DEVELOPMENT OF A SAFETY CLASSIFIED SYSTEM WITH LABVIEW AND EPICS

C. Haquin[†], Ganil, Caen, France
P. Anger, J.C. Deroy, A. Savalle, G. Normand, F. Pillon, Ganil, Caen, France

Abstract

The Spiral2 linear accelerator will drive high intensity beams, up to 5 mA and 200 kW at linac exit. In tuning phase, or when not used by the experimental areas, the beam will be stopped in a dedicated beam dump. To avoid excessive activation of this beam dump, in order to allow human intervention, a safety classified system had been designed to integrate the number of particles dropped in it within each 24 hours time frame. For each kind of beam, a threshold will be defined and as soon as the threshold is reached a beam cut-off will be sent to the machine protection system. This system, called SLAAF: System for the Limitation of the Activation of the beam dump (Arret Faisceau in French) rely on LabView and EPICS (Experimental Physics and Industrial Control) technology. This paper will describe the specification and development processes and how we dealt to meet both functional and safety requirements using two technologies not commonly used for safety classified systems.

PRESENTATION

The Spiral2 project requires the possibility of human intervention on the Beam Dump and its surrounding. Hence the system must guarantee that the Beam Dump activation remain under an acceptable threshold. Since the Spiral2 accelerator will accelerate many ions species, the threshold depends on both mass number and energy of the accelerated ions. When preparing the accelerator parameters, the threshold, expressed in number of particles that can be dropped into the Beam Dump during a 24 hours time frame, will be calculated. The lower limit is a 20 MeV/A deuteron beam. In this case the 24 hour limit is 5.6 10^{18} atoms, corresponding to the shortest times after which the threshold is reached, specified in Table 1, as a function of the beam power.

Table 1: Worst Cases (20 MeV/A deuton beam)

Beam Power	Time to reach the threshold
200 kW	3 minutes
10 kW	1 hour
417 W	Always below threshold

MAIN REQUIRMENTS

Nuclear Safety

System classified in the second category of equipment involved in the safety in the Spiral2 classification system. This is the least requiring level, it can be considered equivalent to a SIL2 (Safety Integrity Level).

Operational

- The system must run permanently as soon as beams with intensity greater than 11 µA are produced. It must be reliable.
- The system must be compatible with all the ions at all intensity (from 11 µA to 5 mA) and energy (from 0.75 MeV/A to 33 Mev/A).

Functional & Technical

- The system must integrate the number of particles over a 24 h period, a period starting at a configurable but fixed hour.
- The beam ions charge and threshold will be entered in the system at each beam change.
- As soon as 95 % of the threshold is reached, a beam cut-off request is sent to the machine protection system.
- The latest value of the integral must be back upped in order to be retrieved in case of failure (power supply failure for example).

SAFETY CLASSIFICATION CHALLENGE

Taking into account miscellaneous Spiral2 project constraints and the system requirements, labView technology was retained for the system. Moreover, it should be integrated in the Spiral2 Control System, consequently the labView-EPICS gateway and EPICS-CSS (Control System Studio) tool for HMI (Human Machine Interface) were required.

As a safety classified system, its conception has been submitted to a Failure Mode and Effect Analysis and a Conception review. Though labView and EPICS are generally not considered convenient for a classified system, we thought we could take advantage of the labView technology using the cRIO (Compact Reconfigurable Input Output) solution with FPGA (Field-Programmable Gate Array) in its backplane in order to be able to prove its reliability.

Architecture

Starting from all these technical choices, the architecture arises, the cRIO with the FPGA and CPU (Central Processing Unit), hosting the LabView-EPICS gateway on one side and CSS for the HMI on the other side. However, during the early stages of the conception, we evaluated the LabView-EPICS gateway and discovered too much limitation (too few record fields, Channel Access monitoring and EPICS alarms not working) in server mode (i.e., gateway used as an EPICS IOC (Input Output Controller)) forcing us to use it in Client mode and to add an intermediate IOC called "IOC

[†] haquin@ganil.fr

SLAAF” as can be seen in figure 1. In this configuration, the HMI writes the integration parameters and read the results in the IOC SLAAF, the cRIO via the LabView-EPICS gateway reads the parameters and write the results in the IOC SLAAF. The behaviour, with the LabView-EPICS gateway in client mode, is safer since it will periodically read and write in the IOC SLAAF instead of being asynchronously written in by the HMI.

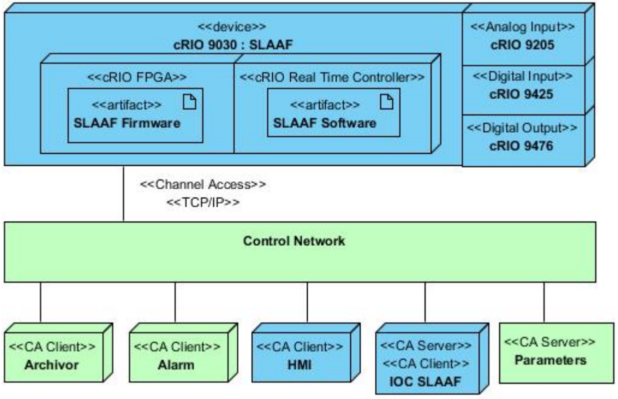

Figure 1: Deployment diagram of the system, in blue are the component of the SLAAF, in green the component involved in its exploitation.

SYSTEM DESIGN

A detailed design document was written, destined to guide the development process but also to provide the input information for the Failure Mode and Effect Analysis. Some safety issues like the handling of hardwired measures and binary information, not mentioned in this paper, were covered. Hereafter is an overview of how the system was designed to fulfil expectations.

Expected Functionality

According to the requirements and the end users expectations, seven main functionality were identified and formalized to establish the use case diagram in figure 2.

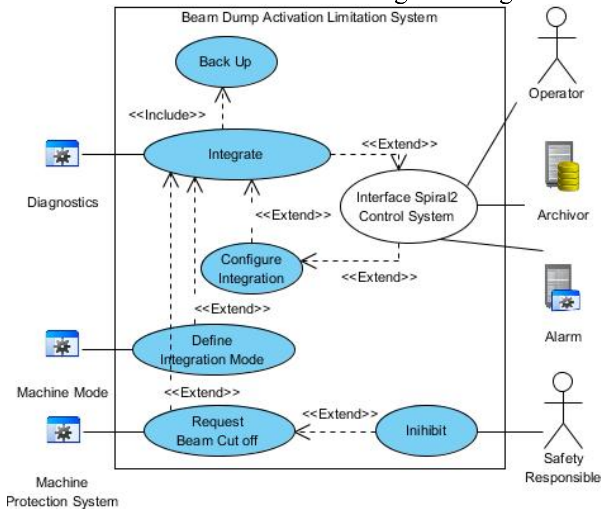

Figure 2: Use case diagram defining the main functionality. Interface EPICS Control System functionality is out of the safety classification scope.

Description of the Main Functionality

Integrate Integrate the number of particles dropped into the beam dump.

Beam Cut Off Request Drive ambivalent contacts to request the Machine Protection System to cut off the beam.

Configure Integration Read integration parameters from HMI and ensure integrity.

Back Up Handle a couple of files to save periodically the integration results on cRIO flash memory (to be able to resume integration in case of power supply failure).

Inhibit Hardwired contacts manually driven by the person in charge of safety (inhibit an erroneous cut off request in case of system failure).

Define Integration Mode Determine if the beam is actually sent in the beam dump or in the experimental areas, in this case, integral is frozen to avoid integrating diagnostics noise and offsets.

Interface Spiral2 Control System Read/Write the EPICS process variables hosted by the LabView-EPICS gateway, the gateway deals with the Channel Access.

Software Design

The system has a real time controller on one side and a FPGA on the other side. The first one is able to access the network and the flash storage, the second one is more robust and able to access the I/O (Input/Output) modules. In order to fulfil the reliability requirement and to minimise the probability of the “feared event” (i.e., Activation above threshold) to occur, it seemed obvious to implement all the integration, threshold comparison and I/O in the FPGA. Hence, the software was packaged as depicted in figure 3:

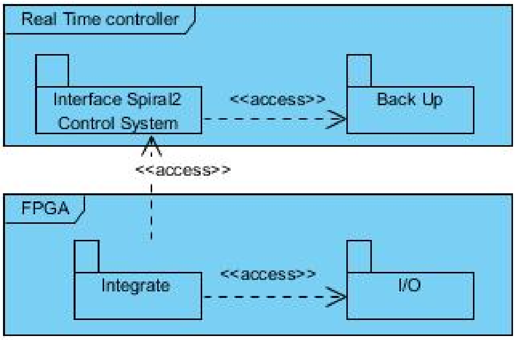

Figure 3: Packages and their execution environment.

Packages Responsibility

Interface Spiral2 Control System package is responsible for the “Interface Spiral2 Control System” and “Configure Integration” functions**.**

Back Up package is responsible for the “Back Up” function (managing files on flash memory).

Integrate package is responsible for the Integrate function.

I/O package is responsible for the “Request Beam Cut Off” and “Define Integration Mode” functions and just read the status of the “Inhibit” function.

FAILURE MODE & EFFECT ANALYSIS

The FMEA was achieved by a specialized company. Though no unacceptable point was raised, there were still important remarks to take into account. In the following sections, you'll find a description of the most important remarks and the solutions retained.

I/O Auto Test

The system must perform an auto test of its I/O modules.

Digital auto test : An output of the cRIO 9476 is connected to an input of the cRIO 9425, the I/O package periodically toggle the output and check the input.

Analog auto test : the system uses only analog input module but, since we use a 24 V power supply and the system requires 9 V to 30 V, we connected the power supply to an analog input of the cRIO 9205 and the I/O package periodically tests its value.

CPU Load

The CPU load has to be measured.

We integrated the dedicated labView VI to permanently monitor the CPU load; the maximal peak value measured is less than 15 %, the nominal value is less than 10 %.

We were rather confident about this point since all the heaviest treatments are done on FPGA side.

Secure Integration Parameters

The integration parameters (Threshold and Ions Charge) received from the HMI had to be strengthened.

The conventional way to do this is to compute a CRC (Cyclic Redundancy Check) on HMI side, transmit both data and CRC in the system, recompute the CRC and check equality with the one received. We wanted to avoid to implement CRC in CSS HMI and to imply the HMI in the safety classification process.

Instead we implemented a double check mechanism: the parameters received are compared to expected ones located in a soft IOC hosting all the accelerator parameters. In case of equality, the parameters are sent back to the HMI and checked by the operator who finally activates the parameters making them actually used by the integration.

Watchdog

To ensure that the system is alive, it must be monitored by an external cycle monitor able to request a beam cut off if the system is out of order.

The solution is to periodically toggle a dedicated digital output to generate a pulsed periodic signal and to monitor it. The ABB CM-WDS cycle controller relay with watchdog functionality was retained. This device operates on a frame of 8 successive periods of the signal to monitor and checks its validity, if the signal is not correct dry contacts are toggled.

Specific Beam Cut-Off Wiring

The beam cut off request is basically achieved with two ambivalent dry contacts, but three actors are involved in their control: The first actor is of course the cRIO, if integration reaches threshold, the second is the cycle controller if the system is dead, and the third is the person in charge of safety if he considers that the system is not working properly. There must be a logical "OR" between the first two actors but the result can be inhibited by the Installation responsible.

Conditions in which the beam cut off is requested or inhibited are summarized in the following equation:

$$\mathrm{BR} \ = \ (\mathrm{IAT\ or\ WD})\mathrm{and}\ \overline{\mathrm{INH}}$$

With: BR = Beam cut off Request
IAT = Integration above Threshold
WD = Watchdog
INH = Inhibition by person in charge of safety

This equation must be implemented in a hardwired manner as described in figure 4 in order to be really independent of the cRIO.

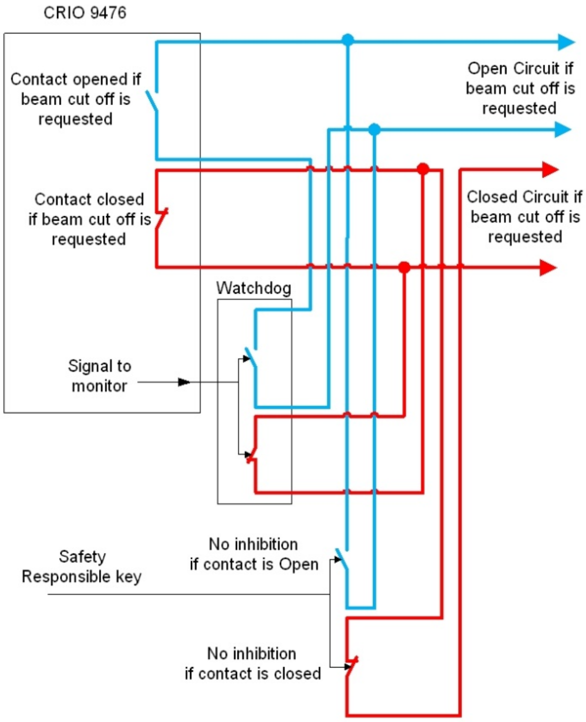
CRIO 9476
Contact opened if beam cut off is requested
Open Circuit if beam cut off is requested
Contact closed if beam cut off is requested
Closed Circuit if beam cut off is requested
Watchdog
Signal to monitor
Safety Responsible key
No inhibition if contact is Open
No inhibition if contact is closed

Figure 4 : Wiring diagram of the beam cut off request contacts, taking into account the three actors.

STATUS

The system was developed according to the design specification, the integration package was split in sub function each one having its own test application to be able to prove the correctness of the safety critical function.

A strong testing effort was required: definition of the tests, realization of a test board to simulate the digital and analog machine signals and finally iterative execution of the tests and report writing.

Actually the whole system, with the LabView gateway, IOC and CSS HMI are permanently running in the lab with the test board, the real life tests are planned for summer 2018.