Rapid prototyping of the ITER safety system

February 24, 2010 – NIdays 2010 – Big Physics Symposium

G. Ambrosino[1] G. Carannante[1] G. De Tommasi[1]
A. Pironti[1] L. Scibile[2]
[1]CREATE – Università di Napoli Federico II
[2]ITER Organization - Interlock and Safety Systems

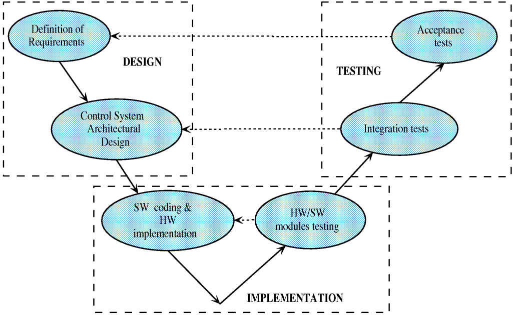
Outline

Motivations

Rapid Prototyping of the ITER Central Safety System

- System requirements
- Architecture overview
- Examples

Development of control systems – V Cycle 1/2



Definition of Requirements

DESIGN

Control System Architectural Design

Acceptance tests

TESTING

Integration tests

SW coding & HW implementation

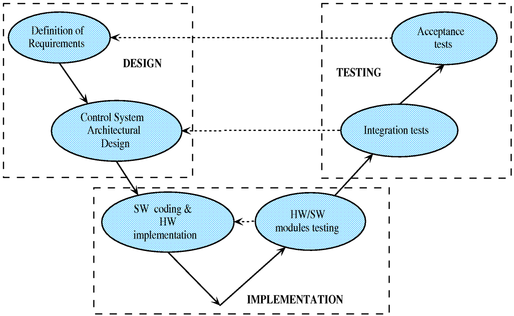
HW/SW modules testing

IMPLEMENTATION

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

- design
- implementation
- testing

Development of control systems – V Cycle 2/2


Definition of Requirements
DESIGN
Control System Architectural Design
Acceptance tests
TESTING
Integration tests
SW coding & HW implementation
HW/SW modules testing
IMPLEMENTATION

- 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**.

Motivations

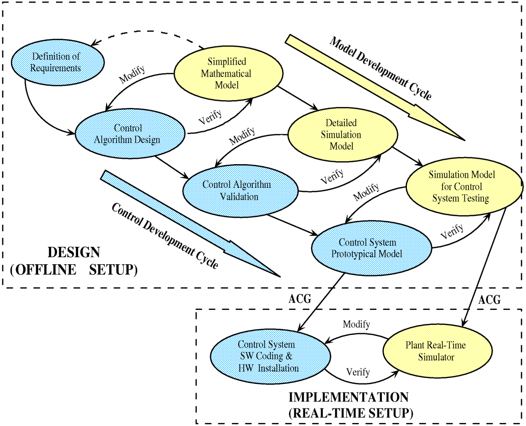
Due to the additional efforts and costs, often the architectural design is carried out without any modeling and simulation support.
However, if

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

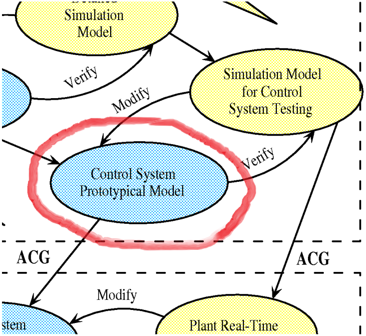
then the use of modeling and simulation tools during the design phase becomes highly recommended.

Design aided with modeling, simulation and rapid prototyping tools

For the design and development of a critical system, it is more appropriate to resort to modeling, simulation and rapid prototyping tools.

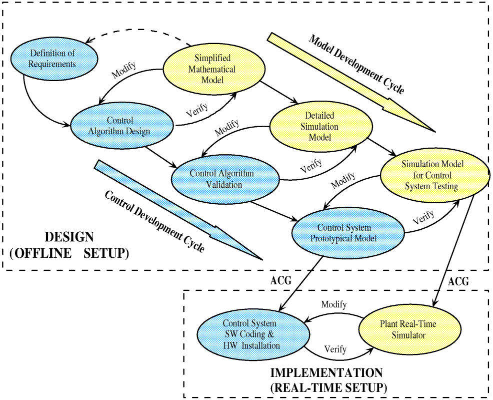

Definition of Requirements
Simplified Mathematical Model
Modify
Verify
Model Development Cycle
Control Algorithm Design
Detailed Simulation Model
Modify
Verify
Control Algorithm Validation
Simulation Model for Control System Testing
Modify
Verify
Control System Prototypical Model
Control Development Cycle
DESIGN (OFFLINE SETUP)
ACG
ACG
Control System SW Coding & HW Installation
Modify
Verify
Plant Real-Time Simulator
IMPLEMENTATION (REAL-TIME SETUP)

Prototype of the controlo system as formal description of the requirements


Simulation Model
Verify
Modify
Simulation Model for Control System Testing
Control System Prototypical Model
Verify
ACG
ACG
Modify
stem
Plant Real-Time

- 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


Definition of Requirements
Simplified Mathematical Model
Modify
Verify
Control Algorithm Design
Detailed Simulation Model
Modify
Verify
Control Algorithm Validation
Simulation Model for Control System Testing
Modify
Verify
Control System Prototypical Model
Model Development Cycle
Control Development Cycle
DESIGN
(OFFLINE SETUP)
ACG
ACG
Modify
Control System SW Coding & HW Installation
Plant Real-Time Simulator
Verify
IMPLEMENTATION
(REAL-TIME SETUP)

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

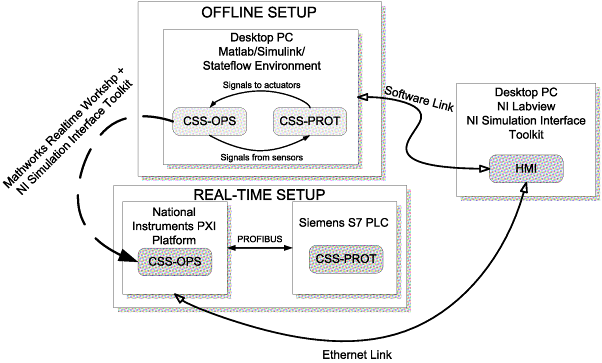
ITER Central Safety System - System Requirements

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.

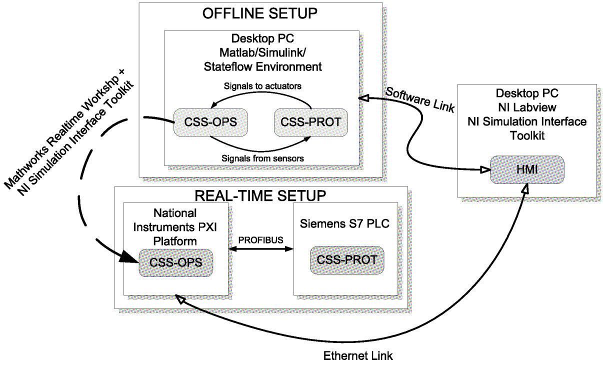
Setup 1/3



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.

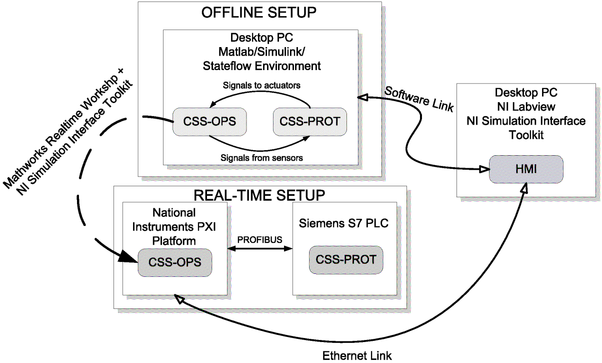
Setup 2/3



In the *offline setup*:

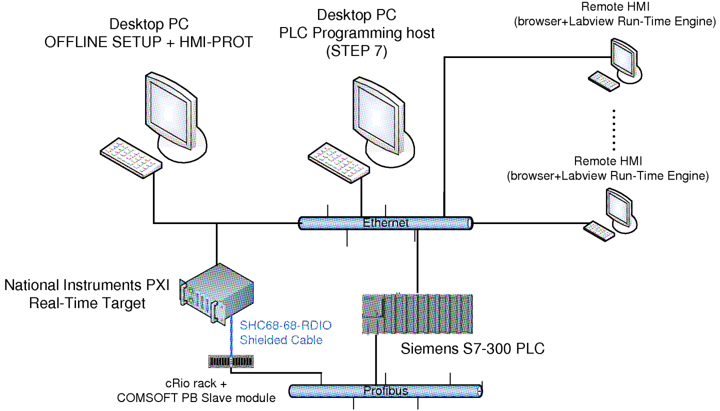
- the prototype of the control system is written in a high level language, such as Sequential Functional Charts (SFCs) or Stateflow. This is an high level description of the control system functional requirements;
- the whole control system is tested against a simplified version of the plant model.

Setup 3/3



By using automatic code generation (ACG) tools, the control system prototype and the plant model 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

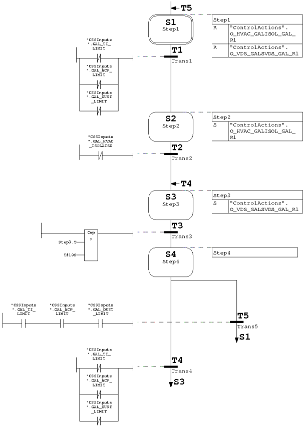


High concentration of tritium and/or contaminated products in the Tokamak Gallery

Two *Mitigation Actions* have to be performed

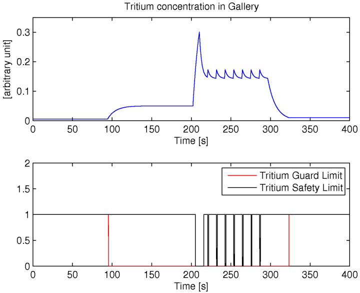
- Service Vacuum Vent Detritiation System
- Relief to Normal Vent Detritiation System

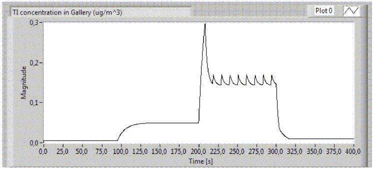
The specification for the CSS are described by two SFCs, which represent also a formal description of the CSS-PROT behaviour.


T5
S1
Step1
Step1
R "ControlActions".O_HVAC_GALISOL_GAL_R1
R "ControlActions".O_VDS_GALSVDS_GAL_R1
"CSSInputs".GAL_TI_LIMIT
"CSSInputs".GAL_ACP_LIMIT
"CSSInputs".GAL_DUST_LIMIT
T1
Trans1
S2
Step2
Step2
S "ControlActions".O_HVAC_GALISOL_GAL_R1
"CSSInputs".GAL_HVAC_ISOLATED
T2
Trans2
T4
S3
Step3
Step3
S "ControlActions".O_VDS_GALSVDS_GAL_R1
Cmp
>
Step3.T
T#10S
T3
Trans3
S4
Step4
Step4
"CSSInputs".GAL_TI_LIMIT
"CSSInputs".GAL_ACP_LIMIT
"CSSInputs".GAL_DUST_LIMIT
T5
Trans5
S1
"CSSInputs".GAL_TI_LIMIT
"CSSInputs".GAL_ACP_LIMIT
"CSSInputs".GAL_DUST_LIMIT
T4
Trans4
S3

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.


Tritium concentration in Gallery
[arbitrary unit]
Time [s]
Tritium Guard Limit
Tritium Safety Limit
Time [s]


TI concentration in Gallery (ug/m^3)
Plot 0
Magnitude
0,3
0,2
0,1
0,0
0,0
25,0
50,0
75,0
100,0
125,0
150,0
175,0
200,0
225,0
250,0
275,0
300,0
325,0
350,0
375,0
400,0
Time [s]