Overview of the Activities for the Central Safety System and the Central Iterlock System of the ITER tokamak

16-18 January 2012 - Jožef Stefan Institute

Gianmaria De Tommasi[1]
[1]CREATE, Università di Napoli Federico II
detommas@unina.it

Outline

Motivations

Rapid Prototyping of the Cental Safety System

Modeling of the Central Interlock System

Modeling support for the ICS prototype built by PROCON Systems

Modeling support for the Quench Loop prototype built by CERN

Required skills

Motivations

This talk. . .

- Introduces the work that has been done for the:
  - *Rapid prototyping of the Central Safety System*
  - *Modeling of the Central Interlock System*
- Shows what were/are the main objectives of these activities
- **Introduces the subjects for possible collaborations**

Motivations

When developing a new system, the architectural design is carried out without any (or with a *small*) modeling and simulation support.

However, when

- 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

the use of modeling and simulation tools during the design phase becomes essential.

Main Objectives

- Use modeling and simulation tools since the early design phase
- **Since ITER systems will be built via procurements:**
  - **modeling can help in the (formal) definition of the system requirements**
  - **models can be used to perform hardware-in-the-loop simulations in order to validate the procured system**

The system = automation system (CSS, CIS,...), control system (shape controller, vertical stabilization,...), plasma diagnostic, ...

ITER Central Safety System

The Central Safety System (CSS)

- is the system responsible for nuclear safety on the ITER plant
- it has a distributed architecture (local Plant Safety Systems + Central Safety System)
- it is mainly an event-driven automation system
- very *simple* computations

Risk events (Fault Conditions)

- **Risks** are the initiating events that follow the occurrence of relevant faults for nuclear safety
- **Risk events** represent the specifications for the **plant model (called 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.

Mitigation Actions (Control Actions)

- **Mitigation Actions** are the actions that must be carried out by the CSS after the occurrence of a safety relevant fault
- **Mitigation Actions** provide the specification for the **control system prototype (called CSS-PROT)**

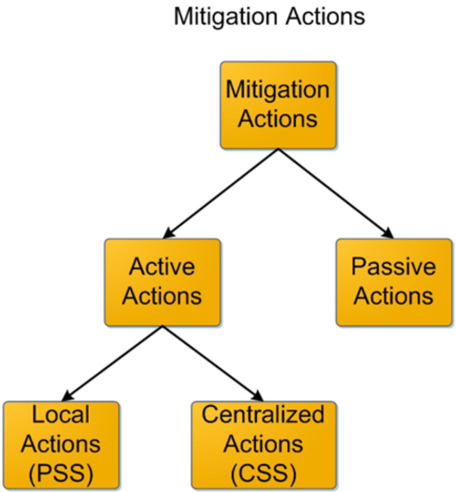
Example: after an overpressure in the main cooling system is detected, the correspondent mitigation action is a *Fast Plasma Shutdown*.

Specification of Mitigation Actions and Risks

Starting from the existing documentation (January 2009, very poor!) we specified:

- a subset of *Mitigation Actions*
- a subset of *Risk Events*

Classification of the Mitigation Actions 1/2



Classification of the Mitigation Actions 2/2

MA ID	Description	CSS (centralized)	PSS (local)	Control Action		Monitoring Action
				Automatic	Manual	
MA_1	Pressure relief from coolant loop to DT		X	X		X
MA_2	FPSS	X		X		X
MA_3	Rupture disk into the VVPSS					X
MA_4	Bleed Line of the VVPSS		X	X		X
MA_5	ST-VS		X	X		X
MA_6	Valve from VV to DT	X			X	X
MA_7	S-ADS + N-VDS-1	X		X		X
MA_8	Vault cooler 100% capacity		X	X		X
MA_9	Stand-by VDS (S-VDS) (95%<2 hr> 99% eficency)	X		X		X

Table 1 - Mitigation Actions. Legend:
Automatic Control Action to be performed by CSS
Manual Control Action to be performed by CSS
Active Control Action to be performed by PSS
Passive Control Action which do not need explicit control logic

CSS Relevant Plant Risks

Risk ID	Description	Subsystems	Mitigation Actions	
			Action #1	Action #2
GAL_R1	High concentration of TI and/or contaminated products in the Gallery	Gallery	MA_9	MA_20
GB_R1	Pressure difference between the Glove Box and the room exceed the safety limit	GB	MA_20	
MAGN_R1	Overpressure in the cryo circuit of the TF coils	TF Coils	MA_26	
PFC_R1	Be surface temperature too high	PFC	MA_2	
PORT_R1	Overpressure in the port cells	Port cells and diagnostic lines	MA_2	MA_12
PORT_R2	High TI concentration in the port cells	Port cells and diagnostic lines	MA_12	
TBM_R1	Overpressure in the cooling water system (TBM)	TBM	MA_2	
TBM_R2	Overtemperature in the cooling water system (TBM)	TBM	MA_2	
TBM_R3	Lost of cooling water flow (LOFA) in the cooling water system (TBM)	TBM	MA_2	
TBUILD_R1	High concentration of TI and/or contaminated products in the T-Builiding	T-Building	MA_9	
TCWS_R1	Overtemperature in one of the 7 PHTS of the cooling water system (TCWS)	TCWS	MA_2	
TCWS_R2	Lost of cooling water flow (LOFA) in one of the 7 PHTS of the cooling water system (TCWS)	TCWS	MA_2	

Risks/Actions Grid

		CSS Mitigation Actions						
		MA_2	MA_7	MA_6	MA_9	MA_12	MA_21	MA_28
Risks	GAL_R1				X		X	
	GB_R1						X	
	MAGN_R1							X
	PFC_R1	X						
	PORT_R1	X				X		
	PORT_R2					X		
	TBM_R1	X						
	TBM_R2	X						
	TBM_R3	X						
	TBUILD_R1				X			
	TCWS_R1	X						
	TCWS_R2	X						
	TCWS_R3	X						
	TCWSV_R1	X				X		
	TCWSV_R2						X	
	VVEXT_R1			X				
	VVEXT_R2		X					
	VVEXT_R3				X			

Risk Description Forms (RDFs) 1/3

For each risk the corresponding Risk Description Form (RDF) specifies:

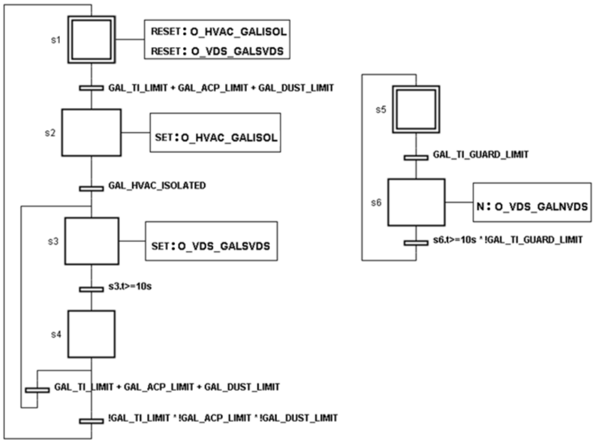
- **General information** about the protection (name, function, risk class, protection architecture type). The most of these data may be not relevant for the development of CSS Prototype and for the CSS Oriented Plant Simulator.
- **I/O signals** to be considered so as to operate the protection.
- **Control Logic** - is the safety logic that implements all the needed Mitigation Actions. **It is specified as an high level Sequential Functional Chart (SFC)** ("behavioral" SFC rather then "operative" SFC).

RDFs 2/3

Protection **name**:	Start VDS when high concentration of TI and/or contaminated products is detected in the Gallery
Protection **function**:	If tritium concentration reaches the guard limit then start N-VDS. If tritium and/or contaminated products concentrations reach the safety limit then S-VDS is started
Protection **for** (People/Environment/Machine):	Environment, People (?)
Risk to protect	Tirtium contamination
Risk description	If the conteminated products concentration in the Gallery is too high there is a risk of Tritium contamination
Risk class	II
SIC classified (NO/YES):	
Protection architecture **type**	E

Sensors					Actuators				
PBS	**Description**	**Signal Tag**	**Type**	**Quant.**	**PBS**	**Description**	**Signal Tag**	**Type**	**Quant.**
6.4	ACP concetration above safety critical limit in the Gallery	I_GAL_ACP_1 I_GAL_ACP_2 I_GAL_ACP_3	Digital	3	3.2 3.2 3.2	Command Gallery S-VDS Command N-VDS in the Gallery Command HVAC isolation in the Galle	O_VDS_GALSVDS O_VDS_GALNVDS O_HVAC_GALISOL	Digital Digital Digital	1 1 1
6.4	Contaminated dust concetration above safety critical limit in the Gallery	I_GAL_DUST_1 I_GAL_DUST_2 I_GAL_DUST_3	Digital	3					
6.4	TI concetration above safety critical limit in the Gallery	I_GAL_TI_1 I_GAL_TI_2 I_GAL_TI_3	Digital	3					
6.4	Gallery HVAC isolated	I_GAL_HVACISOL_1 I_GAL_HVACISOL_2 I_GAL_HVACISOL_3	Digital	3					
6.4	TI concetration above guard limit in the Gallery	I_GAL_TIGUARD_1 I_GAL_TIGUARD_2 I_GAL_TIGUARD_3	Digital	3					

RDFs 3/3



s1
RESET: O_HVAC_GALISOL
RESET: O_VDS_GALSVDS
GAL_TI_LIMIT + GAL_ACP_LIMIT + GAL_DUST_LIMIT
s2
SET: O_HVAC_GALISOL
GAL_HVAC_ISOLATED
s3
SET: O_VDS_GALSVDS
s3.t>=10s
s4
GAL_TI_LIMIT + GAL_ACP_LIMIT + GAL_DUST_LIMIT
!GAL_TI_LIMIT * !GAL_ACP_LIMIT * !GAL_DUST_LIMIT
s5
GAL_TI_GUARD_LIMIT
s6
N: O_VDS_GALNVDS
s6.t>=10s * !GAL_TI_GUARD_LIMIT

From RDFs to a Plant Simulink Models

- A Simulink library of **basic models** was developed starting from the Risks described in the RDFs
- This library was then used to build the CSS-OPS
- A *light* plant model was envisaged, hence **simple** models have been considered:
  - linear time–invariant first order models with saturations
  - bilinear models
  - integrators
  - *simple* static nonlinear models
- A description of the models we used can be found in
  - Software Architectural Detailed Design ITER_D_2MZ2X8

From the RDFs to Control Logics

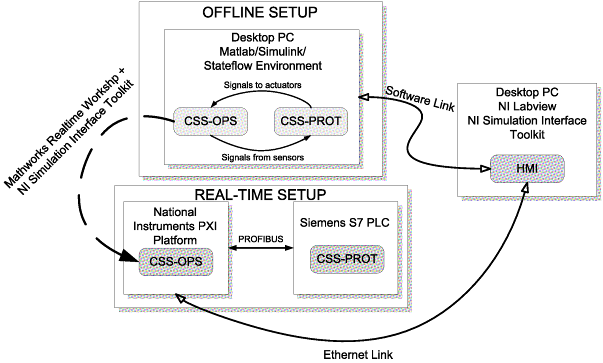
- The CSS-PROT was firstly coded as a set of Stateflow diagrams starting from the SFC control logics specified into the RDFs
- This Simulink/Stateflow prototype was then validated against the CSS-OPS in the Simulink environment
- The CSS-PROT was then deployed on a Siemens S7 PLC and tested against a real-time version of the CSS-OPS, which automatically deployed on a PXI real-time target by using NI Simulation Interface Toolkit (SIT)

Some numbers. . .

The *CSS exercise* was not complete, however we came up with:

- 14 Mitigation Actions
- 47 Risks Events
- A (time–driven) plant model with 70 inputs and 48 outputs

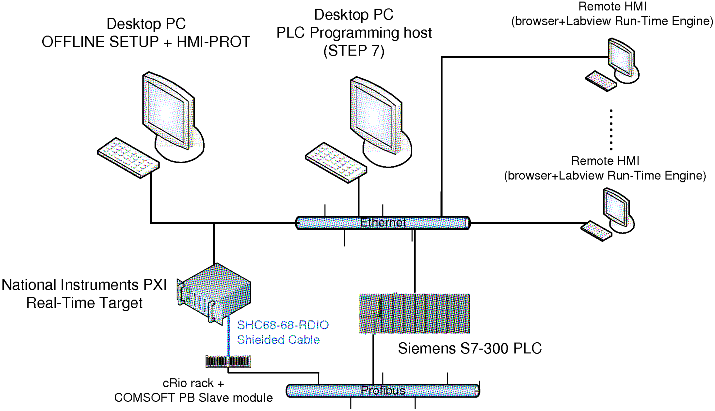
Experimental setup 1/2



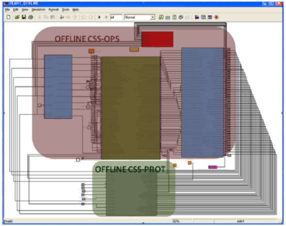
Two operational setups were provided

- 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.

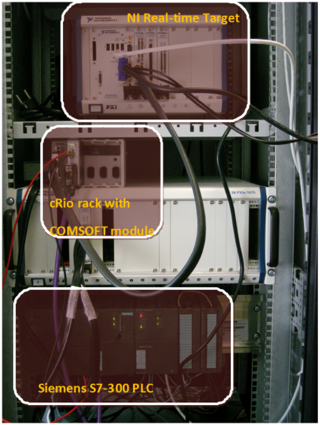
Experimental setup 2/2



Rapid prototyping via NI Labivew SIT

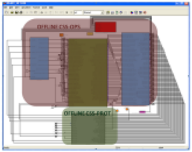


Labview SIT



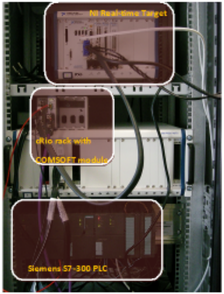
Common HMI with Labview

Offline environment



Local or Remote (via Labview Runtime Engine)

NI Real-time target



Summarizing...

- By using the modeling/simulation environment
  - Risk events
  - Control Logics

  were formally specified
- A procedure to specify the (event–driven) controller architecture in a high level language was provided
- Test and validation of the Control Logics was performed against a (simplified) plant model
- Test and validation of the controller implementation was performed against a real-time version of the plant model

- 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:
  - developed 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)
  - deployed the plant on a PXI Real-Time target to perform HIL simulations with a PLC-based controller

Remarks

- We had no problems for the "rapid prototyping" of the plant model (thanks to National Instruments SIT)
- Problems came with the (event driven) controller:
  - we would like to *rapid prototype* the controller and deploy it on a different vendor HW architecture (Siemens/STEP 7 in the case of ITER)
  - this was not possible with Matlab/Simulink
  - there were some third-party products, but, at that time, they did not work very well

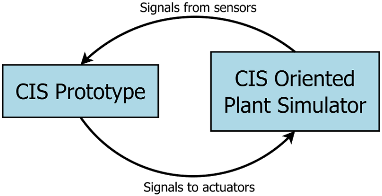
ITER Central Interlock System

The Central Interlock System (CIS)

- provides protection of investment for the ITER tokamak
- it executes automatic interlocks generated on the basis of either the machine status or the operation limits and conditions
- it executes interlock actions manually requested by the operator.

CIS-OPS and CIS-PROT

- The CIS Prototype (CIS-PROT) is a description of the CIS behavior in a high-level programming language. Such high-level software implementation may represents a formal description of the system requirements
- The CIS Oriented Plant Simulator (CIS-OPS) permits to validate the CIS Prototype via simulations



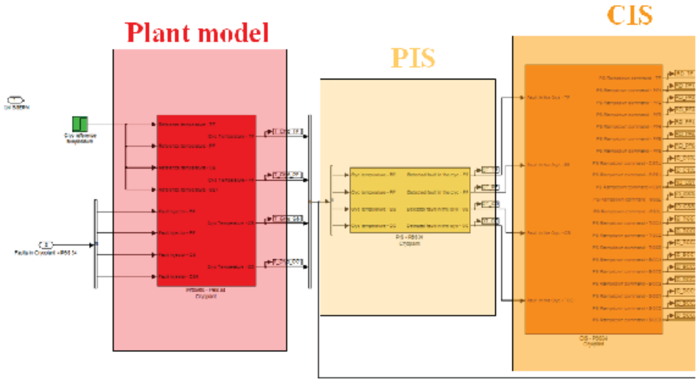
Both the CIS-PROT and CIS-OPS are implemented in the Matlab/Simulink/Stateflow environment

Areas

During the definition of the architecture:

- the overall structure of the ITER facility has been divided in areas
- instead of considering a sole centralized CIS, several CIS components are foreseen, one for each identified area

Plant model, PIS and CIS



Each area contains:

- the corresponding plant models, that describe the plant behavior
- the corresponding *Plant Interlock System* (PIS), that models the local interlock logic
- the CIS section for the considered area

The Interlock Control System (taken from the Conceptual System Design Description ITER_D_3QJ4Z3)

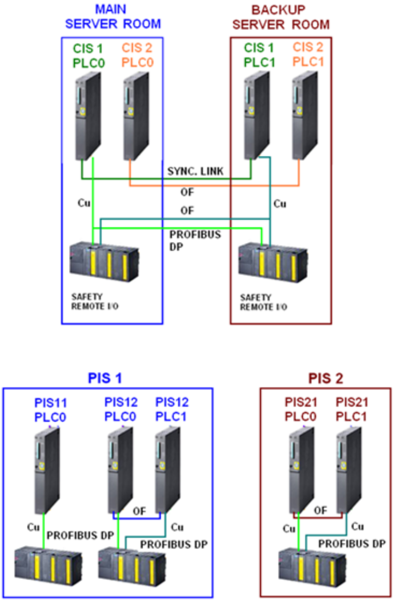
- The **Interlock Control System (ICS)** is in charge of the supervision and control of all the ITER components involved in the instrumented protection of the tokamak and its auxiliary systems.
- The ICS is constituted by the Central Interlock System (**CIS**), the different Plant Interlock Systems (**PIS**) and its networks (**CIN and PIN**). The ICS does not include the sensors and actuators of the plant systems but it is in charge of their control.

The ICS Prototype

- The ICS prototype developed by PROCON is a Siemens S7-400 PLC based control system
- It is aimed to show the feasibility of a reliable and redundant architecture for the slow controllers envisaged in the ITER ICS
- A description of the hardware architecture of the ICS prototype can be found in

PROCON Systems
ICS PROTOTYPES SLOW CONTROLLERS DESCRIPTION REPORT
ITER_D_457VEA, Mar. 2011.

ICS Prototype - HW architecture



CREATE support for the development of the PROCON prototype

The CREATE contribution (2011 and early 2012) to the development of the ICS prototype includes

- formal description of the mitigation actions (**interlock functions**) to be implemented on the ICS prototype
- development of a **Simplified Plant Simulator (SPS)** to be used for the test and validation of the ICS Prototype by means of HIL simulations
- support to the acceptance tests

Functional specifications for the ICS

Formal description of the interlock functions to be implemented on the ICS prototype

- A subset of the possible interlock functions for
  - PBS-11 (Magnets)
  - PBS-31 (Vacuum System)
  - PBS-34 (Cryoplant and cryodistribution)
  - PBS-41 (Coil power supply)

  have been identified in collaboration with ITER
- The functional specifications can be found in **ITER_D_4H8JKS**
- The current version of the prototype implements only a subset of the specified interlock functions

The Simplified Plant Simulator (SPS)

Development of a Simplified Plant Simulator to be used for the test and validation of the ICS Prototype

- The SPS has been developed in Matlab/Simulink
- The first version of the software has been released and it is available on the ITER SVN server
- Similarly to what was done during the CSS activity
  - Labview HMI has been developed
  - it is planned to use National Instruments SIT to deploy the simulator on a real-time target
- A number of documents have been released
  - SPS - Preliminary Design Document - **ITER_D_4GMJEL**
  - SPS - Architectural Design Document - **ITER_D_2MZ2X8**
  - SPS - User's Guide - **ITER_D_4H3V5R**

Support to the acceptance tests

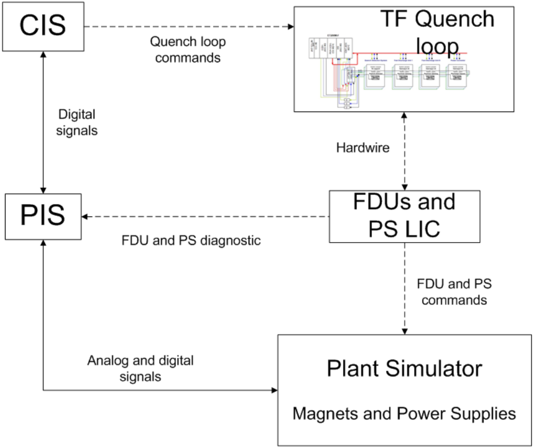
- The Factory Acceptance Test started in December 2011, however. . .
- . . .the real-time target is not yet available (is not even defined!)
- The HIL simulations are envisaged during the Site Acceptance Test in February (?)

CREATE support for the development of the Quench Loop prototype (developed by CERN)

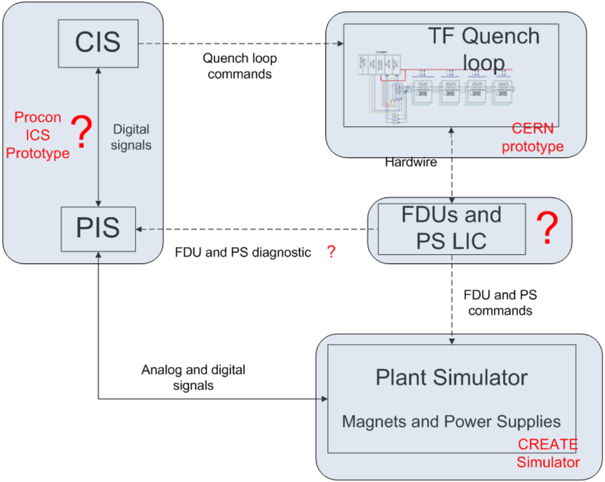
CREATE contributions

- *help* in the definition of the functions to be implemented by the CIS and PISs
- develop a plant model to test and validate the Quench Loop prototype via HIL simulations
- **evaluate the interaction between the Quench Loop and other systems – e.g., CIS, PISs, Plasma Control System (PCS)**

Proposed architecture - 1



Proposed architecture - 2



What are the required skills ?

- Matlab/Simulink/Stateflow
- Labview
- Step 7 - Siemens PLC S7
- Basic modeling skills

CREATE activities for ITER CSS and CIS

G. Ambrosino et al.
Rapid Prototyping of Safety System for Nuclear Risks of the ITER Tokamak
IEEE Transactions on Plasma Science, vol. 38, no. 7, pp. 1662–1669, Jul. 2010.

A. Vergara Fernández et al.
Modeling tools for the ITER Central Interlock System
Fusion Engineering and Design, vol. 86, no. 6–8, pp. 1137–1140, Oct. 2011.