Rapid prototyping of the ITER safety system

June 3, 2010– National Instruments

G. De Tommasi[1]

[1]CREATE – Università di Napoli Federico II

Outline

Motivations

Rapid Prototyping of the CSS

Requirements

Setup

Discussion points

Outline

Motivations

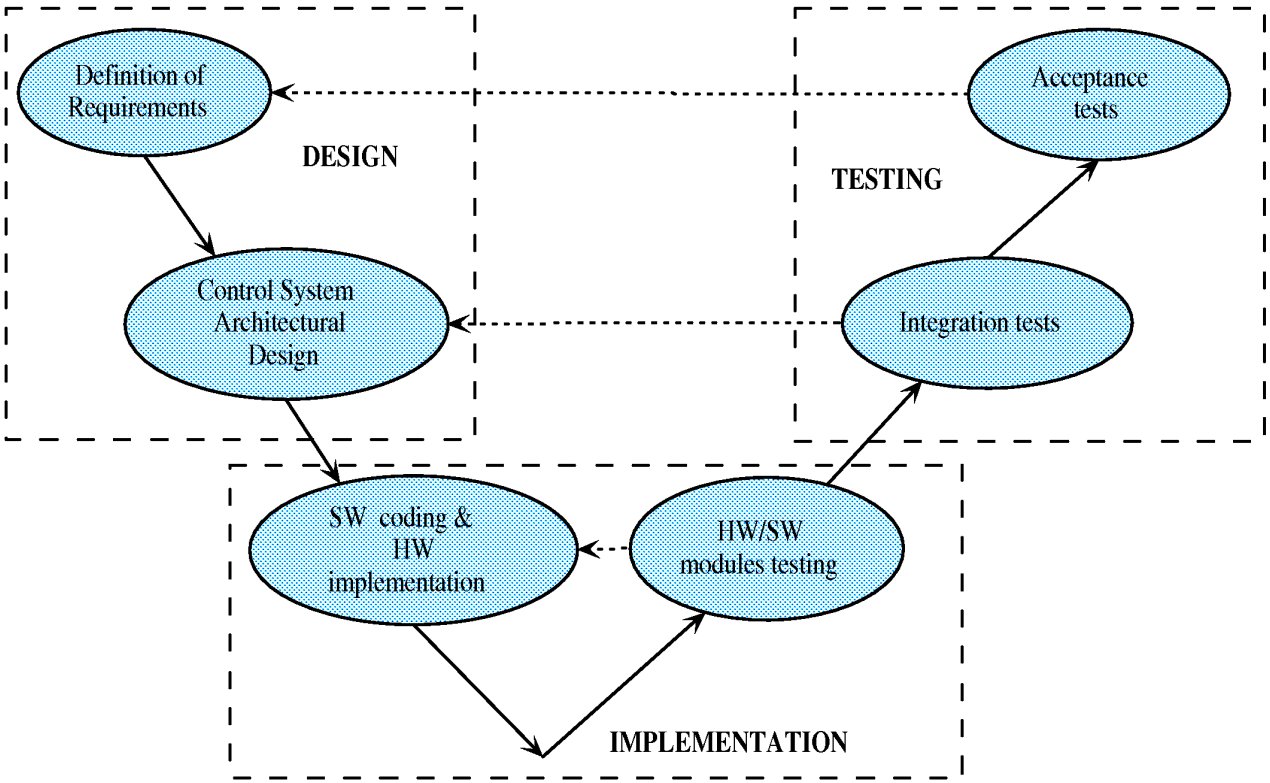
Rapid Prototyping of the ITER Central Safety System

- System requirements
- Architecture overview

Discussion points

Outline
Motivations
Rapid Prototyping of the CSS
Requirements
Setup
Discussion points

Development of control systems – V Cycle 1/2



The traditional development cycle of control systems follows the **three** phases: design, implementation, testing.

Outline

Motivations

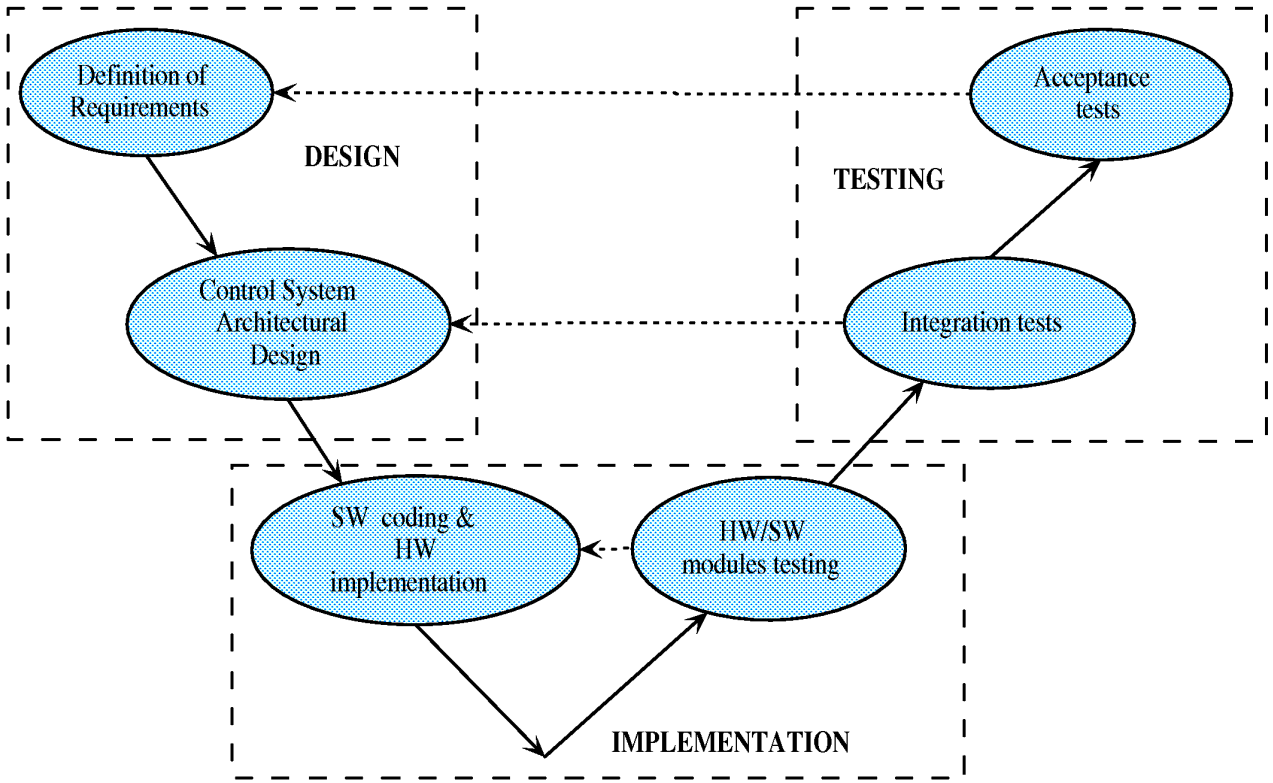
Rapid Prototyping of the CSS

Requirements

Setup

Discussion points

Development of control systems – V Cycle 2/2



- the test and validation phase is **mainly carried out on-site**.

Outline
Motivations
Rapid Prototyping of the CSS
Requirements
Setup
Discussion points

Motivations

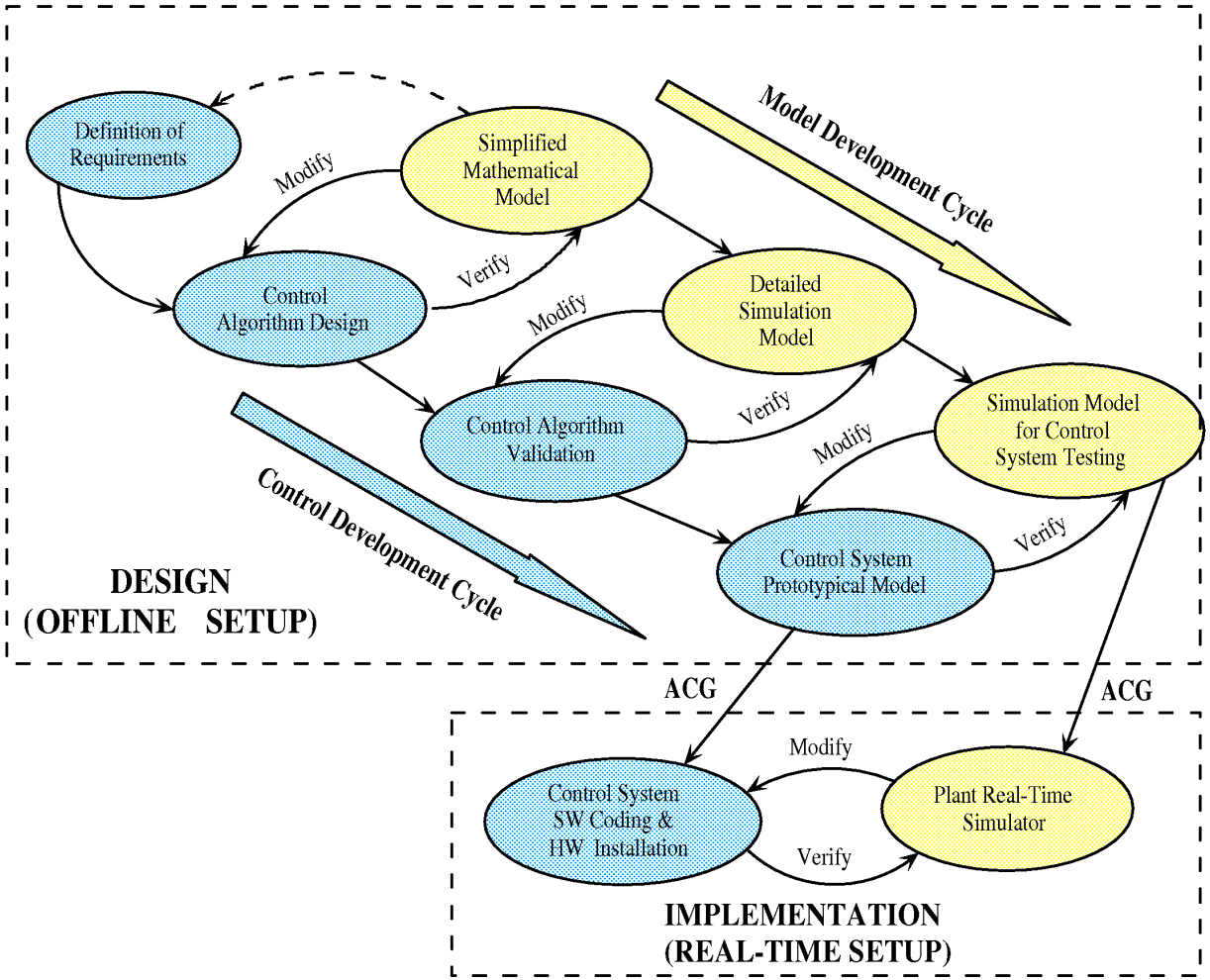
Due to the additional efforts and costs, often the architectural design is carried out without any modeling and simulation support.
However, if

- the system to be controlled is *non-conventional* or new;
- the required performances are very demanding;
- the plant is not yet available (the ITER case) and/or the testing on-site is very risky;

then the use of modeling and simulation tools during the design phase becomes highly recommended.

Outline
Motivations
Rapid Prototyping of the CSS
Requirements
Setup
Discussion points

Design aided with modeling, simulation and rapid prototyping tools



Outline

Motivations

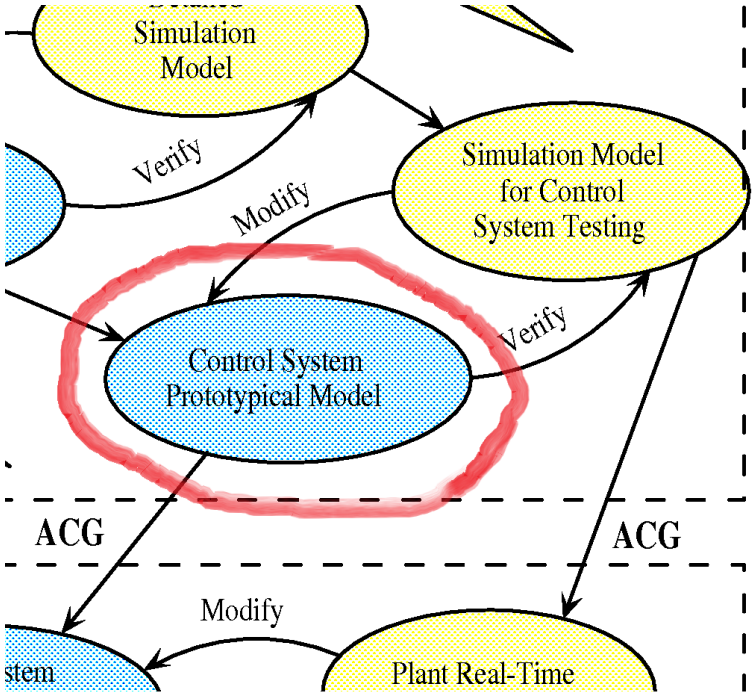
Rapid Prototyping of the CSS

Requirements

Setup

Discussion points

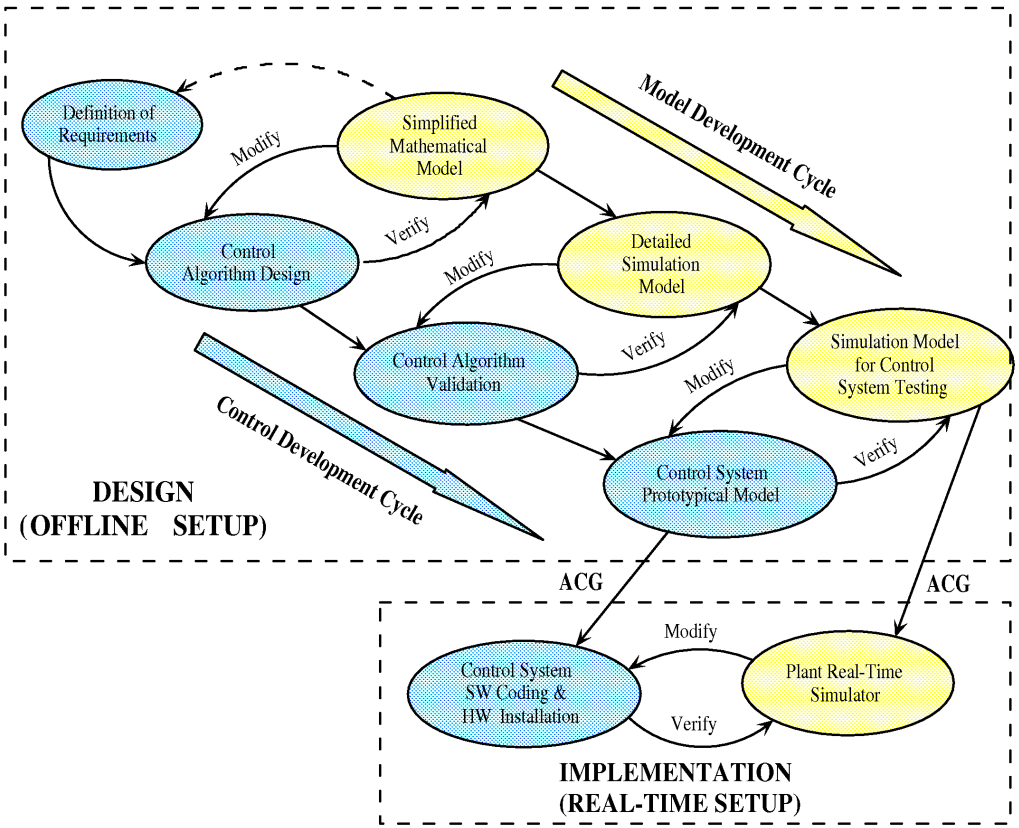
Prototype of the control system as formal description of the requirements



- The high-level description of the prototype represents an unambiguous description of the control system behaviour.
- It can be used as formal specification of the requirements.

Outline
Motivations
Rapid Prototyping of the CSS
Requirements Setup
Discussion points

Tools



The proposed approach is based on the availability of

- several plant models (at different level of details)
- **automatic tools** for the rapid prototyping of both control systems and plant models

Outline

Motivations

Rapid Prototyping of the CSS

Requirements

Setup

Discussion points

ITER Central Safety System

The ITER Central Safety System (CSS)

- is the system responsible for nuclear safety on the plant (there is Tritium)!
- is has a distributed architecture (local Plant Safety Systems + Central Safety System)
- it is mainly an event-driven automation system
- very simple computations
- actuators should be very fast!

Outline
Motivations
Rapid Prototyping of the CSS
Requirements
Setup
Discussion points

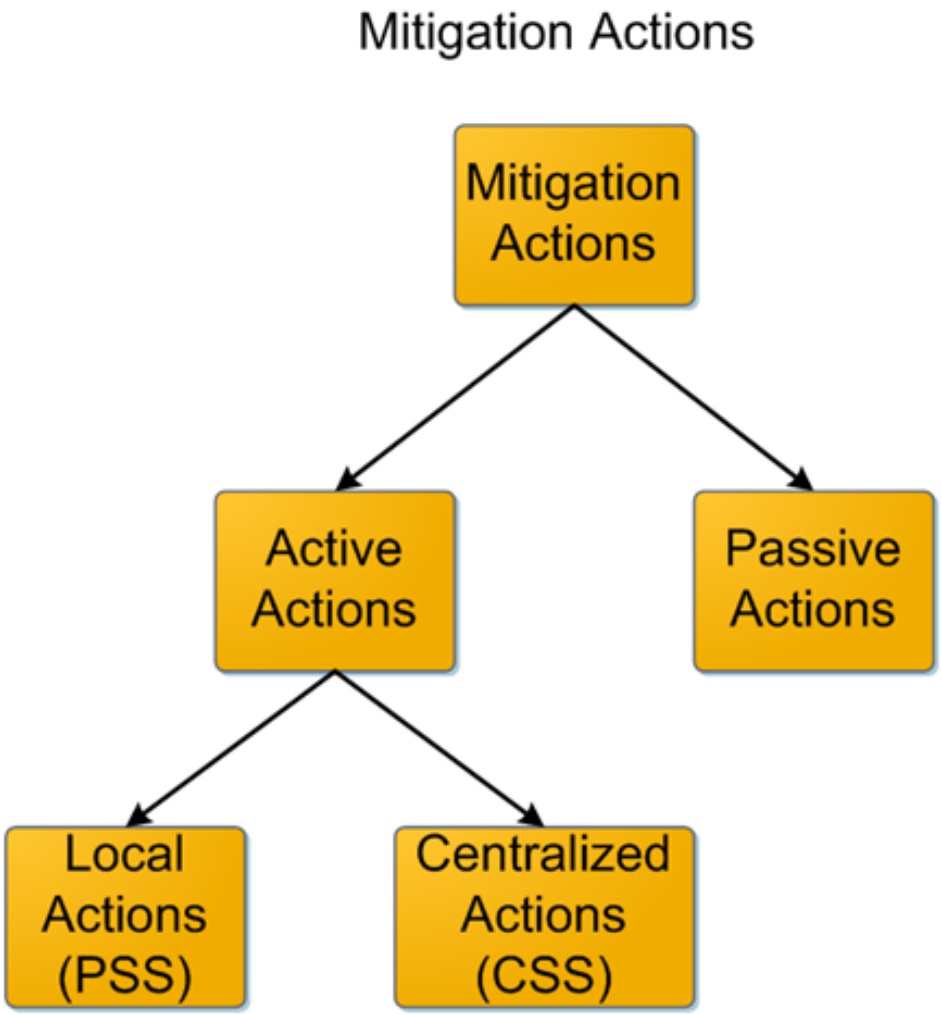
ITER Central Safety System - System Requirements

The functional requirements for the ITER CSS have been specified in terms of

- **Mitigation Actions** - are the actions that must be carried out by the CSS after the occurrence of a safety relevant fault. Hence the *Mitigation Actions* provide the specification for the **control system prototype (CSS-PROT)**.
- **Fault Conditions** - are the initiating events that follow the occurrence of relevant faults for nuclear safety. The *Fault Conditions* represent the specifications for the **plant model (CSS-OPS)**.
  Example a safety relevant fault is a malfunction of the cooling system, while the related initiating event can be an overpressure in the pipeline.

Outline
Motivations
Rapid Prototyping of the CSS
Requirements
Setup
Discussion points

Classification of the Mitigation Actions



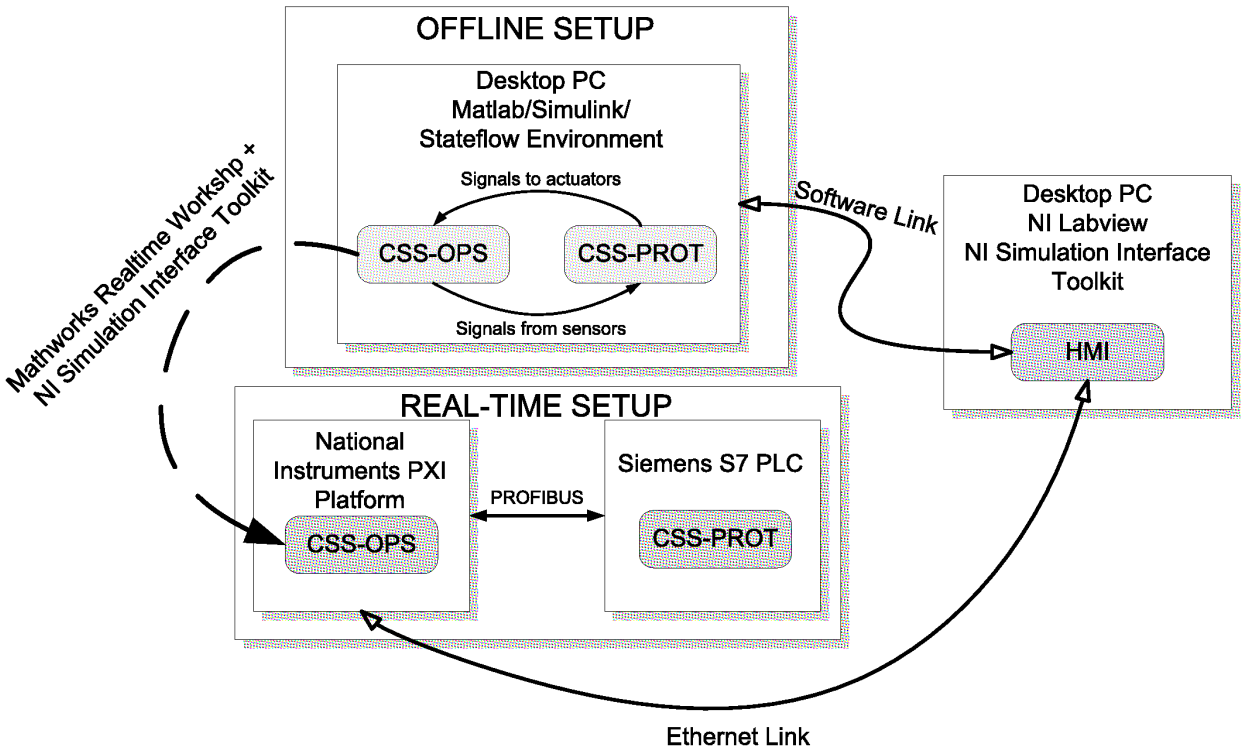
Outline
Motivations
Rapid Prototyping of the CSS
Requirements
Setup
Discussion points

Setup 1/3

- A simplified model of both the plant (CSS-OPS) and of the controller (CCS-PROT) have been developed in the Matlab/Simulink environment.
- Exploiting the Labview Simulation Interface Toolkit (SIT) we:
  - Develop a common Human-Machine Interface both for the *offline* and for the *real-time* (that can be accessed even remotely, thanks to a web server application)
  - Deploy the plant on a PXI Real-Time target to perform HIL simulations with a PLC-based controller

Outline
Motivations
Rapid Prototyping of the CSS
Requirements
Setup
Discussion points

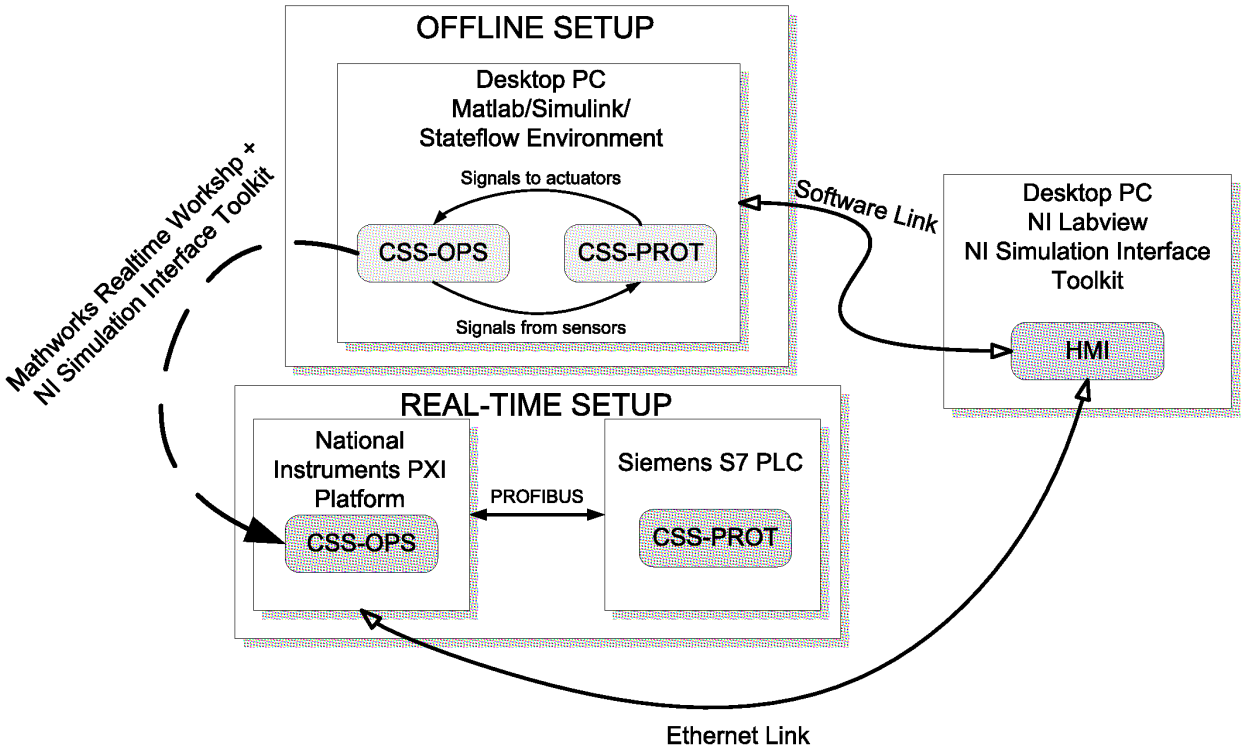
Setup 2/3



Two operational setups have been provided

- the *offline setup* to perform the design of the control system,
- the *real-time setup* whereto perform test and validation with hardware-in-the-loop (HIL) simulations.

Setup 3/3



In the *offline setup*:

- the prototype of the control system is written in a high level language, such as Sequential Functional Charts (SFCs) or Stateflow. This is an high level description of the control system functional requirements;
- the whole control system is tested against a simplified version of the plant model.

Outline

Motivations

Rapid Prototyping of the CSS

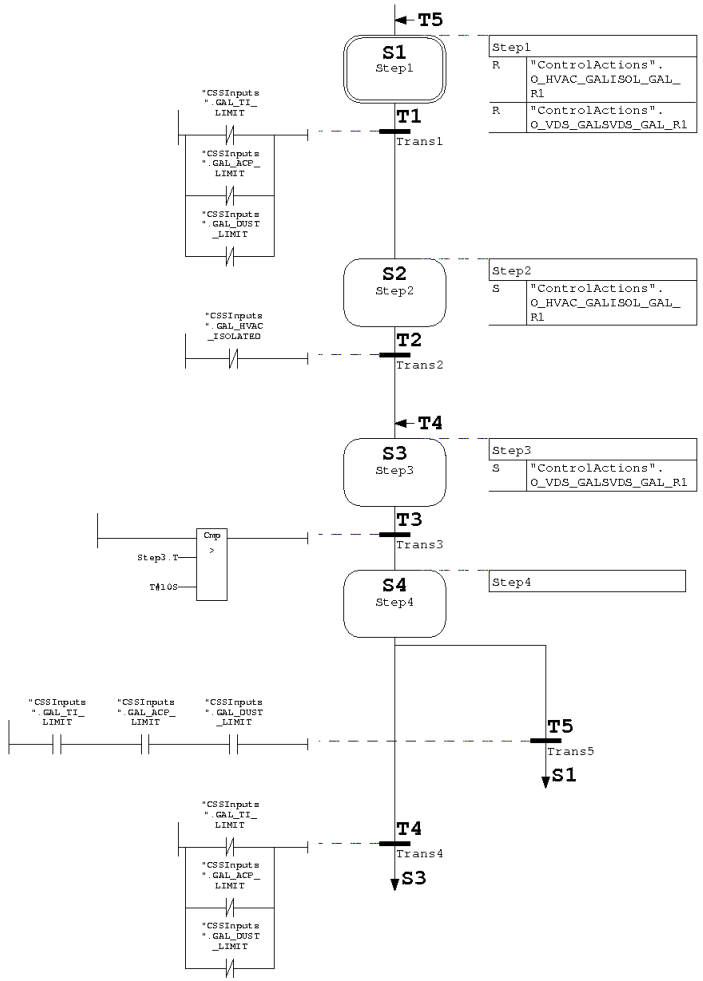
Requirements

Setup

Discussion points

SFC example

The specification for the CSS are described by SFCs, which are a formal description of the controller behavior.



Outline

Motivations

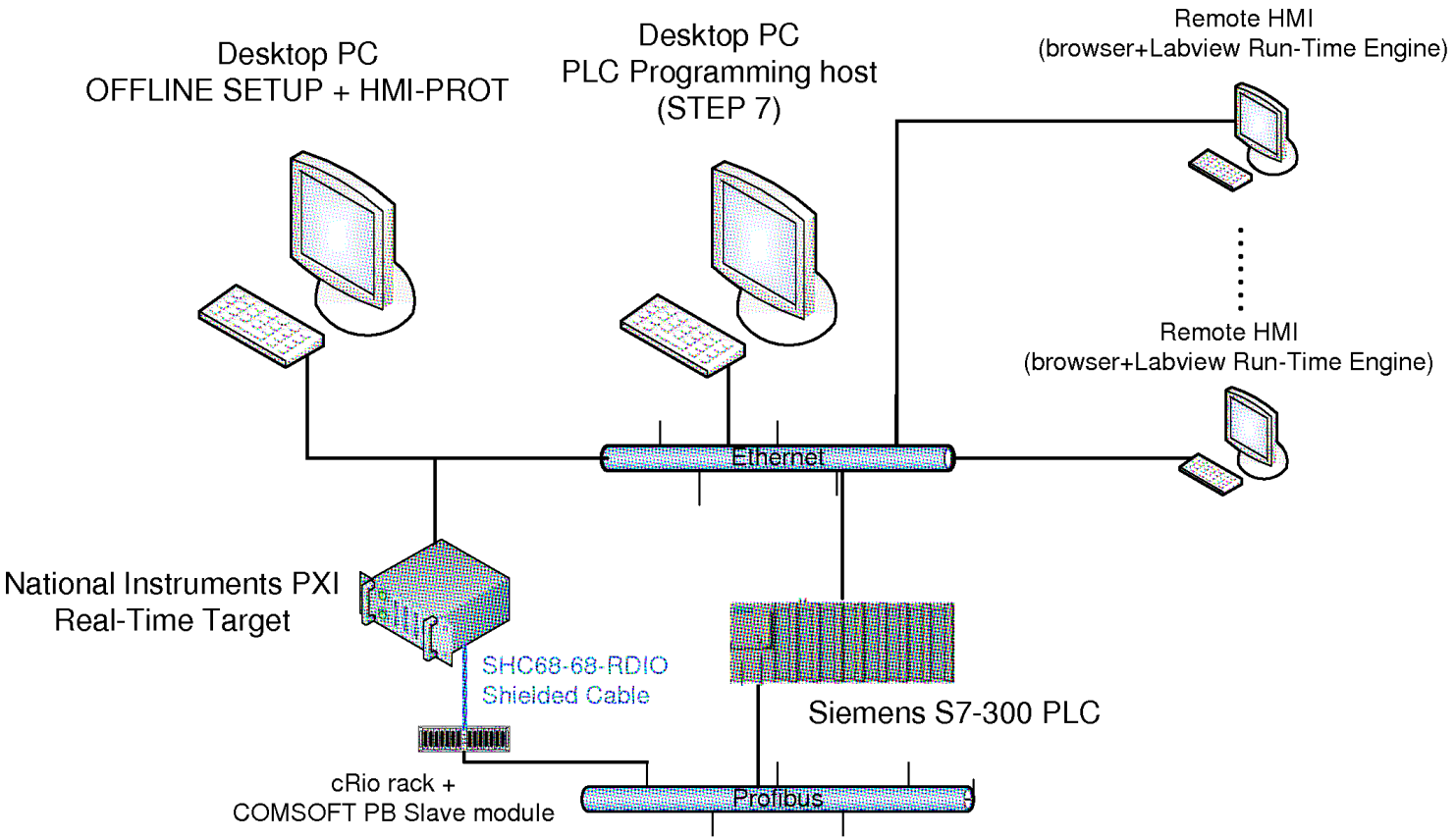
Rapid Prototyping of the CSS

Requirements

Setup

Discussion points

Experimental setup deployed at ITER for the rapid prototyping of the CSS



Outline

Motivations

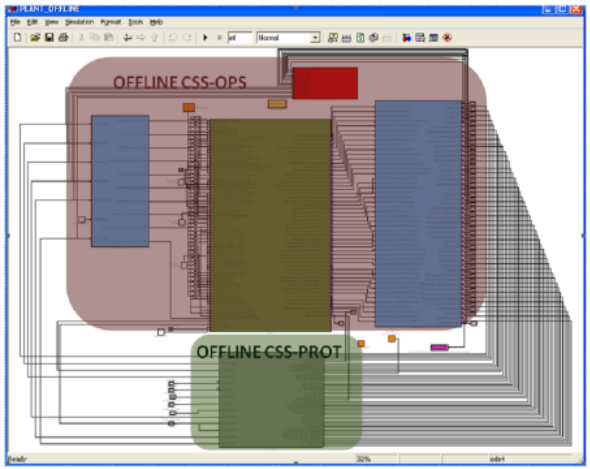
Rapid Prototyping of the CSS

Requirements

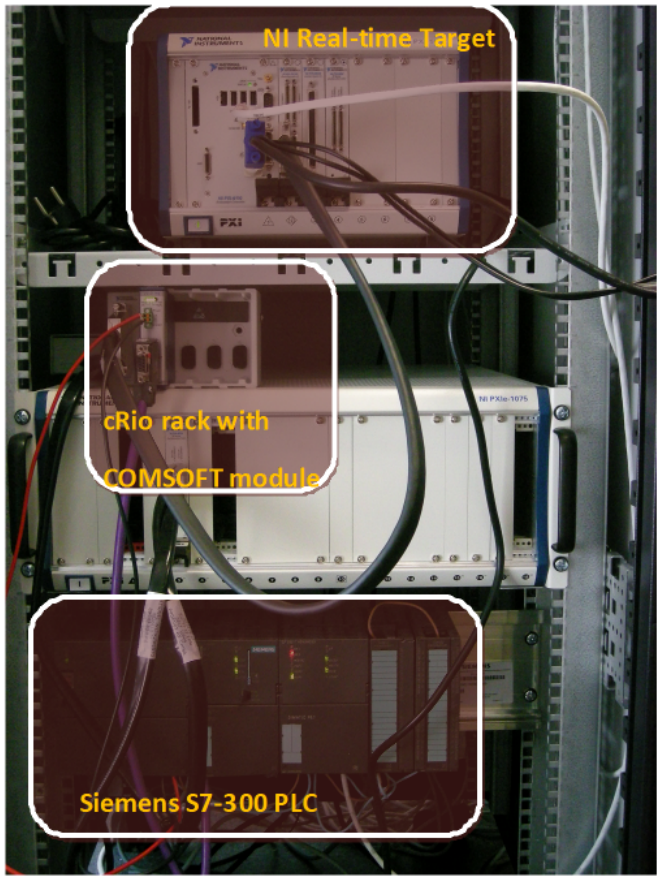
Setup

Discussion points

Rapid prototyping via NI Labivew SIT



Labview SIT

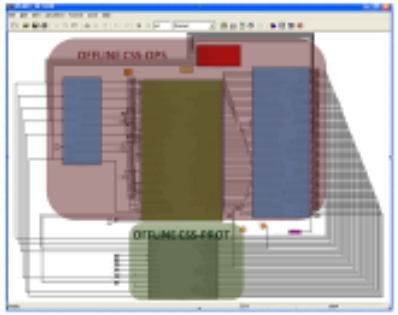


Outline
Motivations
Rapid Prototyping of the CSS
Requirements
Setup
Discussion points

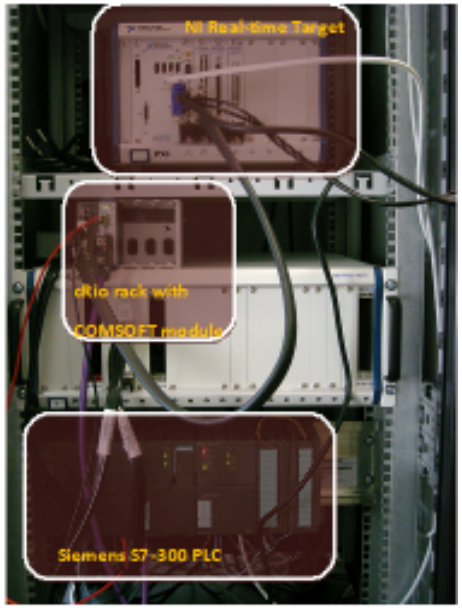
Common HMI with Labview

Local or Remote (via Labview Runtime Engine)

Offline environment



NI Real-time target



Outline
Motivations
Rapid Prototyping of the CSS
Requirements
Setup
Discussion points

Discussion Points

- We had no problems for the "rapid prototyping" of the plant model (thanks to SIT)

Outline
Motivations
Rapid Prototyping of the CSS
Requirements
Setup
Discussion points

Discussion Points

- We had no problems for the "rapid prototyping" of the plant model (thanks to SIT)
- Problems come with the (event driven) controller:

Outline
Motivations
Rapid Prototyping of the CSS
Requirements
Setup
Discussion points

Discussion Points

- We had no problems for the "rapid prototyping" of the plant model (thanks to SIT)
- Problems come with the (event driven) controller:
  - we would like to specify it in terms of SFCs (or equivalently with Finite State Machines, Petri Nets, Stateflow, etc.)

Outline
Motivations
Rapid Prototyping of the CSS
Requirements
Setup
Discussion points

Discussion Points

- We had no problems for the "rapid prototyping" of the plant model (thanks to SIT)
- Problems come with the (event driven) controller:
  - we would like to specify it in terms of SFCs (or equivalently with Finite State Machines, Petri Nets, Stateflow, etc.)
  - we would like to rapid prototyping the controller and deploy it on a different vendor HW architecture (Siemens/STEP 7 in the case of ITER)

Outline
Motivations
Rapid Prototyping of the CSS
Requirements
Setup
Discussion points

Suggestions

- Do we really need Matlab/Simulink to model the controller/plant behavior ?

Outline
Motivations
Rapid Prototyping of the CSS
Requirements
Setup
Discussion points

Suggestions

- Do we really need Matlab/Simulink to model the controller/plant behavior ?
  - For advanced plasma model codes maybe YES (free-boundary nonlinear magnetic reconstruction codes)
  - In the case of a CSS oriented plant model the answer (I think) is NO !

Outline
Motivations
Rapid Prototyping of the CSS
Requirements
Setup
Discussion points

Suggestions

- Do we really need Matlab/Simulink to model the controller/plant behavior ?
  - For advanced plasma model codes maybe YES (free-boundary nonlinear magnetic reconstruction codes)
  - In the case of a CSS oriented plant model the answer (I think) is NO !
- However Labview CD&S must be promoted in University labs and System and Control classes!

Outline
Motivations
Rapid Prototyping of the CSS
Requirements
Setup
Discussion points