# A flexible architecture for the rapid prototyping of control systems in fusion experiments

July 7, 2010 – ISIE 2010 – Bari – Italy

G. Ambrosino[1] M. Banfi[2] G. Carannante [1]
G. De Tommasi[1] A. Mandelli[2] A. Pironti[1]
[1]CREATE – Università di Napoli Federico II
[2]National Instrument Italy



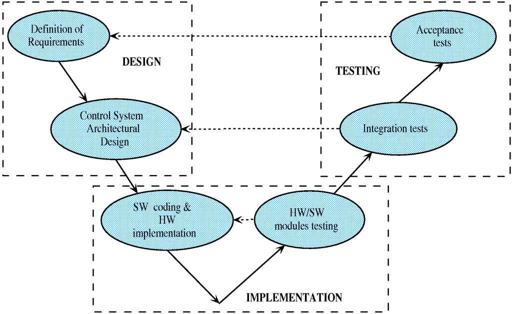
# Outline

## Motivations

## Rapid Prototyping of the ITER Central Safety System

- ITER overview
- System requirements
- Architecture overview
- Examples

# Development of control systems – V Cycle 1/2

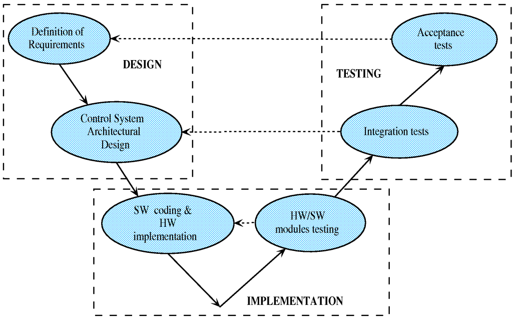



The traditional development cycle of control systems follows the **three** phases:

- design
- implementation
- testing



# Development of control systems – V Cycle 2/2




- the design phase ends with the functional requirement specification;
- the implementation phase starts with the software requirements;
- the test and validation phase is **mainly carried out on-site**, except for standard single modules testing.

# Motivations – 1/2

The V-cicle has several drawbacks:

- **Uncertainty of the control system performance**: due to the absence of simulation tools;
- **Incompleteness in the specification of Functional Requirements**: plant situations neglected and/or not identified;
- **Mistranslation** of the Functional Requirements in SW Specifications;
- **Errors in the Implementation Phase** (SW coding and installation on dedicated HW) not detected before on-site tests;

# Motivations – 2/2

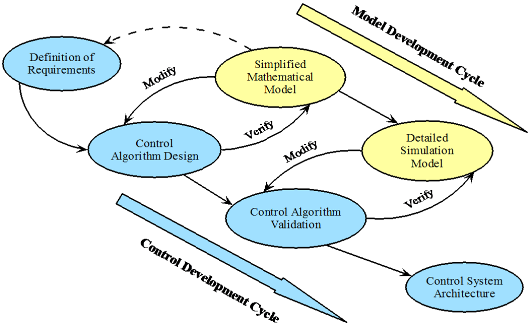
Due to the additional efforts and costs, often the architectural design is carried out without any modeling and simulation support.

However, if

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

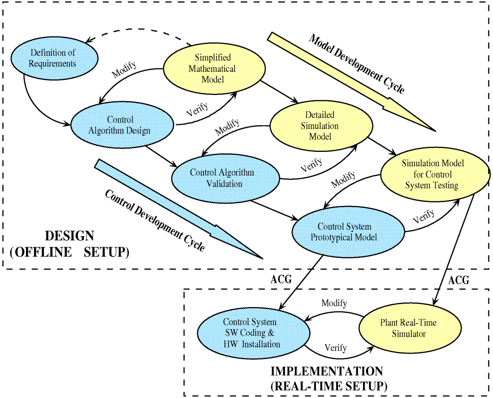
**then the use of modeling and simulation tools during the design phase becomes highly recommended.**

# Design phase with modeling and simulation tools




- A simulation model development cycle runs in parallel with a control system development cycle.
- A simplified mathematical model aides the requirement definition and the preliminary control design.
- The algorithm validation is carried out by means of detailed simulations model.

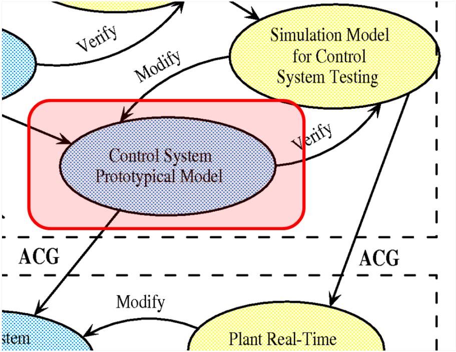
# Rapid prototyping




The following step is the Rapid Prototyping:

- The prototypical model is tested against a plant simulator whose detail level can be chosen by the designer.

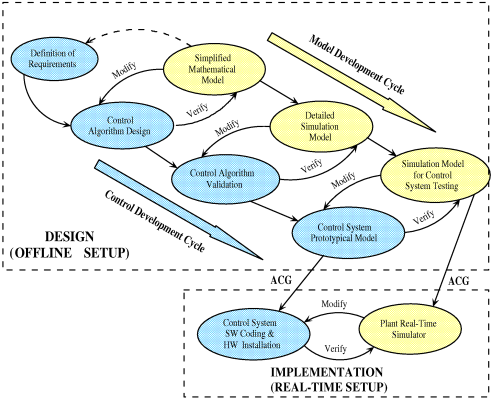
# Prototype of the control system as formal description of the requirements




- 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**.



# Tools – 1/2

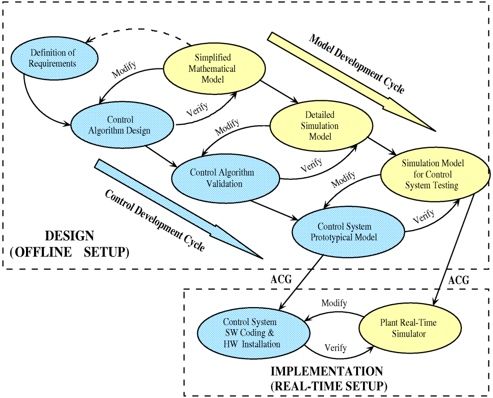



The proposed approach is based on the availability of

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

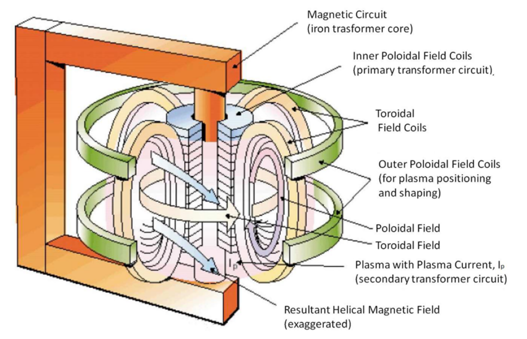


# Tools – 2/2



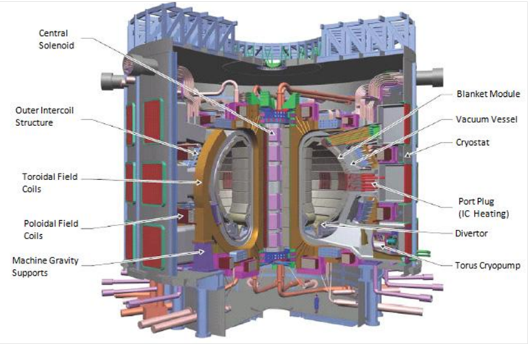

Once the real implementation of the control system will be delivered by the contractors, it can be tested against the real-time simulator before the installation on the plant.

# Tokamak




A tokamak is an electromagnetic machine containing a fully ionised gas (plasma) at about 100 million degrees within a torus shaped vacuum vessel. Poloidal and toroidal field coils, together with the plasma current, generate a spiralling magnetic field that confines the plasma.

# ITER




ITER is a joint venture of 7 participant teams (EU plus Switzerland, Japan, the People's Republic of China, India, the Republis of Korea, Russia and USA). It has been designed to demonstrate the feasibility of fusion energy for peaceful purposes.

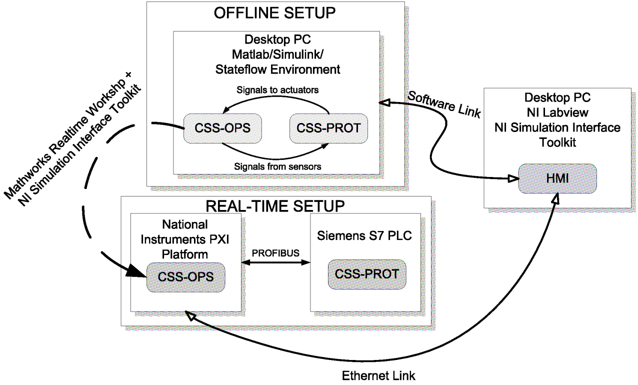
# ITER Central Safety System - System Requirements

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 simulator (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.

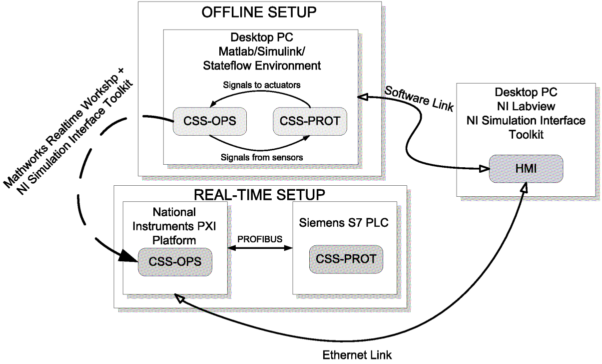
# Setup 1/3




Two operational setups have been provided

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

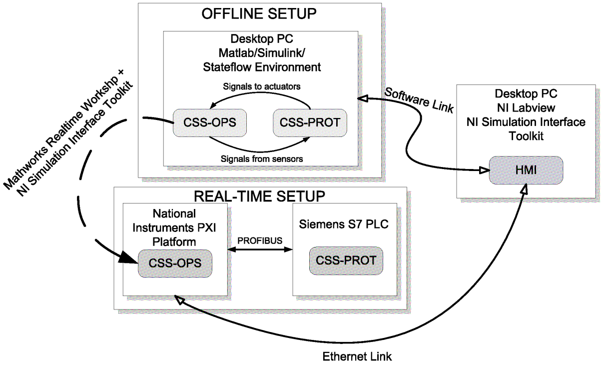
# Setup 2/3




In the *offline setup*:

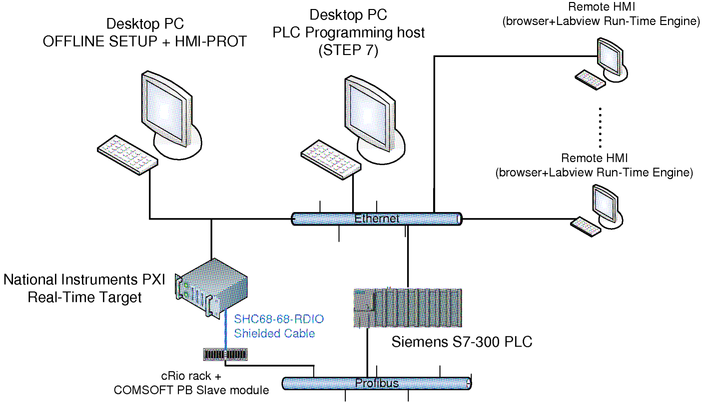
- the prototype of the control system is written in a high level language, such as Sequential Functional Charts (SFCs) or Stateflow. This is an high level description of the control system functional requirements;
- the **whole control system** is tested against the plant simulator.

# Setup 3/3




By using automatic code generation (ACG) tools, the control system prototype and the plant simulator are deployed on real-time targets, in order to validate the real implementation of the safety control system by means of HIL simulations.

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




- The controller runs on the Siemens PLC.
- The plant simulator runs on the NI Real-Time Target.
- Several users can connect remotely to the HMI to monitoring and/or control (inject faults, switch on manual actions ...).

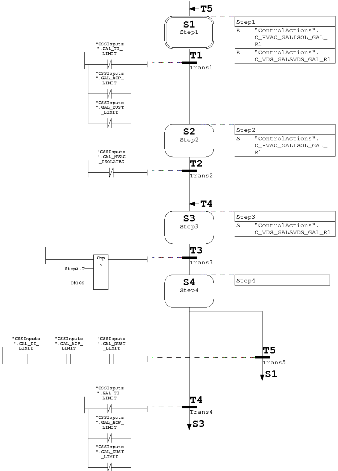


# High concentration of tritium and/or contaminated products in the Tokamak Gallery

Two *Mitigation Actions* have to be performed

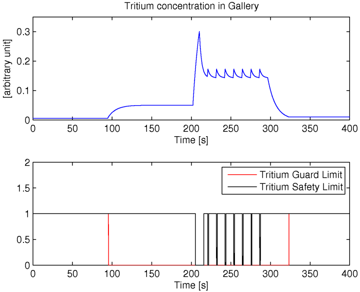
- Service Vacuum Vent Detritiation System
- Relief to Normal Vent Detritiation System

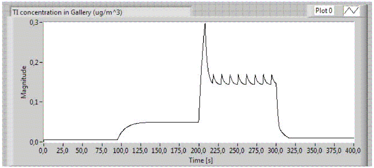
The specifications for the CSS are described by two SFCs, which represent also a formal description of the CSS-PROT behaviour.



# Offline and HIL simulations

Two different values of the tritium inlet flow in the Tokamak Gallery are set, at $t \cong 99\ s$ and $t \cong 200\ s$, respectively. The first change causes the trespass of the guard limit, while the second causes the safety limit to be exceeded.




Offline (left) and HIL simulation (right).

# Conclusions

- **Questions ?**

**Thank you!**