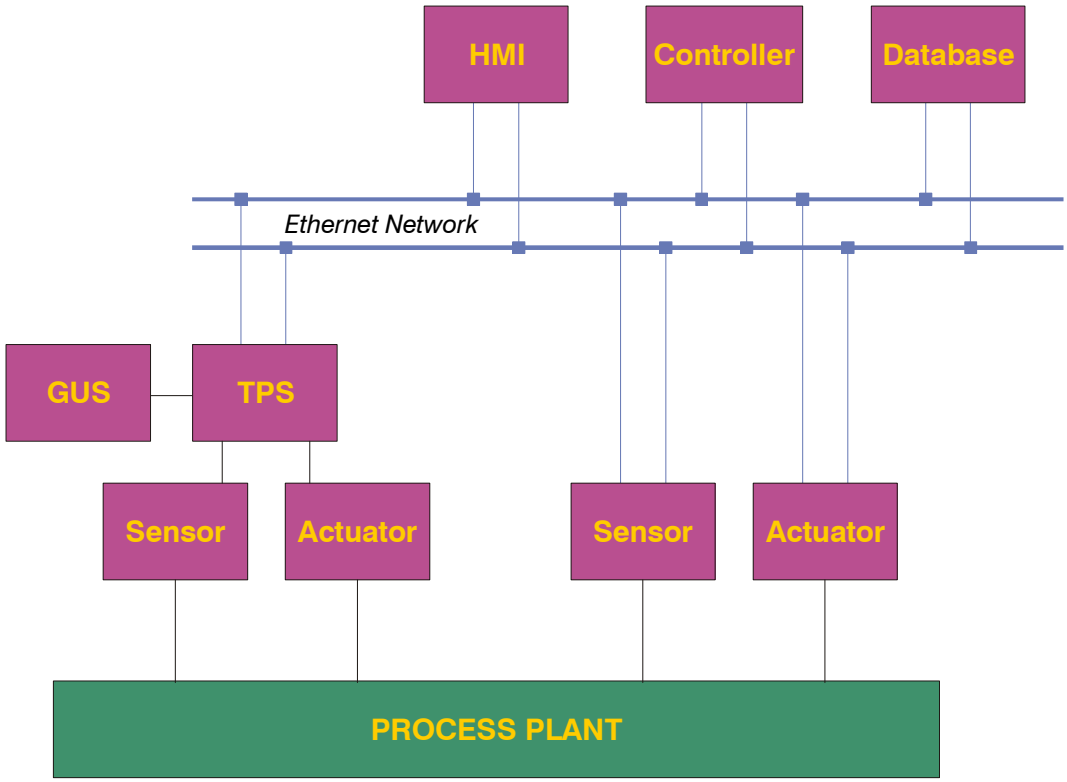

Figure 4: Legacy system integration

Tests and measurements

1. Limitations of the connection
2. Use of the TPS controller with CCS sensor and actuator
3. Use of CCS controller with TPS sensor and actuator
4. Use of TPS sensor with CCS controller and actuator

4.3. Asynchronous events management (sequence of events)

Purpose

To test the ability of CCS for implementing sequence of events register functionality. This is a measure of the accomplishment of the timing properties required by a distributed real-time control system.

Description of the experiment

A sequence of asynchronous events occurring in different nodes is generated in a short period of time. This events are registered in a central database with their time-stamps.

PCT configuration

On both, Ethernet and TTP/C networks, a node with the master clock generates event signals for other nodes connected to the network that time-stamp the occurrence of the event. Initially, a node with interfaces to Ethernet and TTP/C networks will be the event generator node, but the segments do not have to be operative simultaneously.

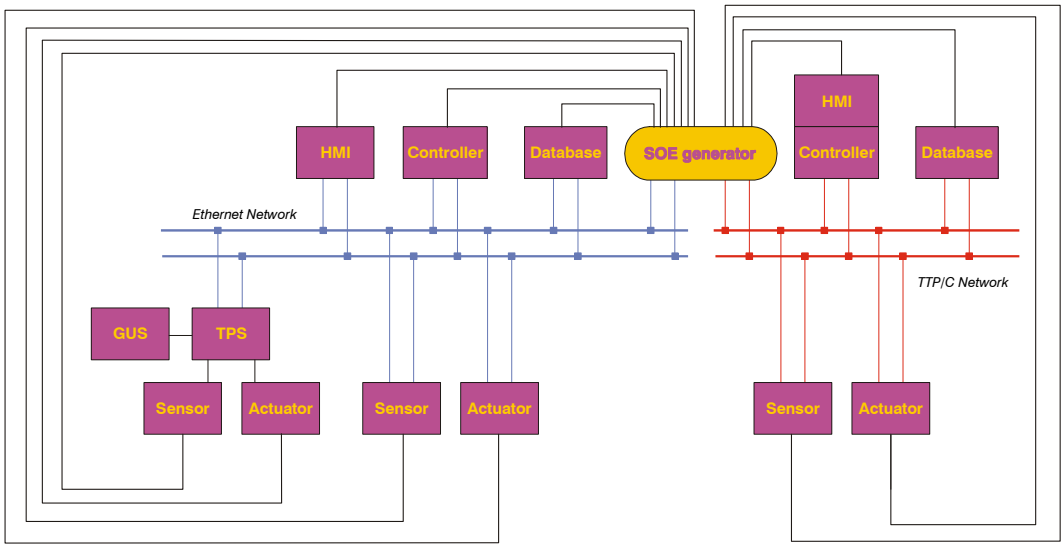

Figure 5: Sequence of events testbed

Tests and measurements

1. Comparison of generated sequence times and recorded times at arrival
2. Conditions for sequence inversion

4.4. Distributed simulation

Purpose

To check the performance of HLA over the implemented network.

Description of the experiment

Several simulation nodes with HLA software running a parts of a distributed simulation model.

PCT configuration

On a Ethernet network, apart from the simulation nodes, there are also the HMI for interaction and database for storing numerical results.

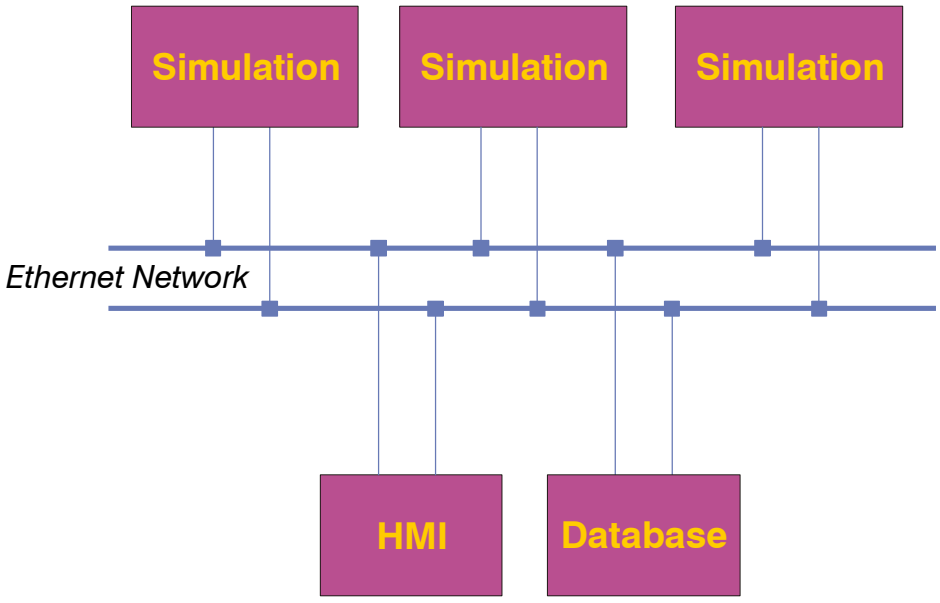

Figure 6:Distributed simulation

Tests and measurements

1. Timing of simulation runs
2. Measurement of traffic increase on the network

4.5. Interaction of simulation objects with control agents

Purpose

To test and identify requirements for the use of simulation objects on a CCS.

Description of the experiment

A simulation node shall be introduced on a Ethernet network with the CCS control loop configuration. This node should interact in several ways with the control agents.

PCT configuration

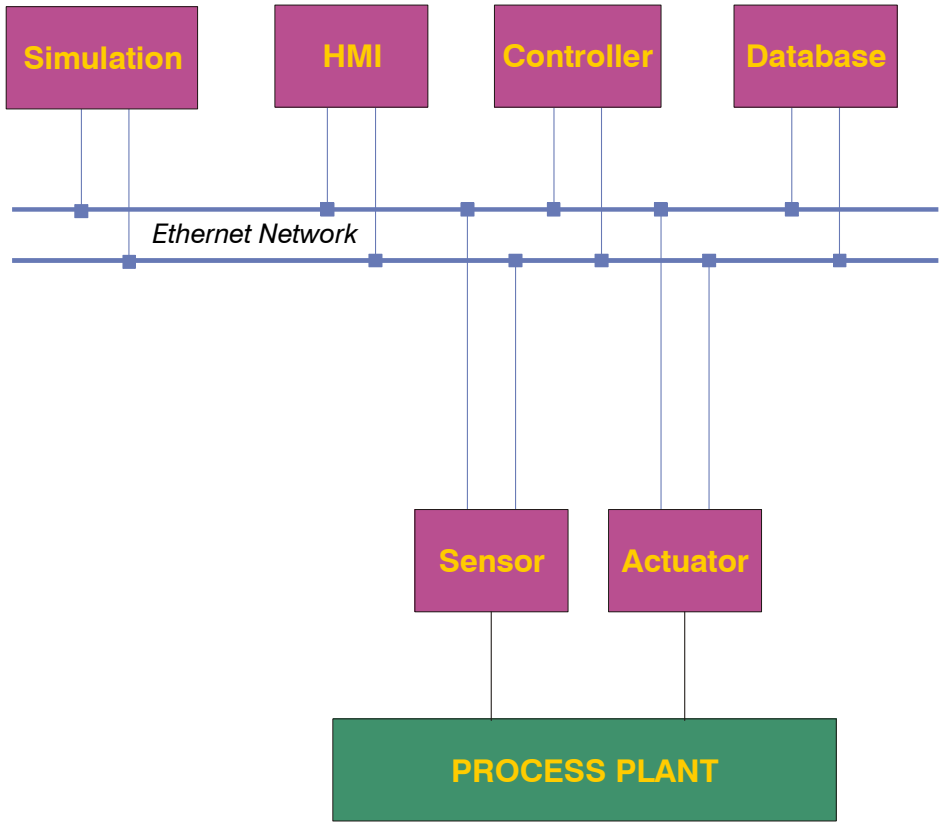

Figure 7: Simulation integration

Tests and measurements

1. Simulated plant and CCS controller. The actual sensor and actuator are substituted by the simulated ones.
2. Operator training. The controller is also included in the simulation, but the operator has the same vision on the HMI.
3. Model based control. The controller uses data from the simulator in order to produce the output signal.

4.6. Intensive data traffic

Purpose

To check capacity limits of the system when the number of control elements increases.

Description of the experiment

During the test, the number of instances of simulated sensors and actuators on their respective nodes is increased progressively, as well as the corresponding number of controllers (in one node), database records and HMI points.

PCT configuration

Similar to Ethernet and TTP/C control loop configurations without the process plant and with simulated controllers and instruments.

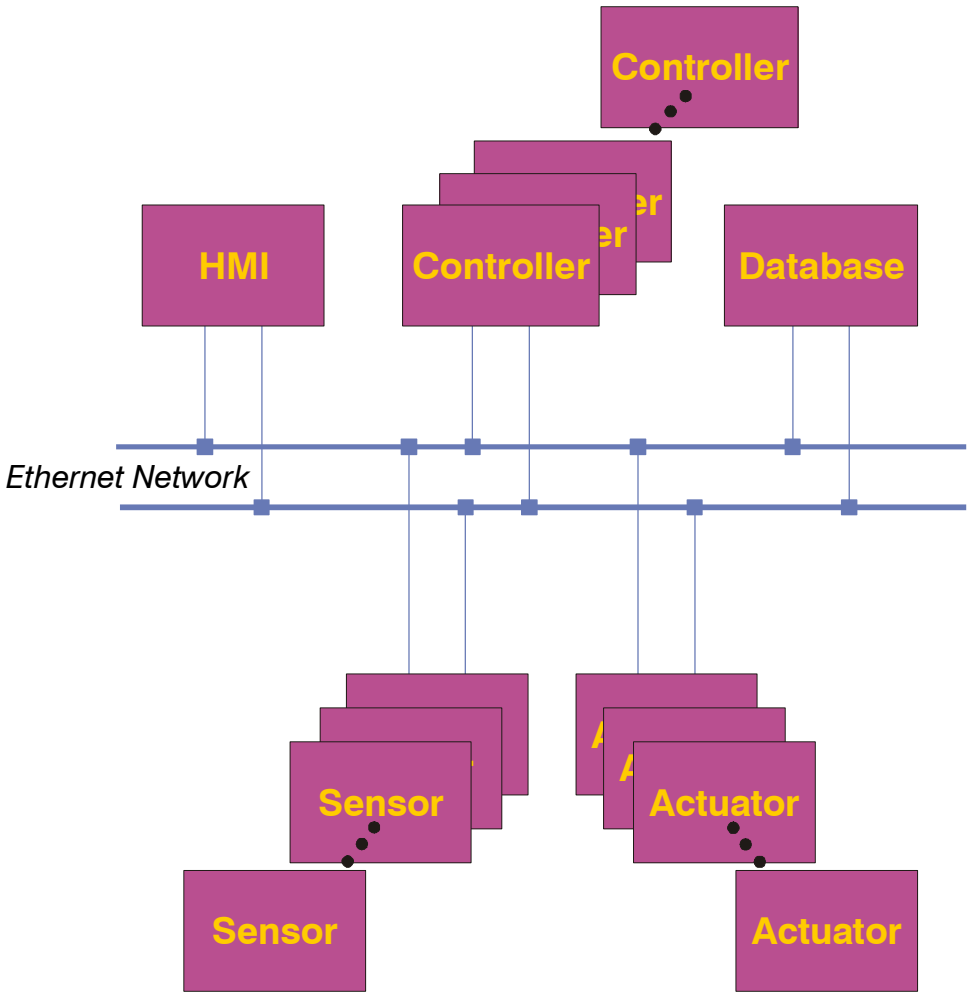

Figure 8: Capacity test configuration (on Ethernet network)

Tests and measurements

1. Detection of modifications in performance as the system grows.
2. Effect of dynamic loads.

4.7. Concurrency test

Purpose

To identify concurrency issues in CCS.

Description of the experiment

In the test several nodes will access concurrently to an instrument. As in the previous test, the number of client instances increases progressively.

PCT configuration

The network topology is similar to the simulation integration one, but with different functionality.

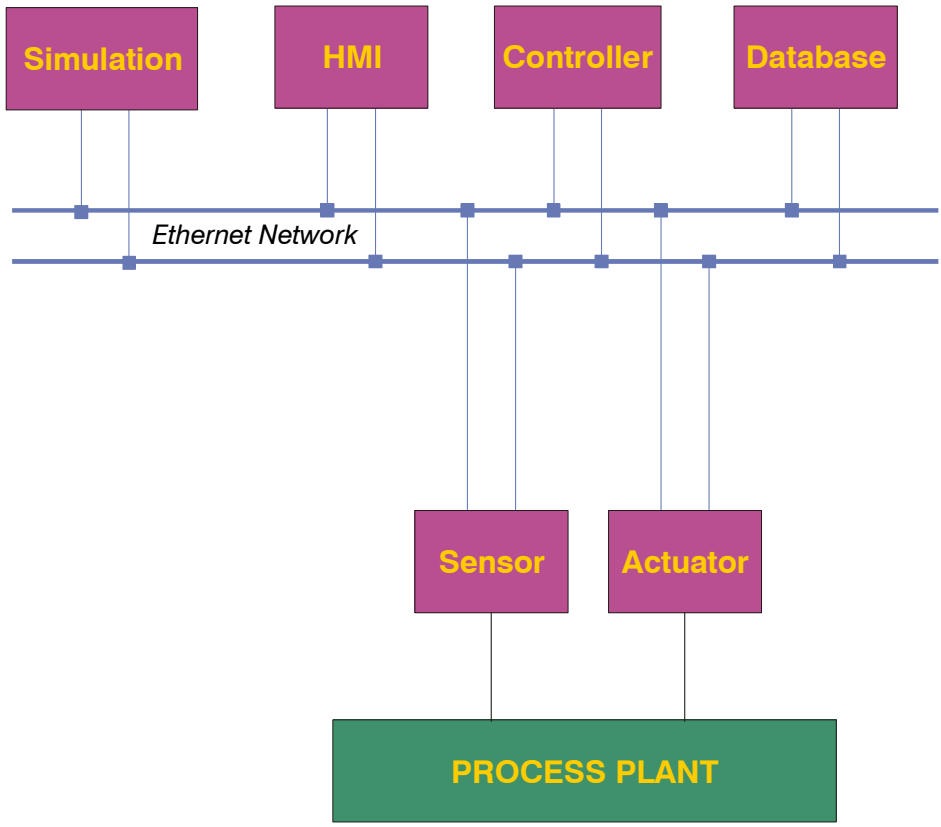

Figure 9: Configuration for concurrency test

Tests and measurements

1. Detection of modifications in performance as the system grows.

4.8. Network bridging

Purpose

To identify requirements and limits for the use of several (possibly heterogeneous) segments in a CCS network.

Description of the experiment

Two CCS network segments shall be communicated through a bridge.

PCT configuration

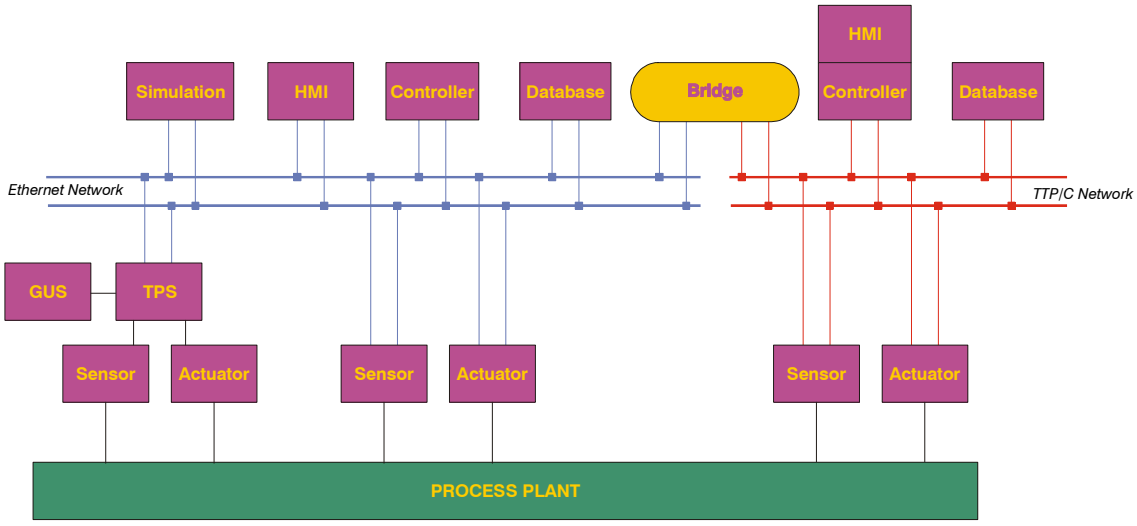

Figure 10:Network bridging configuration

Tests and measurements

1. Visibility of nodes in different segments
2. Identification of limits for hard real-time operation over bridges

4.9. Error management

Besides the indicated tests and measurements for every experiment there are two general ones:

1. The register of the relevant incidents.
2. The performance of the system under faulty conditions.

5 Satisfaction of Requirements

A formal statement of the satisfaction of the requirements specification included in document D4.1 by the designed Process Control Tested follows.

All the requirements are satisfied, EXCEPT the ones related to the hot-replacement of components (SR17, SR18 and SR319). This desirable functionality would need software whose development exceeds the time scope of the project.

GR1: Representativity

The PCT mimics a process control system: redundant networks (SR6) with instruments, controllers and monitoring nodes.

There is a simple process plant (neutralization tank) with a pHmeter and flow control (SR1). The instruments can be connected to a commercial DCS (SR4) or directly (wrapped) to the network (SR2). Controllers can be CCS nodes (SR3) or the ones in the commercial DCS (SR4).

Two networks are constructed: Ethernet (SR6) with TCP/IP (SR7) and TTP/C (SR8). The bridging of several (possibly heterogeneous) segments (SR9, SR10) is planned. There are simulation (SR5), database (SR14) and HMI (SR15) nodes.

The scalability (capacity test, SR12) and synchronization will be measured (GPS, SR13) in experiments. The use of synchronization methods has to be evaluated in tests.

GR2: Reconfigurability

The PCT has a modular structure (SR16) that easily allows the building of different topologies.

Hot-replaceability of hardware (SR17) and software (SR18) components is NOT expected to be accomplished in the PCT.

GR3: Testability

The PCT has been designed to perform test on process control, but it is only to a limited extent a hard real-time testbed.

All the nodes are visible by design (SR19) and the software components will be provided of monitoring tools for time stamping (SR21) and logging on the database (SR20), that has a hard-disk with enough capacity for recording the data generated in experiments (SR22).

The following experiments are programmed:

1. CORBA control loops (SR23)
2. Integration of legacy systems (SR33)
3. Asynchronous events management (SR26)
4. Distributed simulation (SR29)
5. Interaction of simulation objects with control agents (SR27)
6. Intensive data traffic (SR24, SR25)
7. Concurrency (SR30)
8. Network bridging (SR28)
9. Error management (SR32)

As it has been said above, no provision for hot-replacing of components has been made, what means that SR31 will NOT be satisfied.

GR4: Cost-adapted

As by design, the cost of the PCT is in accordance with the project budget (SR34).

GR5: Non risky

The process plant is a small set with essentially safe chemical components (SR35) under normal conditions. Experiments are performed at room temperature and pressure (SR36).