A HAZARD DRIVEN APPROACH TO ACCELERATOR SAFETY SYSTEM DESIGN – HOW CLS SUCCESSFULLY APPLIED ALARP IN THE DESIGN OF SAFETY SYSTEMS *

E. D. Matias#, Mighty Oaks, Victoria, BC, Canada
Grant Cubbon, Allen Hodges, Hao Zhang, Canadian Light Source, Saskatoon, SK, Canada
M. Benmerrouche, Brokhaven National Laboratory, Upton, NY, United States

Abstract

All large scale particle accelerator facilities end up utilising computerised safety systems for the accelerator access control and interlock system to supervise lockup search sequences and perform other safety functions. Increasingly there has been a strong move toward IEC 61508 based standards in the design of these systems. CLS designed and deployed its first IEC 61508 based system nearly ten years ago. The challenge has increasingly been to manage the complexity of requirements and ensure that features being added into such systems were truly requirements to achieve safety.

Over the past few years CLS has moved to a more structured Hazard Analysis technique that is tightly coupled and traceable through the design and verification of its engineered safety systems. This paper presents the CLS approach and lessons learned.

BACKGROUND

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. Other standards also taken into account include [1], [2] and [3].

One critical aspect in the application of these techniques is the need to perform structure hazard and risk analysis.

SAFETY SYSTEM DEVELOPMENT PROCESS

In the past accelerator facilitates when designing safety systems simply scaled up the rigor used in the design of their non-safety critical systems and tried to make the system as fail safe as possible. Over the past decade and half there has been 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[4]. The process starts with the hazard analysis, based on which requirements and specifications are generated, and the design and implementation naturally follows. 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.

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, general control functions developed by the facilities and those system that are modified by outside researches and users to meet their specific experimental needs are important.

A strong emphasis is places 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.

Care is required to clearly define these boundaries and limit the size and scope of the safety functionality.

This information is captured in a systems boundary drawing with the interfaces document and tightly controlled.

Hazard Analysis

The ACIS development process starts with the Hazard and Risk Analysis to identify the hazards and associated mitigations required[5]. This document is then used as an input to the following development stage.

The As Low as Reasonably Practicable (ALARP) methodology was adopted. Using a qualitative as opposed to quantitative process appears best especially given some of the limit custom designed components that are used in some of the systems. Special care has been needed in doing the HAZAN to try to identify anticipated changes in ensuring that the design does not preclude potential future experimental programs.

*Research described in this paper was performed at the Canadian Light Source, which is funded by the Canadian Foundation for Innovation, the Sciences and Research Council of Canada, the National Research Council Canada, the Canadian Institute of Health Research, the Government of Saskatchewan, Western Economic Diversification Canada and the University of Saskatchewan.
#elder.matias@mightyoaks.com

ISBN 978-3-95450-139-7

This process involved detailed analysis of the overall system driven by detailed analysis of the systems, interviews and workshops.

Careful attention was also given to the human factors engineering consideration of how operators and users interact with the systems. NREG-700 was used a basis for the human factors design.

We express each of the hazards in a generic way analysis the hazards posed by a generic lockup sequence, this then 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.

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 systemS. Other internal or external guidelines, such as human factor guideline [6] 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 are an input documents for the generation of engineering details in the following design phases.

HAZARD ANALYSIS PROCESS

The hazard analysis process being used is based on hazard identification and a qualitative risk analysis to determine adequate mitigation measures to ensure that residual risk is brought to a tolerable level. This process is illustrated in Figure 1. The outputs from the process consist of:

1. Establishing an enumerated list of the hazards and associated causes.
2. For each hazard and cause performing:
   a. a qualitative risk analysis to determine initial (unmitigated) risk,
   b. enumeration of the appropriate mitigation needed to achieve a tolerable level of risk, and
   c. a qualitative risk analysis to determine residual risk.
3. Each mitigation then becomes a requirement on the design of the facility or the associated operating procedures; these requirements are allocated to the appropriate sub-systems.
4. A safety integrity categorization level is defined for any safety system that must be developed.

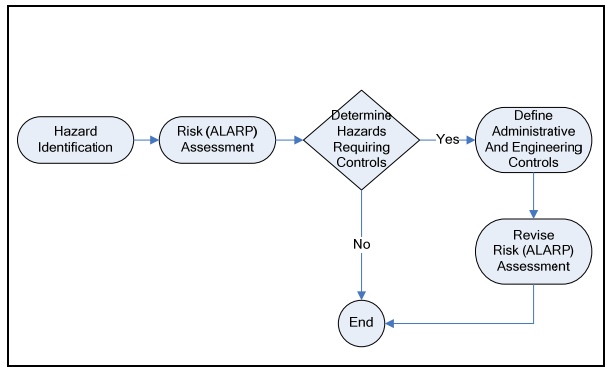

Figure 1: Hazard Analysis Process.

Hazard Identification

The hazard identification is based on normal use and reasonable foreseeable misuse. Once the hazards are established, the causal factors are then determined.

The analyst performing the hazard analysis must work with stakeholders to establish the risks. This activity is multi-disciplinary and requires applying many of the same techniques used for requirements analysis capture. At a minimum the following should be performed:

1. the conceptual design reviewed to determine if there are hazards intrinsic to the design,
2. human factors based task analysis should be performed to understand the actions required of operational staff and the associated systems permitting actions to be effectively performed, using walkthrough (through simulation and desktop walk-throughs)
3. by examining each aspect of the processes under control and examining any potential failures at each stage in a work process using hazard guide words,
4. the partitioning of functions between workers and various control sub-systems systems.

It is up to the analyst to determine the best method to gain the necessary information, for example, this could be through one-on-one interviews with stakeholders or through a structured meeting/workshop driven by key-words.

Depending on the stakeholder and the complexity of the system it may be necessary to focus the stakeholders into thinking about the hazards and mitigation as separate distinct concepts.

The analyst must critically review all of this information and ensure that conflicting information is resolved and structured in a coherent way. It is also necessary for the analyst to assess and resolve any gaps that may exist in the hazard identification.

The analyst must also probe situations where defence-in-depth is challenged, such as the EUC operating in a degraded fashion, under partial or complete power failure or reduced/fatigued staffing conditions. It is necessary to postulate the plausible failure of sub-components, procedures, services and examine how the defences in the system design are challenged.

ISBN 978-3-95450-139-7

For some types of system it may be useful to review process and instrumentation (PID) and process flow drawings (PFD) [7]. In this case guide words can be used to help explore failure modes, for example, for a flow instrument, one should consider what happens where there is a failure of the instrument, reversal, too much flow, to little flow, or contamination. Depending on the complexity and nature of the systems it may be necessary to systematically review specific parts or elements of the system to increasing levels of detail..

Once the risks are identified work is undertaken to identify the frequency and the consequence of the hazard. Two different scales are used for consequence one based on potential radiological exposure and the second used for conventional safety. Based on these criteria Table 1 is used to establish a risk class.

Table 1: ALARP Risk Class Assignment Table.

		Consequence			
		Severe	High	Medium	Low Negligible
Frequency	Frequent	I	I	I	II
	Probable	I	I	II	III
	Occasional	I	II	III	III
	Remote	II	III	III	IV
	Improbable	III	III	IV	IV
	Incredible	IV	IV	IV	IV

As illustrated in Figure 2 risk classification and mitigation is done based on a cost benefit analysis.

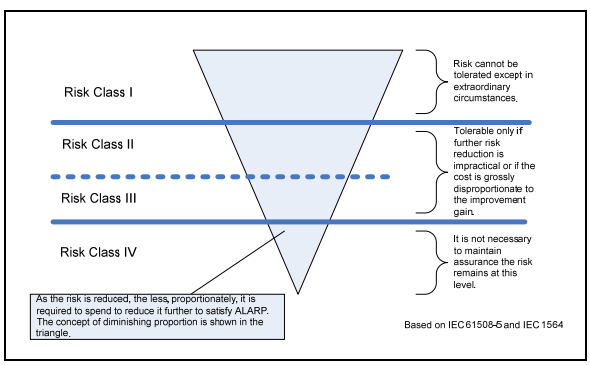

Figure 2: Tolerable Risk and ALARP.

Mitigation

Based on the risk class mitigation may be required.

When establishing mitigation, preference shall be given for mitigation in the following order:

1. Inherently Safe Design (ISD) – where possible, an inherently safe design shall be used, in other words the hazard shall be designed out of the system,
2. Fault-Tolerant Measure (FTM) – where an inherently safe design cannot be used, fault-tolerant measures shall be incorporated into the design to detect potential hazards and take appropriate actions,
3. Protective Measures (PM) – where the system cannot be designed to be inherently safe or fault-tolerant, protective measures (such as interlocks) shall be employed, and
4. Administrative Measures (AM) - where engineering controls (items 1-3) are not sufficient to fully protect against the hazard it may be necessary to provide human oversight or rely on other administrative or procedural controls.
5. Risk Transfer (RT) – where risk is transferred to an underwriter or other organization; (normally not used as part of the design process but in the case where the enterprise needs adequate assurance that it can recover from the risk; e.g., building insurance to rebuild after a fire.

The mitigation then becomes requirements placed on the safety system design. Traceability is provided from the requirement into the section of the design the implements the mitigation and down into the verification and validation procedures used to commission the system.

CONCLUSION

CLS has now successfully applied these techniques on several safety system over several years. We have found this to be both effective and efficient providing focus in identifying what mitigation is truly requirement and contributes to safety. Not only does this approach aid in ensuring appropriate mitigation is in place it also helps identify where mitigation is ineffective and should not be used.

REFERENCES

[1] ANSI N43.1 “Radiation Safety for the Design and Operation of Particle Accelerators”.
[2] IAEA Report !88 “Radiological Safety Aspects f the Operation of Electron Linear Accelerators” IAEA Vienna. Report No. 188. 1979.
[3] NCRP “Radiation Protection For Practical Accelerator Facilities” NCRP Rep. No. 144.
[4] E. Matias, “CLS Safety System Development Process” CLS Report 0.2.37.2 Rev. 3.
[5] E. Matias. “Hazard and Risk Analysis Procedure” CLS Report 7.7.52.5 Rev. 0.
[6] M. McKibben. “CLS Human Factors Work Scope” CLS Report 0.1.1.1 Rev. 2. 2008.
[7] E. Matias, et. al. “The use of PID for Accelerator and Beamline Control Applications at the CLS” ICALEPS 2009. Kobe, Japan TUP047.

ISBN 978-3-95450-139-7