Development of an Accelerator Safety System Using IEC 61508 and Design Pattern

Hao Zhang, Elder Matias

Canadian Light Source Inc.
University of Saskatchewan
Saskatoon, Canada
hao.zhang@lightsource.ca, elder.matias@lightsource.ca

***Abstract*—For particle accelerator facilities, Access Control and Interlock Systems (ACIS) are required to protect personnel from radiation hazards associated with accelerator operations. As an early adopter of IEC 61508 standard for safety system development, the Canadian Light Source, Inc. (CLS) faced several challenges in how to design engineering processes around the standard that reflected the safety requirements as well as the domain specific environment that we were working within. This industrial report outlines some of the challenges, considerations, and decisions on the adoption of IEC 61508 into a research facility like CLS. By following these principles and methods, overall Safety Integrity Level three (SIL-3) has been achieved. One contribution the CLS made in the adoption of IEC 61508 is that, applied design pattern approaches to domain specific safety algorithms like those used in ACIS. This paper outlines the introduction of design pattern approaches in CLS. A CLS developed design pattern is given as an example.**

Keywords-IEC 61508; ACIS; Design Patterns

I. INTRODUCTION

Historically, accelerator safety systems relied on relay-based interlock systems. As safety-rated Programmable Logic Controller (PLC) equipment became available in the market, it has been widely used for industrial safety systems. However, until very recently, the use of safety rated PLC equipment in accelerator safety systems has been rare. Accelerators built over the past five years have started to adopt safety rated PLC equipment primarily intended for the process control industry. CLS was an early adopter of such equipment.

Within the accelerator research and medical therapy community, the industry consensus has been that IEC 61508 [1] forms the basis of best practice, and this has resulted in wide adoption of this standard with specific examples including:

- Synchrotrons: ALBA Synchrotron [2], and Diamond Light Source [3].
- Accelerators: Large Hadron Collider (LHC) of the European Organization for Nuclear Research (CERN) [4], Jefferson Labs' Thomas Jefferson National Accelerator Facility (TJNAF) [5], Mégajoule Laser Program [6], and ISIS spallation neutron source [7].
- Medical Accelerator Facilities: Heidelberg Ion Therapy Facility [8], and Selective Production of Exotic Species (SPES) [9].

When applying the IEC 61508 standard to the design of the Access Control and Interlock Systems (ACIS) for CLS accelerator, the special contexts of the accelerator environment need to be taken into considerations. To address these considerations, a design pattern approach is introduced into the system life cycle for the CLS ACIS system.

Conventional software engineering techniques have embraced the concept of design pattern over the past two decades. However, these approaches have seen limited use in safety critical systems design [10]. Some recent work has focused on very generic design patterns [11] [12]. Yet, we are not aware of these approaches being applied to domain specific algorithms across the entire IEC 61508 life-cycle.

The following lists some key points and considerations when adopting design pattern approaches in CLS ACIS design:

a) Unlike other systems, in the case of accelerator access control and interlock, some common safety scinarios repeat themselves from one accelerator zone to another. In this contxt, we see pattern as a valuable tool in the design of ACIS. In this design approch, the ACIS algorithm involves a series of design patterns that provide general solutions to the common recurring situations for accelerator access control and interlock.

b) Though all lockup zones operate in similar manners, there are different variations based on the number of entrieis, exits, lockup stations and search paths.The ACIS design patterns provide a set of templates or guidelines with the flexibility that the patterns can be altered to fit specific design needs for individual zones.

c) The hazard analysis, design, verification and validation procedures must be able to effectively manage and deal with both the generic issues in common safey situations and special cases and exceptions for individual zones in an effective way. Here, again, the extended concept of design pattern provides a good solution.

The motivation of this industrial report is to give an overview of major aspects of CLS ACIS with the following two emphases:

1) The application of IEC 61508 principles, methods, and processes in the design and development of the CLS

 ISBN: 978-1-61208-246-2

ACIS. Some of the challenges, considerations, and decisions on the adoption of this industrial standard into a research facility like CLS will be outlined. By following these principles and methods, overall SIL-3 rate, as defined in [1], has been achieved for the ACIS.

2) The adoption of design pattern methods in the CLS ACIS design. By using patterns in ACIS design, we are able to create reusable solutions for common accelerator safety scenarios, promote software reuse, and save time in the design and engineering stages.

In Section II, additional background is provided on aspects of regulatory context, the development process and requirements of the system, and the considerations and practices for CLS to establish system boundaries. Section III gives details of the major safety functions for the ACIS. Sections IV, V, and VI, cover the aspects of hardware, software, and interface of ACIS, respectively. A short introduction to the validation and verification procedure is given in section VII. Section VIII identifies possible future works for improvement.

II. BACKGOUND

A. Application Context

The Canadian Light Source (CLS) facility consists of two accelerators in series used to take electrons from rest to 2.9 GeV, the electronics are then deposited into a high current storage ring. Synchrotron light (covering a wide spectrum from visible to hard x-ray) is extracted from the storage ring and used to perform experiments on suite of independent beamlines covering a wide range of science from advanced materials, to environmental and life sciences.

Particle accelerators can produce hazardous levels of radiation if not appropriately shielded during operation. This is usually accomplished through the use of shielding and a safety system that ensures that staffs are not present during normal operation. Due to safety considerations, a systematic systems engineering process needs to be adopted, and tailored to provide sufficient flexibility for use in a research organization such as the CLS.

In CLS, ACIS is used in restricted areas to protect personnel from radiation hazards. The ACIS controls access to the accelerator hall and tunnels during accelerator operation to ensure staffs are not present when the accelerators are in operation. These areas are divided into lockup zones, which contain the Linear Accelerator (Linac), Linac-to-Booster Transfer Line (LTB), the Booster Ring (BR), the Booster-to-Storage Ring Transfer Line (BTS), and the Storage Ring (SR). Lockup zones are locked up independently, each having its own Emergency off Stations (EOS), Door Interlock Switches (SWDI), Lockup Stations (LUS), zone lockup lights (ZLL), and horns (HRN).

This system adopts a two-level, redundant protection mechanism, which consists of two independent chains, one is governed by a PLC system rated SIL-2 as defined by [1], and a relay based hardware logic to provide diversity for major safety functions. Overall, the ACIS requirement is for SIL-3. SIL-3 is achieved by the use of the two independent, redundant, fail-safe systems that are SIL-2 certified.

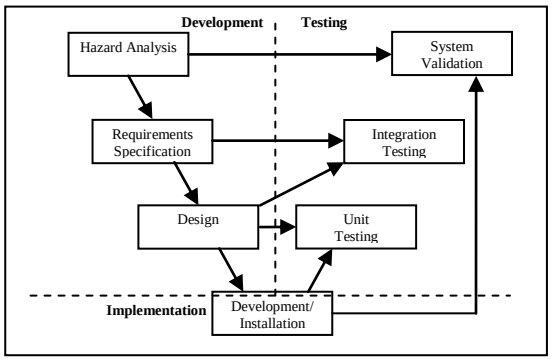

Figure 1. Safety System Development Process.

B. Regulatory Context

CLS holds a Particle Accelerator Operating Licence (Class IB) issued by the Canadian Nuclear Safety Commission (CNSC); as a result, the definition of internal process is left to the CLS to define and propose with the CNSC providing regulatory oversight.

C. Safety System Development Process

In the past, when accelerator facilitates designed safety systems, the common approach was to simply scale up the rigor used in the design of their non-safety critical systems, and try to make the system as fail safe as possible. Over the past decade and a half, there has been an increasing interest in the community in the adoption of broader industrial standards and certified equipment, more specifically IEC 61508. CLS was one of several facilities that were early adopters of IEC 61508.

The above Figure 1 shows the Safety System Develop Process. As illustrated in Figure 1, the CLS safety system development process starts with the Hazard and Risk Analysis [1]. The mitigation measurements identified by the Hazard and Risk Analysis are then allocated to different sub-systems, which includes administrative procedures, preventive measurements, and safety systems. Those allocated to the safety system become the basis of design requirements and specifications. Once detailed requirements are generated and documented, the design and implementation can be carried out. Testing and validation are performed in all development stages. Respectively, integration and unit testing verify the design meets the requirements, and the installation is done as the design.

D. System Boundaries

Establishing system boundaries is critical in this type of environment. The main control for the CLS facility has in excess of 600 control computers working with 50,000 to 100,000 data points. Clearly, generating system boundaries between safety systems, equipment protection systems, critical control functions developed by the facilities, and

 ISBN: 978-1-61208-246-2

systems modified by outside researches and users to meet their specific experimental needs are important.

A strong emphasis is placed on high system cohesion and minimizing inter-system coupling within the design. After ten years of evolution of these systems, we have found it necessary to periodically revisit the boundaries and adjust the allocation of requirements based on evolving system requirements.

The primary accelerator control system is implemented using a distributed control system platform called Experimental Physics and Industrial Control System (EPICS) [16]. EPICS was originally developed at Los Alamos for the control of particle accelerator and has gain wide acceptance within the accelerator and nuclear physics community. However, it is not suitable for implementation of the safety functions directly. Care is taken to ensure that the system boundaries between the ACIS system and the rest of the control system are failsafe.

E. Hazard Analysis

The ACIS development process starts with the Hazard and Risk Analysis to identify the hazards and their causes, and to list appropriate mitigations needed to achieve a tolerable risk level. The document issued was used as input to the following development stage.

IEC 61509 [1] defines several alternative risk analysis tools/techniques. On most CLS safety projects the As-Low-As-Reasonably-Practical (ALARP) technique is used [1]. Using a qualitative as opposed to quantitative process appears to be the best practice for CLS, especially given the unique nature of some of the limit custom designed components that are used in some of the systems. Special care has been needed in doing the Hazard and Risk Analysis to try to identify anticipated changes in ensuring that the design does not preclude potential future experimental programs.

This process involves conceptual design review to determine if there are hazards intrinsic to the design, human factors task analysis to understand how operators and users interact with the systems., simulation and desktop walk-throughs to examine any potential failures at each stage using hazard guide words, in the forms of one-one interviews with stakeholders or a structured meeting/workshop driven by keywords.

For some common hazards found in the accelerator operation context, basic design pattern concept is also applied in the Hazard and Risk Analysis process. We express each of such hazards in a generic way when analyzing the hazards posed by a generic hazardous situation; this allows us to subsequently examine special cases that may exist in specific applications of the pattern.

Within the hazard analysis the mitigation is identified for each hazard to bring the residual risk to an acceptable level.

F. Design Requirements

The mitigations identified in the Hazard and Risk Analysis are then allocated to the sub-systems and refined to generate design requirements for the ACIS. Other internal or external guidelines, such as human factor guideline [13] and Canadian Electrical Code were also incorporated as requirements in this stage. A design manual is generated to document all requirements. Lockup zone layout drawings are generated to capture detailed requirements and design information. The drawings show zone configurations, lockup paths, and all safety components, which were all identified and numbered. The ACIS layout drawings make an IO count possible and will be used as the input documents for generation of engineering details in the following design phases.

III. SAFETY FUNCTIONS

The ACIS provides four major functions: *secure*, *lockup*, *annunciation*, and *interlocking*. As described in earlier sections, 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.

A. 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.

The accelerator 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 accelerator.

B. Lockup

A zone is considered locked up only when the lockup sequence, designed by the CLS Health Safety and Environment (HSE) department specifically 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

 ISBN: 978-1-61208-246-2

provide extra protection. Therefore, lockup function is implemented only in the PLC chain.

C. Annunciation

Horns and flashing lights are positioned in the zones and control room to provide audible and visual annunciations to personnel in those areas.

D. Interlocking

The accelerator is interlocked from both chains through multiple permissive channels to avoid single failure point. When the accelerator is interlocked the radiation source is removed and the system falls to the safe state.

Figure 2 shows the implementation of safety functions of Secure, Lockup, and Interlocking.

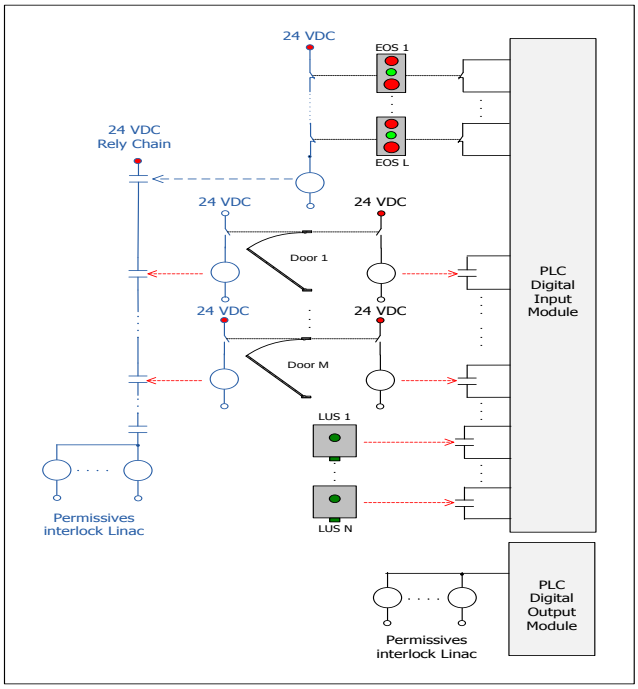

Figure 2. Implemetation of Secure, Lockup, and Interlocking

IV. ACIS HARDWARE

A. 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 Inputs/Outputs (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. 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, Electromagnetic Interference (EMI) noise and signal degradation using conventional means, this architecture is more reliable and safe.

B. Field Wiring

Some of the field wirings are located in the basement Linear Accelerator (Linac) hall, where leaking underground water at certain locations can cause problem. For this reason, National Electrical Manufacturers Association (NEMA) Type 4 rated 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 Canadian Standard Association (CSA) approved.

Extended design pattern concept is also adopted for the wiring design. Standard patterns associated with common sensor types and their common combinations are identified, and optimized wiring templates are developed. These patterns repeat themselves over and over for each common sensor type and combination and are generated using automated scripts in AutoCAD.

C. Operator Interface

The principle operator interface is based on the use of hard-wired operator panels. Some discrete I/O points are provided from the safety system to the EPICS based control system.

V. ACIS 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.

A. Design Pattern Based Program Sturcture

The concept of design pattern was first introduced in the field of architecture [14] and later has been adopted in other disciplines, especially software domain [15]. A design pattern involves three major elements: context, problem and solution [14]. Generally speaking, a design pattern is a solution to a commonly reoccurring problem in a given context.

In CLS ACIS design, several design patterns have been developed. These design patterns include the Zone Lockup design patter, the Major-Fault design pattern, and the All-Clear design pattern, each provides solution to a common ACIS problem. In this section, the Zone Lockup design pattern is used as an example to illustrate how design pattern approaches are used in CLS ACIS design.

For CLS lockup zones, although each of them are different in layout and geographical size, and contains different numbers of ACIS components, with different

 ISBN: 978-1-61208-246-2

lockup paths designed individually; the types of ACIS components in each zone are limited to a common set including Emergency Off Stations (EOSs), Lockup Stations (LUSs), Door Interlock Switches (SWDIs), Zone Lockup Lights (ZLLs), and Horns (HRNs), and the lockup sequence and interlock logic for all zones follow the same principles. Locking up an individual zone, and interlocking the accelerator based on zone lockup status, is a recurring problem in the context of CLS accelerator operations. A well-designed, optimized, and thoroughly tested set of best practices should be standardized to provide reusable solution to this problem. This formed the basis for design pattern based program structure.

The Plant View function under the Siemens SIMATIC Manager provide an ideal tool to support design pattern based program structure. In Plant View, the software is structured hierarchically following the actual lockup zone layout. A folder is assigned to each zone, and each zone folder has three CFC charts, known as the standard zone charts. The names of the standard zone charts comply with conventions as follow:

- ZONE<ID>_EOS
- ZONE<ID>_DOORS
- ZONE<ID>_LOCKUP

In the above naming convention, <ID> is a generic descriptor, when assigned to a specific zone, the real zone ID number should be used instead.

The ZONE<ID>_EOS chart contains codes to monitor EOS inputs of this zone and provide EOS status output to the ZONE<ID>_LOCKUP chart. The ZONE<ID>_DOORS chart monitors SWDI inputs of all doors and gates in this zone and provide shielding status output to the ZONE<ID>_LOCKUP chart. The ZONE<ID>_LOCKUP chart monitors inputs from zone LUSs and incorporated these inputs with the inputs from the other two charts to perform lockup sequence and provide outputs to annunciation and interlock modules.

In each of the standard zone charts, standard ACIS FBs are used to handle functions associated with generic components and process. All these ACIS FBs are developed in CLS, and have been thoroughly tested. The implementation details of FBs can be hidden from programmers who are new to ACIS design. For a programmer to use these FBs, all he or she needs to do is, choosing the right types and numbers of ACIS FBs based on the actual zone situation, and making interconnections between the inputs/outputs of component and process FBs .

The zone folder, standard charts, and standard ACIS FBs, as a whole, defines the structure of the Zone Lockup design pattern. As a template and a set of guidelines for the zone lock up problem, the design pattern is generic in nature, however, when instantiated, can accommodate differences and variations from zone to zone.

In a sense, the Zone Lockup design pattern encapsulates the initial ACIS designers' time and expertise to a reusable standard solution for the zone lock up problem. Therefore, the future designers need not to reinvent the wheel, and thus helps to lower cost and save time for future ACIS development. And reuse of well tested pattern also increases the reliability and continuity of the system as a whole.

B. 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. As mentioned in earlier section, those ACIS FBs play an important role in the implementation of design pattern based program structure.

C. 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.

D. Real-time Requirements

Based on the PLC cycle time, and execution time for the logic blocks, a spreadsheet is used to calculate the algorithm executive time and verify that the real time performance of the system can be achieved.

E. Version Control

For safety system software, it is critical to ensure correct version is loaded onto 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, a commercial version control software called MKS Source Integrity [18] is used for version control. Versions of the ACIS program at different development and maintenance stages are saved in the MKS repository. With the signatures as identifiers, the correct version can be easily located for download.

VI. EPICS INTERFACE

Currently, a limited number of discrete digital I/O channels are used to provide an interface between the ACIS and the EPICS system, with the EPICS based control system not performing a direct safety function.

The EPICS software is implemented in C/C++ running on either Real-Time Executive for Multiprocessor Systems (RTEMS) [17] or Linux based computers. The process variables from acquired by EPICS can be displayed to the operator as well as being feed into a central alarm management system for the entire facility.

An expected future enhancement is to feed both the ACIS and other high speed control interlocks into a custom sequence of events record to provide more accurate first fault indicator information.

 ISBN: 978-1-61208-246-2

VII. VALIDATION AND VERIFICATION

Validation and Verification (V&V) procedures are 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 document was developed by staffs who were not involved in the design process to assure independence. The V&V procedure is executed by HSE department, which was independent of the responsibilities for the design of the system. 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.

VIII. CONCLUSION AND FUTURE WORK

As an early adopter of IEC 61508, we faced several challenges in how to design engineering processes around the standard that reflected the safety requirements as well as the domain specific environment that we were working within. The use of design patterns played an important role through the entire process in being able to effectively and efficiently design these systems.

Tighter integration between the ACIS and EPICS is required to more effectively provide operational staff with the ability to accurately understand the sequence of events on an accelerator machine trip. There is currently a simplified sequence of events recorder in use for the Storage Ring (SR); however, this needs to be expanded. It is expected that such as system will require the use of high speed electronics.

Work is also underway in developing methods to streamline the verification and validation process, where testing is targeted separately at both the generic pattern that is reused as well as those aspects of the pattern that have the potential to be incorrectly implemented.

ACKNOWLEDGMENT

Research described in this paper was performed at the Canadian Light Source, which is supported by the Canadian Foundation for Innovation, Natural Sciences and Engineering Research Council of Canada, the National Research Council Canada, the Canadian Institutes of Health Research, the Province of Saskatchewan, Western Economic Diversification Canada, and the University of Saskatchewan.

REFERENCES

[1] International Electrotechnical Commission, IEC 61508, “Functional Safety of Elecronic/Programmable Electronic Safety-Ralated Systems" International Electrotechnical Commission, Geneva, 1998

[2] D. Fernandez-Carreiras et al., "ALBA, the PLC based protection system," in Proc. ICALEPCS 2009, pp. 397-399, Kobe, Japan, 2009.

[3] M. C. Wilson and A. G. Price, "Development of the Diamond Light Source PSS in conformance with 61508," in Proc. of ICALEPSC2011, pp. 1289-1292, Grenoble, France, 2011.

[4] P. Nanin, "IEC 61508 experience for the development of the LHC Functional Safety Systems and future perspectives," in Proc. of ICALEPCS 2009, pp. 400-402. , Kobe, Japan, 2009.

[5] K. Mahoney and H. Robertson, "Jefferson Lab IEC 61508/61511 safety PLC based safety systems," in . Proc. ICALEPCS 2009, pp. 394-396., Kobe, Japan, 2009.

[6] J. C. Chapuis, J. P. Arnoul, A. Hurs, and M. Manson, "The Laser Megajoule Facility personal safety system," in Proc. of ICALEPCS 2011, pp. 1070-1072, Grenoble, France, 2011.

[7] D. J. S. Findlay et al., "ISIS upgrade – a status report.," in Proc. HB2006, pp. 20-23, Tsukuba, Japan, 2006.

[8] S. Scheloske, S. Hanke, and J. Mosthaf, "Overview of the personal protection System at the Heidelberg Ion Therapy Facility," in Proc. of PCaPAC08, Ljubljan, Slovenia, pp. 88-90, 2008.

[9] G. Bassato et al.,"Safety requirements in SPES control system: preliminary design," in Proc. of ICALEPCS09, pp. 585-587, Kobe, Japan, 2009.

[10] A Armoush., E. Beckschulze, and S. Kowalewski. “Safety assessment of Design Patterns for safety-critical embedded systems” in Proc. 35th Euromicro Conference on Software Engineering and Advanced Applications pp. 523-527. DOI 10.1109/SEAA.2009.12, Paras, Greece, 2009

[11] S. P Kumar, P. S. Ramaiah, and V. Khanaa, “Architectural patterns to design software safety based safety-critical systems.” in Proc. ICCCS11, pp. 620-623, Odisha, India

[12] J. Rauhamäki1, T. Vepsäläinen1, and S. Kuikka1 “Functional safety system patterns.” in Proc. VikingPLoP 2012, pp. 47-68, Saariselkä, Finland

[13] M. McKibben, “CLS human factors workscope”, 0.1.1.1, Rev 1, 2008, unpublished

[14] C. Alexander, “A pattern languge : twons, buildings, construction.” Oxford University Press, New York, 1977

[15] E. Gamma, R. Helm, R. Johnson, and J. Vlissides. “Design Patterns: element of resusable object-oriented software.” Addison-Wesley, Boston, MA, USA, 1997

[16] http://www.aps.anl.gov/epics/ [retrieved: December, 2012]

[17] http://www.rtems.org/ [retrieved: December, 2012]

[18] http://www.mks.com/ [retrieved: December, 2012]

 ISBN: 978-1-61208-246-2