SYRF project
the SRI case study

Albert Benveniste

October 28, 1998

1 Description

The figure 1 shows a synopsis of the SRI circuit. This is part of the auxiliary steam circuit, it aims at cooling certain parts of the plant in consideration, therein referred to simply as "use of refrigeration". There are four subsystems in the SRI system, they correspond to the indicated patches, taken from left to right (I indicate the colours, for those who see them):

Refrigeration *(in pink).* Refrigeration is continuously controlled, very much like the water of your bathroom. Hot water/steam (last link when ordered from top to bottom, the link with no heat exchanger for cooling) is mixed with cool water/steam (first two links when ordered from top to bottom). This is performed by one of the valves in the refrigeration subsystem, the one shown being controlled, called a *bypass.* This valve is the only continuous valve, other valves are just on/off.

Use of refrigeration *(in green).* This is considered as exogeneous, i.e., the environment.

Water input subsystem *(in yellow).* The two reservoirs are used to put adequate pressure in the water/steam circuit. The level within the reservoirs is not continuously controlled, it is only monitored by the bench of sensors depicted on the left of the bottom reservoir (each depicted sensor just says "I see/I don't see water", this provides a coarsely discretized information about the water level). In case of excessive level or pressure in these reservoirs, the safety valve allows water/steam to

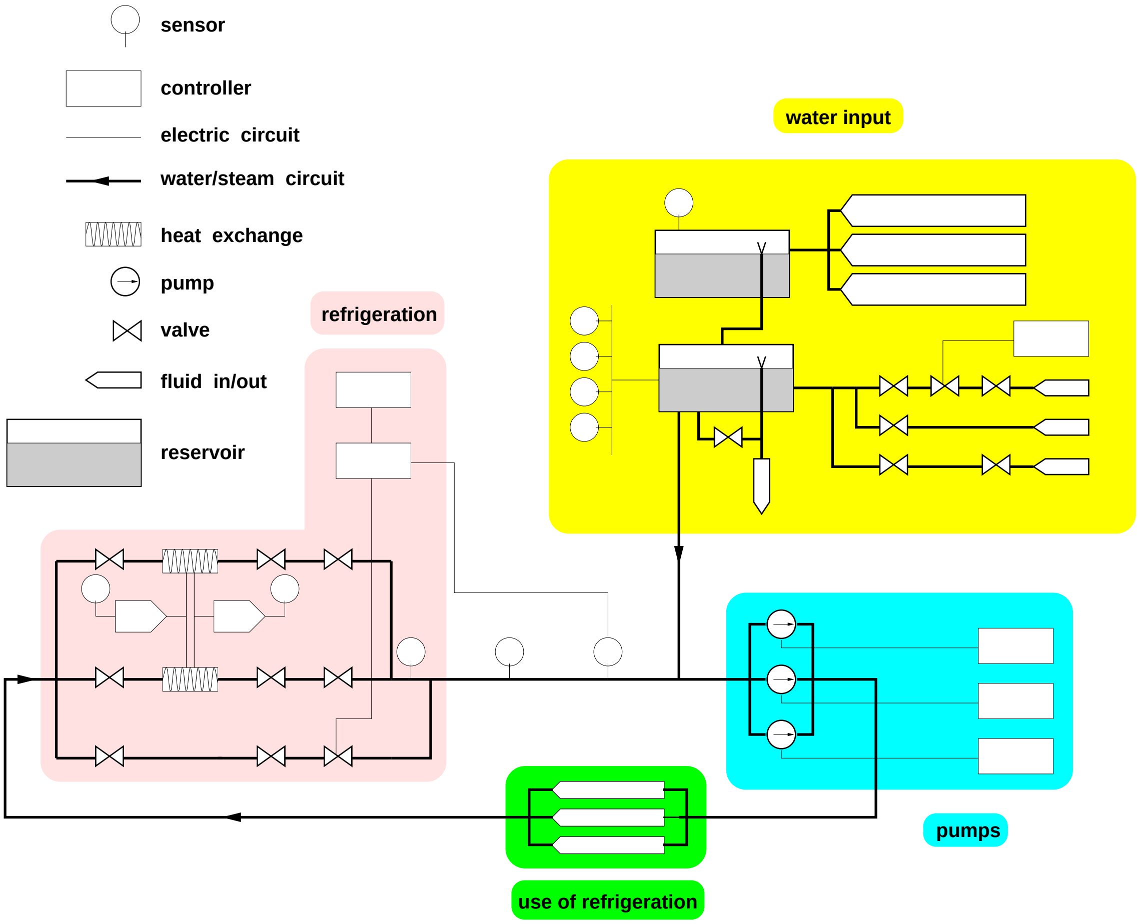

Figure 1: *The* SRI *heat exchange circuit.*

exit (shown down-right to the bottom reservoir), much like the safety valve of the device for high pressure cooking in your kitchen. In case of insufficient level, on/off valves are open and water enters (shown on the right). In any case of abnormal water level in the reservoirs, alarms are set and dispatched to the operator.

Pumps *(in cyan).* Only 1 or 2 among the three pumps are in operation, the other(s) are backup. Pumps are on/off, they are not controlled, just protected. Whenever needed, a pump can be disabled and replaced by a backup.

In addition, various alarms are attached to the electric/electronic peripherals devoted to control or protection.

2 Requirements

I start here with the overall requirements for the system. In a second (forthcoming) subsection, I shall refine this into specific verification and/or testing objectives.

2.1 Overall requirements

There are mainly two :

Requirement 1 *Under* nominal *perturbations exercised by the environment, the closed-loop system shall operate within its safety margins and acceptable performance level.*

Requirement 2 *Under* any *perturbation from the environment, switching to manual control shall always be possible.*

Comments.

1. Verifying or testing requirement 1 requires the following to be at hand :
   (a) a model of the plant
   (b) a description of the controller
   (c) a model of the nominal perturbations than can be exercised by the environment
   (d) a model of the safety margins and acceptable performance level.
2. Verifying or testing requirement 2 requires the following to be at hand :
   (a) a specification of the scenarios that can be applied by the operator in case of manual operation of the plant, with, in particular,
   (b) a description of those states for the system in which switching to manual operation mode is possible.

2.2 Detailed requirements

`to be done`

3 What is available about SRI

(i) A SIMULINK[1] joint description of the plant and its control system. *This is to be taken as the high-level description of plant+control.* In particular, the various abstractions for the plant, needed to generate tests or perform verifications, should be based on this description.

(ii) From this SIMULINK description, C code can be generated for joint plant/control simulation.

(iii) The controller has been *manually* programmed for the following two types of industrial PLC's: P320 (Cegelec), and Teleperm (Siemens). The PLC's communicate via a real bus. The whole has been connected to a dSpace hardware DSP board emulating in real-time the SIMULINK model for the plant. This provides a hardware-in-the-loop simulation for the PLC's.

(iv) A DFL description of the controller. DFL is an in-house formalism of EdF of dataflow style, with a predefined collection of icons. Compared to modern dataflow formalisms, there is no hierarchy, i.e., an overall specification is just a flat collection of diagrams than can share wires for their interconnection.

(v) TNI has developed, under Sildex[2], a DFL editor. The resulting diagrams are automatically translated into SIGNAL code. The SRI application is available[3] under Sildex, it generates DC_+ code, from which LEA code is automatically generated for the P320. The same with the STEP language for the Teleperm PLC is under progress. The, TNI also has developed automatic test case generation with a "white box" approach, in which coverage is measured with respect to the different Sildex boxes.

[1] version 4 or 5 ?
[2] Sildex is the editor for SIGNAL marketed by TNI.
[3] Can the SYRF partners have it ?

(vi) SRI is available in both Lustre and Scade[4], and preliminary studies have been performed by Pascal Raymond regarding test case generation.

(vii) Fernando Jimenez-Fraustro also has developed, under the Irisa Signal environment, a DFL editor, and the SRI application has been coded.

(viii) Thomas Kasten has developed a simple prototype, called MM, linking Signal to Simulink, and the SRI application has been modelled using this prototype tool. The principle of MM is simple: Signal controls the calls to Simulink (the upsampling mechanisms offered by Signal are very helpful for this), and each call has the form of launching the Simulink ODE–solver with given initial conditions and time horizon.

4 Selected questions for the case study

4.1 Improving modelling and simulation

Items (i,ii,iii) from section 3 provide the current facilities concerning simulation. What would be desirable in addition is:

(α) To have, in a synchronous language, models of the distributed PLC architectures for control, including models of the communication layers for Cegelec and/or Siemens PLC.

(β) To have a joint simulation of

- the Simulink model of the plant, and
- the distributed PLC architecture for control.

(γ) Same as (β), but aiming at emulating real-time performance.

(δ) To have, in a synchronous language, models of the scenarios for manual operation, with a simple control panel. To combine this with the joint Simulink/synchronous language simulation of plant+controller, in order to simulate switching between automatic and manual operating modes.

[4]Scade is the editor for Lustre marketed by Verilog.

4.2 Validation & testing

See the requirements of section 2.

4.3 Code generation

Same as (v), but for distributed code generation.