CLS LINAC SAFETY SYSTEM UPGRADE

Hao Zhang, Elder Matias, Grant Cubbon, Carmen Britton, Robby Tanner, Carl Finlay
Canadian Light Source Inc., Saskatoon, Canada

Abstract

The Canadian Light Source (CLS) upgraded the safety system for Linear Accelerator (Linac) in October 2009. IEC 61508 SIL 3 certified components and methods were adopted in the development of the new system. This paper outlines major aspects of the upgrade.

INTRODUCTION

In the CLS, Access Control and Interlock Systems (ACIS) are used in restricted areas to protect personnel from radiation hazards. In the Linac area, a legacy ACIS was used since 1980's until October 2009. The system was based on early Micro84 Programmable Logic Controller (PLC). Given the age of the system, difficulty in procurement of spares as the vendor had discontinued support for the platform; a decision was made to upgrade. Another reason is the old AICS used 120 VAC whereas CLS has adopted 24 VDC for all other control systems. The upgrade ensures the Linac ACIS is consistent with other systems in the facility. All the old sensors, wirings, components, and PLC units were removed. The new ACIS was redesigned and built from scratch.

The new ACIS adopts a two-level, redundant protection mechanism which consists of two independent chains, one governed by a safety-rated PLC system providing SIL-2 as defined by IEC 61508 [1], and a relay-based hardware logic to provide diversity for safety functions.

The system controls access to an area divided into 6 lockup zones [2]. The zone layout was also changed in the upgrade. The zones contain the electron gun, accelerator sections, switchyard, LINAC-to-Booster Transfer Line (LTB), the LTB/Booster Ring (BR1) interface and some adjacent areas including the BR1 RF cavities.

Fundamentally, all lockup zones operate in the same principle, each having its own Emergency Off Stations (EOS), Door Interlock Switches (SWDI), Lockup Stations (LUS), zone lockup lights (ZLL) and horns (HRN).

BACKGROUND

Regulatory Context

CLS holds a Particle Accelerator Operating Licence (PA1OL-02.00/2012) issued by the Canadian Nuclear Safety Commission (CNSC) to operate as a Class 1B facility; as a result the definition of internal process is left to the CLS with the CNSC providing review, oversight, and audition.

Project Plan/Management

The upgrade was carefully planned and documented. The plan identifies project objectives and goals, specifies the upgrade scope, lists standards and guidelines for the development, and defines roles and responsibilities of team members. The plan also includes work structure breakdown, budget, timelines, and a list of documents need to be generated or modified. The plan served as the guiding document during the development process.

Safety System Development Process

The upgrade followed a V-model variant for safety system development.

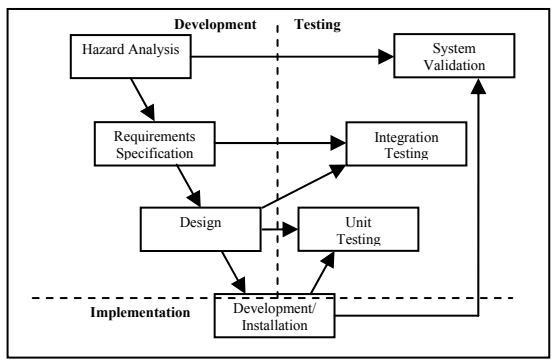

Figure 1: Safety System Development Process

The process starts with the hazard analysis, based on which requirements and specifications are generated, and design and implementation naturally followed from there. Testing was performed in all stages. Respectively, integration and unit testing verify the design meets the requirements and the installation is done as the design.

Hazard Analysis

Since the layout of Linac lockup zones was to be changed, a Hazard Analysis (HAZAN) [3] was necessary to identify the hazards and associated mitigations required with regard to the proposed redesign and upgrade. This was performed by the Health, Safety, and Environment (HSE) department of CLS. The document issued was used as input to the following development stage.

Requirements

The hazards which have been identified and allocated to the ACIS for mitigation in the HAZAN were then examined and refined to generate requirements for the ACIS. Other internal or external guidelines, such as human factor guideline [4] and Canadian Electrical Code were also incorporated as requirements in this stage. Operation experience on the old Linac ACIS and other ACISs was also taken into consideration. A design manual was generated to document all requirements. Linac lockup zone layout drawings were generated to

* Research described in this paper was performed at the Canadian Light Source, which is supported by the NSERC, NRC, CIHR, the Province of Saskatchewan, Western Economic Diversification Canada, and the University of Saskatchewan.

capture detailed requirement and design information. The drawings show zone configurations and lockup paths. All components were identifies and numbered, which makes an IO count possible and perfect input document for wiring diagrams.

FUNCTIONS

The Linac ACIS provides four major functions: *secure*, *lockup*, *annunciation*, and *interlocking*. As mentioned, the system consists of two separate chains, each having their own inputs and outputs.The PLC chain provides all four functions; the relay chain provides redundant functions in safety critical aspects of secure and interlocking.

Secure

A lockup zone is secured only when all the doors are closed and none of the EOSs is pressed. The secure function is implemented independently in both chains.

Limit switches are used to monitor door position. Each door has two physically independent switches for signalling the two separate chains.

An EOS consists of an emergency off button, a reset button, and three mechanically-interlocked and latching contacts - two normally close contacts for signaling the two chains and one normally open contact for activating a local red LED when the EOS is pressed. If the emergency off button is pressed, all contacts remain latched and the red LED remains on until the reset button is pressed.

Linac is interlocked if any of the zones are not secured. The redundant design ensures even component in one chain fails, the other still functions to interlock the Linac.

Lockup

A zone is considered locked up only when the lockup sequence, designed by the HSE for each individual zone, has been performed successfully in this particular zone. Two inspectors are required to perform the sequence, which involves walking through a prescribed path within certain time limit to ensure every part of the zone is inspected in a timely manner.

LUSs are installed in selected locations to ensure the path is followed and the process is timed. Each LUS has a lockup button for signalling the PLC chain, and a green LED to provide visual indication to the inspectors.

As an administrative procedure, the lockup sequence is performed by inspectors and redundantly verified by the PLC. As the complexity of a system increases, so does the potential to introduce errors and possibly hazards. Implementing the multiple sequences in hardware is more likely to introduce error and potential hazards than it is to provide extra protection. Therefore, lockup function is implemented only in the PLC chain.

Annunciation

Horns and flashing lights are used to provide audible and visual annunciations.

Interlocking

Linac is interlocked from both chains through multiple permissive channels, such as Linac RF and gun triggers, RF source switch, etc., to avoid single failure point.

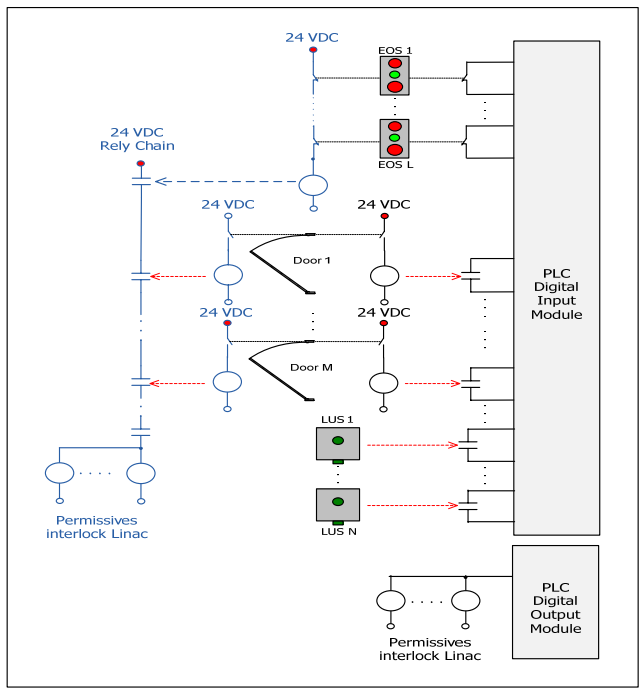

Figure2: implementation of secure and lockup functions

HARDWARE

PLC Configuration

Siemens AS414-4H processor was selected for the CPU. With the fault-tolerant run-time license installed on the processor, the built-in fail-safe run-time logic is activated. Password protection is also activated to protect the processor from re-programming.

SIL-3 certified modules with internal diagnostics and redundant circuitry are used for field I/O. These modules are installed in remote I/O stations communicating with the CPU over Profibus using the PROFISAFE protocol. Fibre-optic cable is used for data link. This configuration is based on accepted practice for SIL-3 applications as per IEC 61508. The protocol is deterministic and failsafe when used with failsafe hardware. The use of distributed I/O via fibre-optic cable provides electrical decoupling of the system, thus avoiding problems associated with running signals over long distances. Given potential problems with ground loops, EMI noise and signal degradation using conventional means, this architecture is more reliable and safe.

Field Wiring

Most of the field wirings are located in the basement Linac hall, where leaking underground water at certain locations can cause problem. Proper NEMA type enclosures were carefully chosen for PLC panels, junction boxes, EOSs, and LUSs to achieve water protection. For

the same reason, field instrumentations are wired using water-proof multi-conductor armoured instrumentation cables, which run in dedicated conduit with distinct color and not shared with other systems or equipment. All field components are CSA approved.

SOFTWARE

The PLC programming toolset is Siemens SIMATIC Manager, using Continuous Function Chart (CFC), a graphical language involving interconnecting elementary Function Blocks (FB) to implement control logics.

Program Structure

The code is structured hierarchically following the actual lockup zone layout. A folder is assigned to each zone, and each zone folder has three CFC charts, which can be considered as programming logical sections. The three charts contain codes to monitor and control EOSs, doors, and lockup sequence respectively. Another folder assigned to control room and contains charters for zone status summation and interlocking.

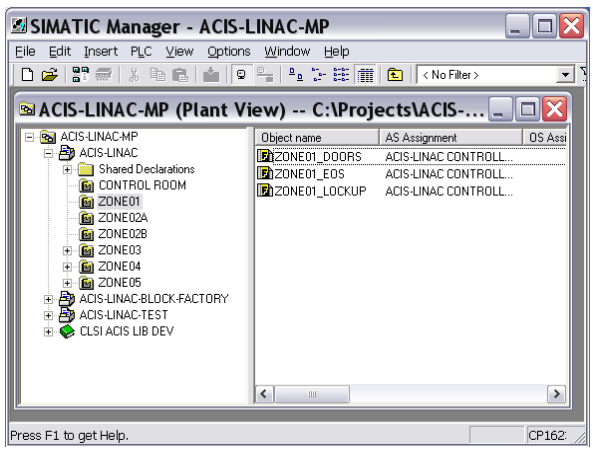

Figure3: Program hierarchy structure

Failsafe Code

Safety critical codes are developed using TÜV-certified function blocks from S7 Fail-Safe Systems Library to ensure fail-safe feature. All failsafe codes are assigned to Organizational Block (OB) 35 by default and are executed cyclically every 100ms in runtime.

Siemens allows developers to create their own standard or failsafe FBs. In CLS, FBs for typical ACIS functions were developed in earlier projects and a CLS ACIS block library are created to save them. In the Linac upgrade, some CLS made FBs were reused and some new FB's were developed and added into the library.

Simulation

The ACIS program had been tested thoroughly using Siemens software simulator, PLCSIM, before it was downloaded to the CPU for on-line testing. Since the system involves only On/Off variables, software simulation is sufficient to test the control logic.

Version Control

For safety system software, it is critical to ensure correct version is loaded on the processor. Siemens S7 F system provides safety program signature to uniquely identify a particular state of the safety program. Generally speaking, a 32-bit number known as the signature is generated across all the fail-safe blocks of the safety program at the end of the compilation phase.

In CLS, MKS Source Integrity is used for software version control. Versions of the ACIS program at different development and maintenance stages are saved in the MKS repository. With the signatures as identifiers, we can easily locate the correct version for download.

VALIDATION AND VERIFICATION

A Validation and Verification (V&V) procedure was developed to examine if the operation of the ACIS within specifications as outlines in requirements and design documents. The overriding approach to the testing methodology is a meticulous and exhaustive series of tests to ensure that the system operates as required. The V&V was performed by HSE personnel before the system was approved for operation. Any modifications to the system after the V&V will cause the V&V procedure being updated and the V&V has to be performed again.

CONCLUSION

The new ACIS was approved for operation in October 2009. Couple of lessons have been learned. Thorough planning and complete documentation in the initial project stage was the key for timely completion. A great portion of early development time went on clearly identifying, defining, and visualizing requirement details in the zone layout drawings and in design manual. This turned out increased the efficiency in the following phases. In the implementation stage, hierarchical program structure provided better readability and made it easier for future Siemens WinCC Graphical User development. Reuse of ACIS FBs reduced programming time. The development of new FBs expanded the block library for future projects. The CLS will continue to use a relay-bsed chain to backup simple, life-safety functions.

REFERENCES

[1] "Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-Related Systems" IEC 61508 or ANSI/ISA S84.01-1996

[2] "LINAC, LTB1, BR1, & HR1 ACCESSCONTROL AND EMERGENCY OFF SYSTEM LAYOUT", CDAC/RAD/0039405, Rev 7.

[3] "LINAC ACIS Upgrade Hazard and Risk Analysis", 11.18.52.1, Rev. A

[4] McKibben, M. 2008. "CLS Human Factors Workscope", 0.1.1.1, Rev. 1