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

Canadian Light Source
Centre canadien de rayonnement synchrotron

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

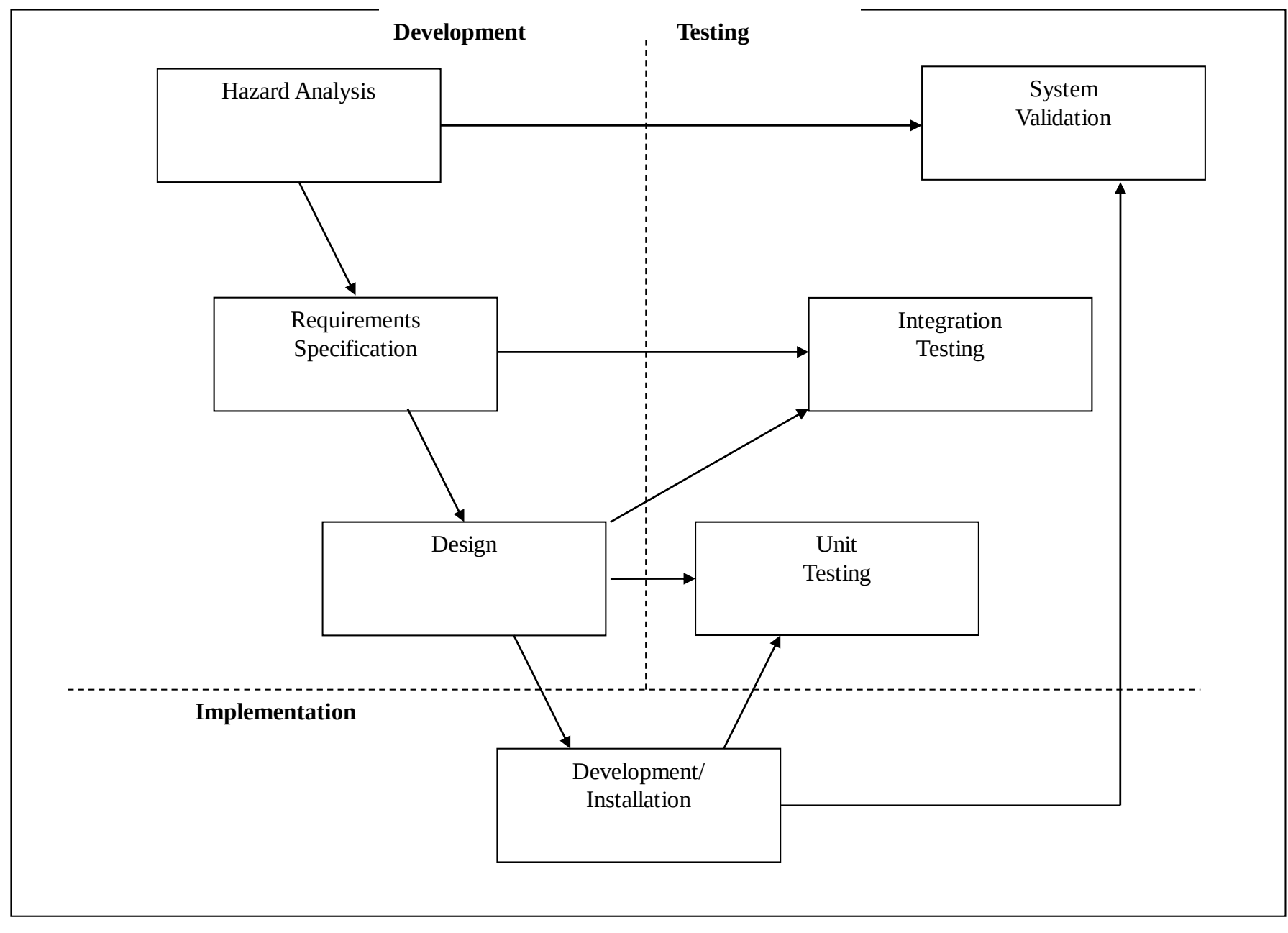
In the CLS, Access Control and Interlock Systems (ACIS) are used in restricted areas to protect personnel from radiation hazards. In the Linac area, a legacy ACIS was used since 1980's until October 2009. The system was based on early Micro84 Programmable Logic Controller (PLC). Given the age of the 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).

Safety System Development Process



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.

Linac Lockup Zone Layout Drawings

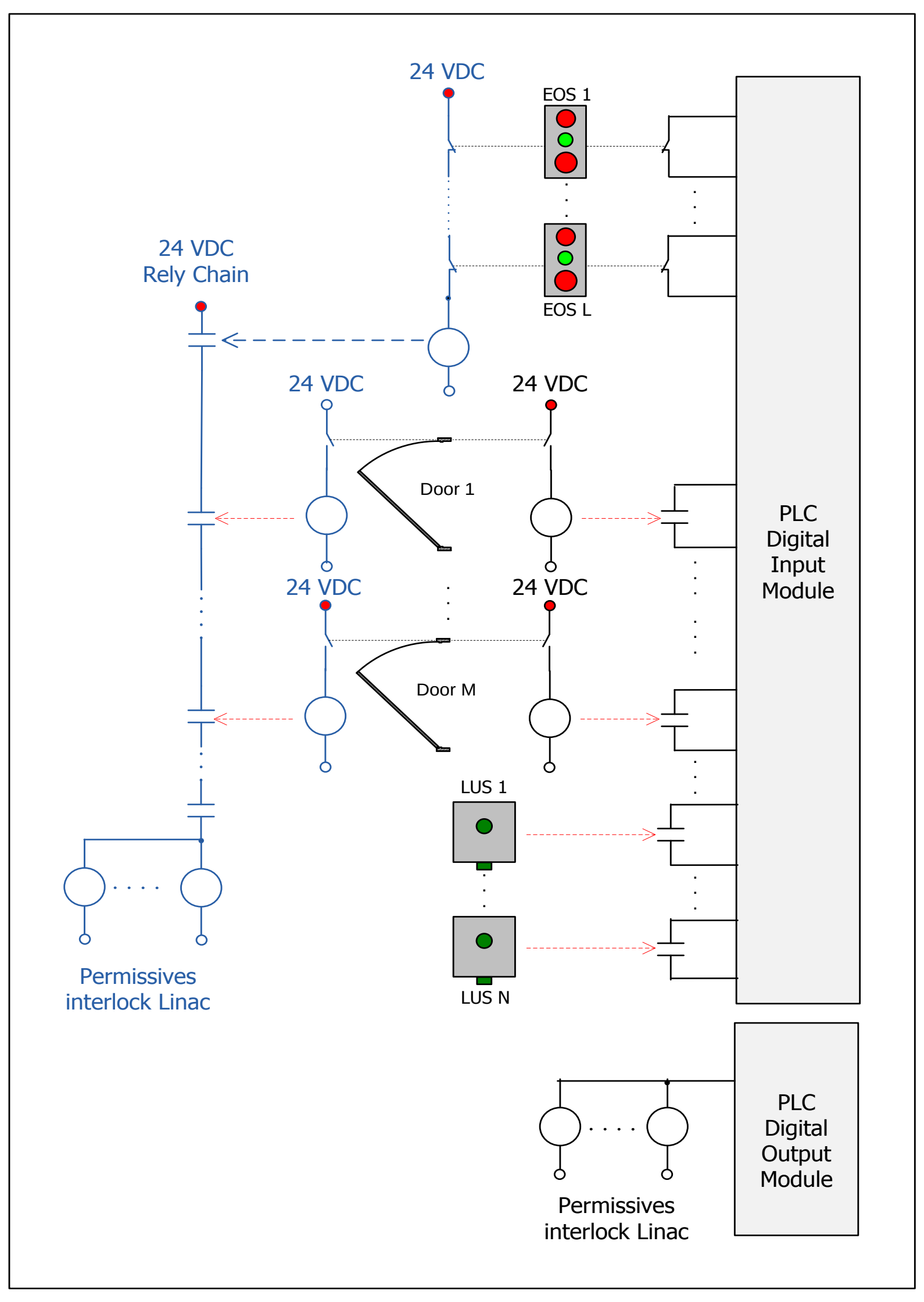
Linac lockup zone layout drawings were generated to capture detailed requirement and design information. The drawings show zone configurations and lockup paths. All components were identifies and numbered, which makes an IO count possible and perfect input document for wiring diagrams.

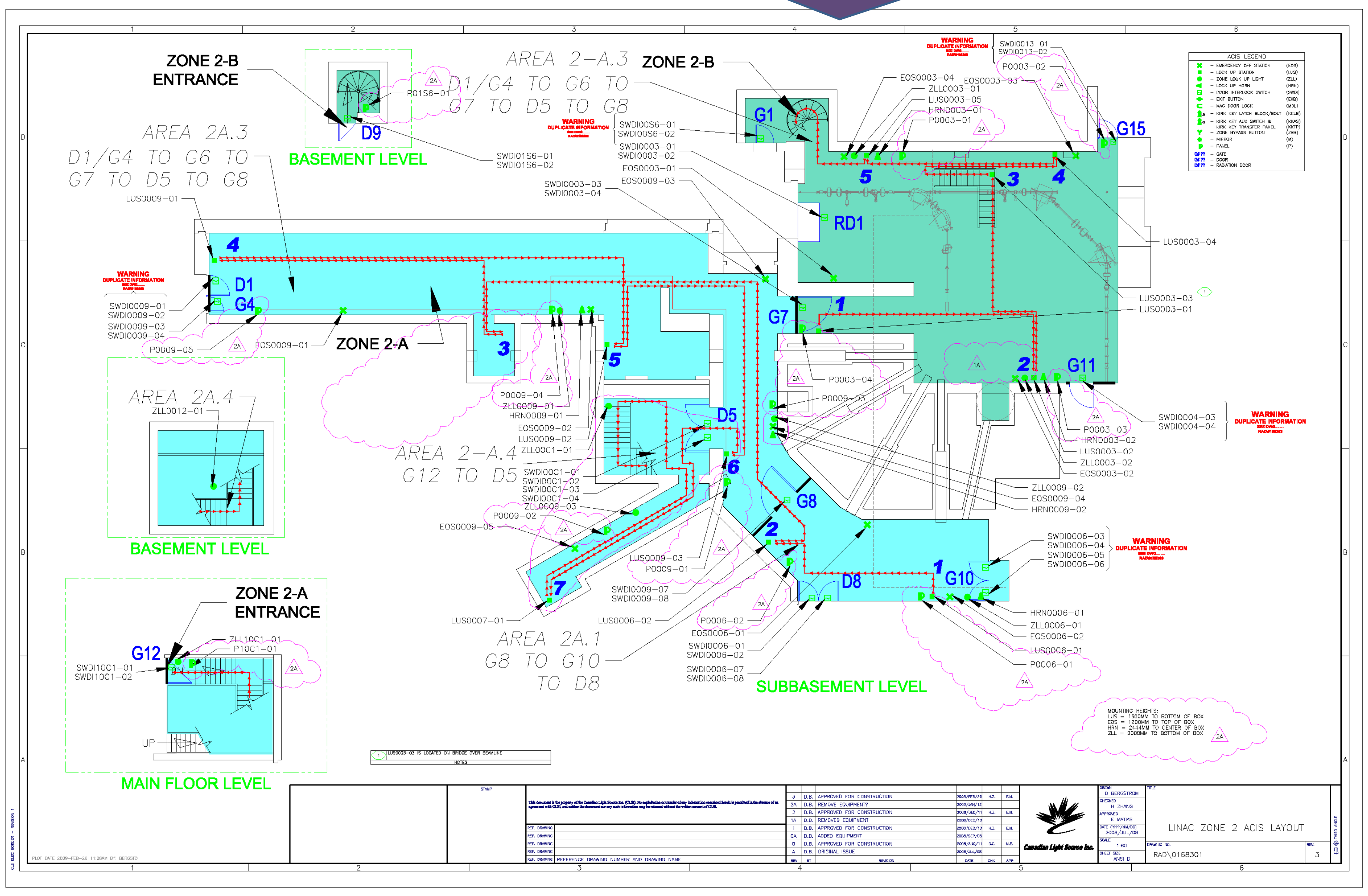
Two-Chain Redundant Architecture For Safety-Critical Functions

The ACIS provides four major functions: *secure*, *lockup*, *annunciation*, and *interlocking*. The PLC chain provides all four functions; the relay chain provides redundant functions in safety critical aspects of secure and interlocking.

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.

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. lockup function is implemented only in the PLC chain.





Door limit switch

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

Lockup station

Emergency off station

Lockup stations 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.

An Emergency Off Station consists of an emergency off button, a reset button, and three mechanically-interlocked and latching contacts – two normally close contacts for signalling 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.

Flashlight

Annunciation

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

Sign light

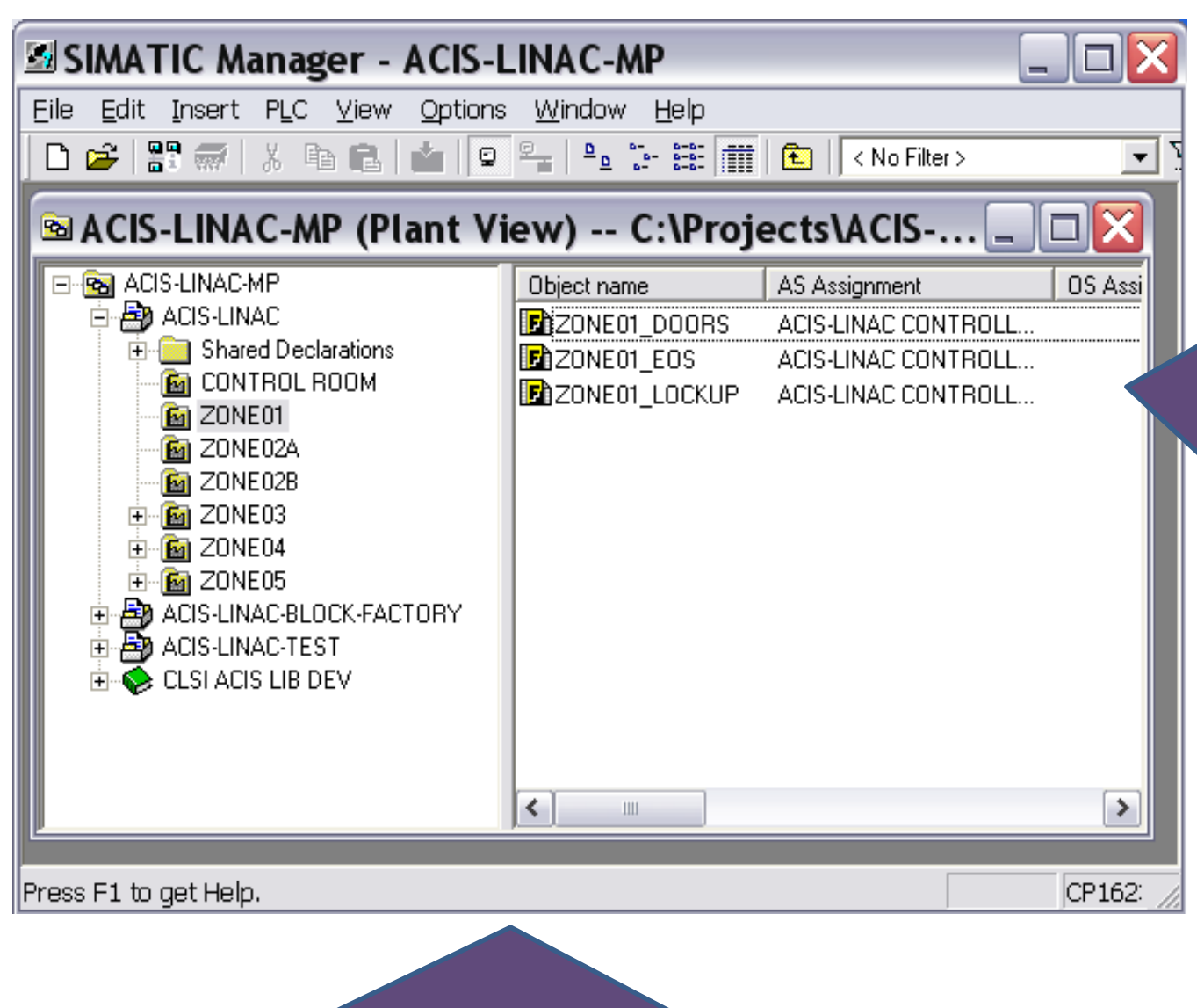
ACIS PLC - CPU

Fiber-Optic cable

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.

Remote I/O station and Fail-Safe I/O modules

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 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.



ACIS-LINAC-MP (Plant View) -- C:\Projects\ACIS-...

- ACIS-LINAC-MP
  - ACIS-LINAC
    - Shared Declarations
    - CONTROL ROOM
    - ZONE01
    - ZONE02A
    - ZONE02B
    - ZONE03
    - ZONE04
    - ZONE05
  - ACIS-LINAC-BLOCK-FACTORY
  - ACIS-LINAC-TEST
  - CLSI ACIS LIB DEV

Object name	AS Assignment	OS Assi
ZONE01_DOORS	ACIS-LINAC CONTROLL...	
ZONE01_EOS	ACIS-LINAC CONTROLL...	
ZONE01_LOCKUP	ACIS-LINAC CONTROLL...	

Press F1 to get Help. CP162:

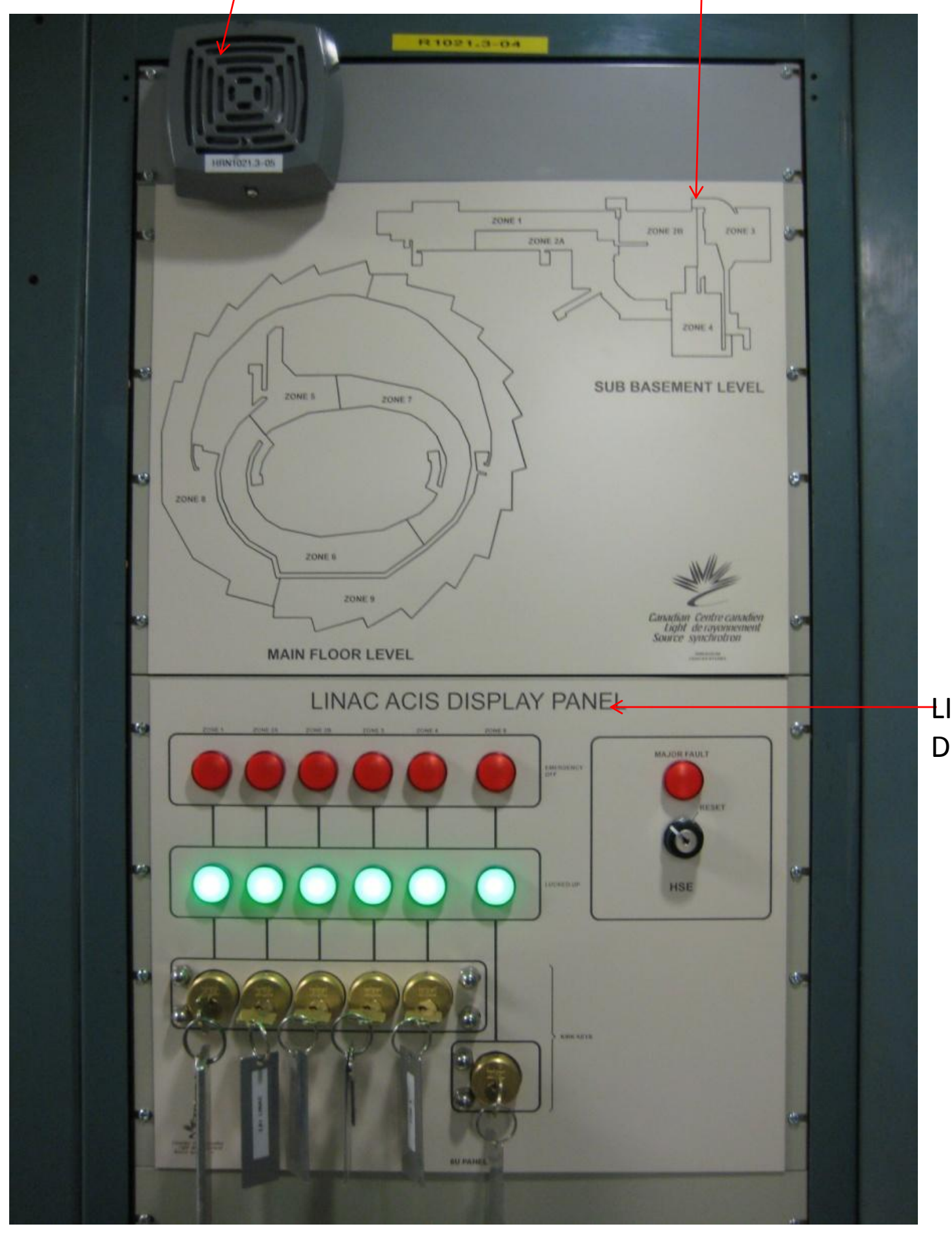
The programming toolset is Siemens SIMATIC Manager, using Continuous Function Chart (CFC) language.

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.

Horn

LINAC lockup zone layout



LINAC ACIS Display Panel

2009 ICALEPCS

International Conference on Accelerator and Large Experimental Physics Control Systems
Kobe, Japan

www.lightsource.ca