



CLS Safety System Development Strategy

0.2.37.2 – Rev. 3

Date: 2008-10-09

Copyright 2008, Canadian Light Source Inc. This document is the property of Canadian Light Source Inc. (CLSI). No exploitation or transfer of any information contained herein is permitted in the absence of an agreement with CLSI, and neither the document nor any such information may be released without the written consent of CLSI.

Canadian Light Source Inc.
101 Perimeter Road
University of Saskatchewan
Saskatoon, Saskatchewan
S7N 0X4 Canada

	Signature	Date
	<i>Original signed by:</i>	
Author	_____ E. Matias	_____
Reviewer #1	_____ R. Tanner	_____
Reviewer #2	_____ G. Cubbon	_____
Reviewer #3	_____ M. de Jong	_____
Approver	_____ J. Hormes	_____

BLANK PAGE

Revision History

<i>Revision</i>	<i>Date</i>	<i>Description</i>	<i>Author</i>
A	1999-11-26	Original Draft	F. T. West R. Verhulst R. Thompson
0	2000-01-07	Issued for use.	F. T. West R. Verhulst R. Thompson
0A	2007-06-19	Issued for review.	E. Matias
0B	2007-06-22	Issued for review.	E. Matias
1	2007-07-13	Issued for use.	E. Matias
2	2007-12-07	Updated Section 4.2.7, 4.2.8 based on legal opinion and Section 5.0 based on recent documents. Issued for use.	E. Matias
2A	2008-09-25	Updated for Linac ACIS upgrade project, minor update to document references.	E. Matias
3	2008-10-09	Issued for use.	E. Matias

BLANK PAGE

TABLE OF CONTENTS

1.0	Introduction	1
1.1	Terminology.....	1
1.2	Abbreviations.....	1
2.0	Safety Systems	2
2.1	Linac Hall Safety System.....	2
2.2	BR1/SR1 ACIS	2
2.3	Beamline ACIS	2
2.4	ALFT ACIS	2
2.5	BMIT ACIS.....	3
2.6	Equipment motion control Systems	3
3.0	Management of Functional Safety.....	3
3.1	Policy and Strategy for Achieving Functional Safety	3
3.2	Organizational Responsibility	3
4.0	Safety Life Cycle Development Plan	4
4.1	Concept	4
4.2	Regulatory Context.....	5
4.2.1	Nuclear Safety and Control Act - Canadian Nuclear Safety Commission	5
4.2.2	System Engineering Guide	6
4.2.3	Quality Assurance - CAN/CSA-ISO 13485:03	6
4.2.4	IEC 61508.....	7
4.2.5	Ethical Review	7
4.2.6	Privacy	7
4.2.7	Radiation Emitting Devices Act.....	7
4.2.8	Food and Drug Act - Medical Devices Regulations	8
4.3	Overall Scope Definition	8
4.4	Hazard and Risk Analysis.....	8
4.5	Overall Safety Requirements.....	9
4.6	Safety Requirements Allocation	9
4.7	Overall Operation and Maintenance Planning.....	9
4.8	Overall Safety Validation Planning	9
4.9	Overall Installation and Commissioning Planning	10

4.10	Safety Related System Realization	10
4.11	Other Technologies Safety Related System Realization	10
4.12	External Risk Reduction Facilities: Realization	10
4.13	Overall Installation and Commissioning	10
4.14	Overall Safety Validation	10
4.15	Overall Operation Maintenance and Repair	11
4.16	Overall Modification and Retrofit	11
4.17	Decommissioning and Disposal	11
5.0	Documentation Plan	12
5.1	Accelerator Systems	12
5.2	Beamline Systems	13
5.3	ALFT	15
5.4	BMIT	15
5.5	O ₂ Monitoring	15
	References	16
	Appendix A: Committee Terms of Reference	18

1.0 INTRODUCTION

This document serves as the design input document for the various safety systems developed at the CLS. As such it serves the following purposes:

- a) defines the development plan for safety systems at the CLS, and
- b) defines the regulatory context for the systems.

Predominately based on IEC 61508, guidance in developing safety critical systems has also been taken into consideration, such as Leveson (1995) and Jackson et al. (2007).

Additional details on CLS Software and Control System Engineering process and procedures can be found in Matias (2006) and Matias (2007).

Human Factors Engineering activities have been embedded into the CLS engineering process, additional details can be found in McKibben (2008). Detailed operator interface design standards can be found in McKibben (2006).

1.1 TERMINOLOGY

Equipment Under Control (EUC) – Equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities (IEC 61508-4).

1.2 ABBREVIATIONS

ACIS – Access Control and Interlock System

ALARP – As Low As Reasonably Practical

BMIT – Bio-Medical Imaging and Therapy Facility

BMIT-BM – BMIT Bend-Magnet Beamline

BMIT-ID – BMIT Insertion Device Beamline

CID – Control and Instrumentation Development Department

E/E/PE – Electrical/Electronic/Programmable Electronic

E/E/PES - Electrical/Electronic/Programmable Electronic System

EUC – Equipment Under Control

HSE – Health Safety and Environment Department

IEC – International Electrotechnical Commission

ISO – (from the Greek *isos*) – International Organisation for Standardization

PLC – Programmable Logic Controller

POE – Primary Optical Enclosure

SIL – Safety Integrity Level

SOE – Secondary Optical Enclosure

2.0 SAFETY SYSTEMS

The CLS constructs and operates safety systems primarily for ensuring staff is not present in radiation areas when beam is on, monitoring hazardous material (cryogenics) and protecting the safety of employees, users and contractors (Benmerrouche 2006).

2.1 LINAC HALL SAFETY SYSTEM

Most synchrotron light source facilities have adopted a two-level redundant lock-up system and have a long history of safe operation. Historically the Saskatchewan Accelerator Laboratory (SAL) used two diverse chains for the lockup system, specifically:

- a) A hard-wired 115 VAC system.
- b) A Micro 84 programmable controllers system.

When the CLS was established in 1999, these systems were retained and still remain in use. These two systems have been in place since 1981 without any major failure. From 1981 to 2006 the only failures were minor ones such as light bulbs, a couple of relays and a few area horns all of which were found during normal lockup or on regularly scheduled maintenance periods. In each case the system failed in a safe way. With this experience it was felt that a two-level lock-up system was suitable for the CLS.

Over the past few years more failures have been detected and attributed to the age of the equipment. This system is now being replaced with a newer safety system.

The new proposed Linac ACIS system makes use of two redundant and diverse chains for the ACIS. One chain is based on modern safety-rated PLC technology that is certified for use in IEC 61508 applications. The second chain is based on relay technology. For the upgrade project a project plan (Zhang and Cubbon 2008), hazard analysis (Cubbon 2008) and a design manual (Zhang 2008b) have been prepared.

2.2 BR1/SR1 ACIS

The booster and storage ring tunnel make use of two redundant and diverse chains for the ACIS. One chain is based on modern safety-rated PLC technology that is certified for use in IEC 61508 applications.

2.3 BEAMLINER ACIS

Beamline enclosures (excluding BMIT) make use of the same ACIS system as the BR1/SR1 and are fully integrated into that system.

2.4 ALFT ACIS

The ALFT VSX-C is a standalone soft x-ray source which produces an 8.0 keV x-ray beam, when coupled with the focusing optics, the unit provides 10^9 photons/s through a 50 micron focal point. The ALFT unit is a registered x-ray source with SaskLabour.

The ALFT facility has a steel hatch. This system has a simple lockup sequence and makes use of a hard-wired lockup system that implements a similar search algorithm to the beamline enclosure ACIS.

2.5 BMIT ACIS

The BMIT ACIS is based on a similar design approach as the booster, storage ring and beamline enclosure. The system is implemented on a separate PLC to facilitate changes and testing of the system on a schedule that is independent of machine operation. It is expected that this system will undergo more frequent changes as it is tailored for specific medical research programs.

The BMIT safety systems have been designed to support Phase I and Phase II of BMIT but excluding Phase III (Matias 2008a). Phase I and II include experiments involving animals but exclude experiments involving humans.

Since BMIT poses special human factors consideration a BMIT specific human factors plan has been developed (McKibben and Matias 2008) and a specific ACIS human factors validation procedure (Matias 2008b).

2.6 EQUIPMENT MOTION CONTROL SYSTEMS

A variety of positioning systems are in use on beamlines at the CLS. These robotics and remote controlled systems are reviewed prior to installation and adequate safeguards are designed based on code and industry practice.

3.0 MANAGEMENT OF FUNCTIONAL SAFETY

This section is based on IEC 61508 Part 1 Section 6.

3.1 POLICY AND STRATEGY FOR ACHIEVING FUNCTIONAL SAFETY

CLSI is committed to ensuring that the safety systems are developed to relevant safety standards and will not unreasonably place at risk the safety of its staff, users or contractors.

3.2 ORGANIZATIONAL RESPONSIBILITY

The following organizational groups within CLS have the following responsibility for the ACIS system:

- a) the Control and Instrumentation Development (CID) Department is responsible for the design and installation of safety systems,
- b) the Engineering and Technical Services (ETS) Department is responsible for the mechanical and electrical design,
- c) the Health Safety and Environment (HSE) Department is responsible for performing Hazard Analysis, and independent Verification and Validation of safety systems,
- d) the Information and Communications Technology (ICT) Department is responsible for information management and data storage facilities at the CLS facility,
- e) the Experimental Facilities Division (EFD) is responsible for the optics design and scientific activities undertaken on and operation of beamline systems, and
- f) the Accelerator Operations Department is responsible for the operation of the accelerator systems.

The respective department manager has management oversight responsibility for the activities of his/her respective department. A more detailed definition of the responsibility can be found in Matias (2007) and Fetch (2004).

The Canadian Nuclear Safety Commission (CNSC) provides regulatory oversight on the CLS facility as the lead federal agency licensing the CLS.

It is the responsibility of the respective department manager to ensure that staff are adequately trained and qualified to perform the activities assigned.

4.0 SAFETY LIFE CYCLE DEVELOPMENT PLAN

IEC 61508 Part 1 is the safety system engineering development standard being used for this project. This standard defines the following life-cycle phases. Each of these is covered in the following sections.

- a) Concept;
- b) Overall Scope Definition;
- c) Hazard and Risk Analysis;
- d) Overall Safety Requirements;
- e) Safety Requirements Allocation;
- f) Overall Operations and Maintenance Planning;
- g) Overall Safety Validation Planning;
- h) Overall Installation and Commissioning and,
- i) Safety Related System Realization.

4.1 CONCEPT

"To develop a level of understanding of EUC and its environment (physical, legislative, etc) sufficient to enable the other safety lifecycle activities to be satisfactorily carried out." IEC 61508-1 Section 7.2.1

The Conceptual Design Report and Preliminary Design Report provide an outline and description of the major system and its associated hazards. For certain systems, such as BMIT, a hazard analysis is prepared.

Appendix A defines the membership of the CLS BMIT Human Studies Committee that has been mandated with developing a strategy for developing the infrastructure necessary to conduct human studies. The committee has representation from CLS, the Saskatoon Health Region, the Saskatoon Cancer Agency and SaskLabour. Section 4.2 defines the regulatory context.

4.2 REGULATORY CONTEXT

Table 1 defines the relevant regulatory standards required for each safety system at the CLS.

Table 1 - Regulatory Context

	Linac Hall Lockup System	BR1/SR1 ACIS	Beamline ACIS	BMIT ACIS	ALFT ACIS	O2 Monitoring System	BMIT Positioning Safety System	Equipment Motion Control Systems
● - Required by Act, Regulation or our Operating License ○ - Voluntarily Adopted by CLS								
Nuclear Safety Control Act and Associated Regulations	●	●	●	●	●	●	●	●
CLS System Engineering Guide ¹ CLS Procedures and Guides Canadian and Sask. Acts	○ ●	○ ●	○ ●	○ ●	○ ●	○ ●	○ ●	○ ●
CLS Safety Report ²	●	●	●	●	●	●	●	●
Canada Labour Code						●	●	●
CLS Quality Assurance Program ¹	●	●	●	●	●	●	●	●
CAN/CSA ISO 13486				●			●	
IEC 61508	○	○	○	○	○	○	○	
Ethical Review				○				
Privacy				●				

¹ CLS System Engineering Guide references certain codes, e.g., Electrical Code, where compliance is required by Law. The System Engineering Guide and Quality Assurance Manual define processes and activities that are subject to review and acceptance by the CNSC.

² CLS Safety Report is an Appendix A document, and can only be changed with the prior approval by the CNSC.

4.2.1 Nuclear Safety and Control Act - Canadian Nuclear Safety Commission

CLSI holds a Class IB Operating License issued by the Canadian Nuclear Safety Commission. Operation of the CLS is governed by the following:

1. CNSC Issued Particle Accelerator Operating License,

2. Nuclear Safety Control Act, and
3. CNSC Regulations for Class IB Nuclear Facilities.

The operating license and associated reference documents in Appendices A and B of the license shall be followed in developing safety systems at the CLS.

4.2.2 System Engineering Guide

CLS follows engineering codes and standards that are required by law, our operating license and professional societies that regulate certain certified or licensed staff engaged in design or development activities. These include the:

1. Canadian Electrical Code¹;
2. National Building Code 2005;
3. National Fire Code 2005;
4. Canada Labour Code (L-2);
5. Canadian Occupational Health and Safety Regulations (SOR/89-304);
6. Boiler and Pressure Vessel Act of Saskatchewan (B-5);
7. Laboratory Animal Facilities – Characteristics, Design and Development (CCAC),
8. Association of Professional Engineers and Geoscientists of Saskatchewan – Codes of Conduct and Practice, (for P.Eng and P Geo. designated staff)²; and
9. Canadian Information Processing Society – Codes of Conduct and Practice. (for ISP designated staff)³.

CLS has established a series of engineering standards covering other areas specific to the facility. Both those standards mandated by legislation and developed internally are defined in the CLS System Engineering Guide (Matias 2007). Some of these standards are locally developed while others are mandated by legislation.

The System Engineering Guide shall be followed in developing safety systems at the CLS.

4.2.2.1 Canada Labour Code

In 2006 the CLS was deemed to be a federal-work. CLS therefore falls under the jurisdiction of the *Canada Labour Code* and *Canadian Occupational Health and Safety Regulations* (SOR/86-304).

The Canada Labour Code and associated regulations shall be followed in developing safety systems at the CLS.

4.2.3 Quality Assurance - CAN/CSA-ISO 13485:03

CLS has developed a quality assurance program that governs the activities undertaken by CLSI. This quality assurance program has taken into account ISO 13495:03. S-213 is the Quality Assurance Standard for Class I Nuclear Facilities in Canada. ISO 13495:03 defines the Quality Assurance Program requirements for the design and manufacture of Medical Devices in Canada under Health Canada Regulations.

¹ As per the Electrical Inspections Act of Saskatchewan E-6.3

² As per the Engineering and Geosciences Professions Act of Saskatchewan E-9.3

³ As per the Canadian Information Processing Society of Saskatchewan Act C-0.2

The Quality Assurance Manual shall be followed in developing safety systems at the CLS.

4.2.4 IEC 61508

CLS has utilized IEC 61508 as a guide for developing safety systems. The plan in this document is in part derived from IEC 61508.

This development plan shall be considered and used where practical in developing safety systems at the CLS.

4.2.5 Ethical Review

The operation of the CLS and most CLS users' research projects are tri-council funded and therefore require compliance with the *Tri-council Policy Statement on Ethical conduct for Experiments involving Humans* (Interagency Secretariat 2005). Through a series of agreements between CLSI, the University of Saskatchewan and between the University of Saskatchewan and the tri-councils CLSI is bound by these requirements. CLS has developed procedures based on these requirements (Carter 2007 a & b).

The operation of BMIT shall be bound by the requirements of CLS procedures on ethical review.

4.2.6 Privacy

CLS is a "federal-work, undertaking, or business" falling under the *Personal Information Protection and Electronic Documents Act*. All personal information, including medical information, gathered by CLS is protected under this act. CLS is bound under Interagency Secretariat (2005) to protect the privacy of patient information.

CLS is not a "trustee" under the *Saskatchewan Health Information Protection Act* (H-0.021) and therefore is not covered by the Act. However the health region and any hospital involved in conducting experiments on the BMIT beamline would be covered by this act. For this reason the requirements of this act should be taken into account in designing the data acquisition and information management systems on the BMIT beamline. This is of a specific concern when doing research involving human subjects.

Specifically, CLS must maintain adequate procedures and information management controls over personal information (including personal data) collected on the BMIT beamline. This would impact ICT data management procedures and beamline data acquisition software design. This requirement is not expected to affect the design of the BMIT ACIS system, but will obviously impact the design of the BMIT control and data acquisition systems.

The Privacy Acts and Regulations shall be followed in the design of the BMIT facilities.

4.2.7 Radiation Emitting Devices Act

The Radiation Emitting Devices Act (R-1) governs the sale and importation of certain radiation emitting devices including medical x-ray machines, x-ray imaging equipment and electron microscopes. This act and the Radiation Emitting Devices Regulations are administered by the Minister of Health and Welfare.

Section 3 provides that the Act does not have application to a radiation emitting device designed primarily for the production of nuclear energy as defined under the Nuclear Safety and Control Act and the CLS is a licensed facility regulated under this legislation. The beamlines (including BMIT) are not a radiation emitting device as they are not capable of both producing and emitting radiation in isolation from the CLS facility which is regulated under the Nuclear Safety and Control Act. As a result, the beamlines (including BMIT) are not regulated under the Radiation Emitting Devices Act.

4.2.8 Food and Drug Act - Medical Devices Regulations

The BMIT beamline is the only part of the CLS facility intended to conduct experiments on human beings. Neither the Food and Drug Act (F-27) nor the Medical Devices Regulations (SOR/98-282) of Canada have application to the BMIT beamline or its operation.

The Food and Drug Act (F-27) and the Medical Devices Regulations (SOR/98-282) of Canada regulate certain activities for a broadly defined group of medical devices. Under the definition of medical devices and the schedules to the regulations, BMIT is a device by virtue of its intended employment as a research and, more pertinently from the perspective of this Act, a diagnostic tool and potentially a future therapeutic tool for human beings and animals, and a medical device for purposes of the regulations in connection with its human applications. Its specific classification as a medical device is Class III by virtue of its employment of ionizing radiation.

The Act's provisions do not apply to the BMIT beamline as the activities regulated by the Act proper in sections 3, 19 or 20 are not activities that will be conducted in connection with the BMIT beamline.

In connection with the regulation of devices under the regulations, the BMIT application for use in connection with animals is specifically excluded from the definition of medical devices and as a result from the application of the regulations. In regard to the regulation of medical devices under these regulations, none of the regulated activities which relate to either the sale or importation of such devices apply to the BMIT beamline. While the BMIT beamline will be constructed by CLSI in accordance with strict safety and technical requirements, CLSI is not a manufacturer for purposes of the regulations. The CNSC may impose certain provisions on the act on the CLS in the future.

Any conventionally available medical equipment that may be needed to support the operation of BMIT will be equipment licensed for sale in Canada under the act.

4.3 OVERALL SCOPE DEFINITION

"To determine the boundary of the EUC and the EUC control system; To specify the scope of the hazard and risk analysis (for example process hazards, environmental hazards, etc.)." IEC 61508-1 Section 7.3.1

Each system manual contains a detailed definition of the scope of the safety system, including a system boundary drawing. To the extent practical, the functionality of safety system is limited to those functions important to safety, while other functions are allocated to non-safety systems.

4.4 HAZARD AND RISK ANALYSIS

"To determine the hazards and hazardous events of the EUC and the EUC control system (in all modes of operation), for all reasonably foreseeable circumstances including fault conditions and misuse; To determine the event sequences leading to the hazardous events determined; To determine the EUC risks associated with the hazardous events determined". IEC 61508-1 Section 7.4.1.

The existing ACIS system on the accelerator and beamlines was based on the original 1981 design approach and philosophy. In 2001, CLS switched to implementing this approach using IEC 61508 certified equipment.

Subsequently for the BMIT facility a detailed Hazard Analysis based on the ALARP was developed. It is expected as the historical systems undergo major changes a similar hazard analysis will be performed.

4.5 OVERALL SAFETY REQUIREMENTS

“To develop the specification requirements, for the overall safety in terms of the safety functions requirements and safety integrity requirements, for the E/E/PE, safety-related systems, other technology safety-related systems and external risk reduction facilities, in order to achieve the required functional safety.” IEC 61508-1 Section 7.5.1

The hazard and risk analysis results in the definition of a series of mitigation requirements. These are identified and allocated to specific sub-systems to achieve a reasonable risk reduction. Based on the risk reduction needed to achieve a tolerable risk it is possible to identify a safety integrity level. The Hazard and Risk Analysis includes a discussion of the SIL level required for each E/E/PE system defined.

4.6 SAFETY REQUIREMENTS ALLOCATION

“To allocate the safety functions, contained in the specification for the overall safety requirements (both the safety functions requirements and the safety integrity requirements), to the designated E/E/PE safety-related systems, other technology safety related systems, and external risk reduction facilities; To allocate a safety integrity level to each safety function”. IEC 61508-1 Section 7.6.1

In the Hazard and Risk Analysis Report, under each hazard, a table can be found that lists each mitigation applicable to that hazard. Each of these mitigations is then allocated to a specific subsystem (e.g., ACIS) or, in the case of administrative controls, to a specific procedure (citing the relevant document number).

4.7 OVERALL OPERATION AND MAINTENANCE PLANNING

“To develop a plan for operating and maintaining the E/E/PE safety-related systems, to ensure that the required functional safety is maintained during operation and maintenance”. IEC 61508-1 Section 7.7.1

The Design Manual for each safety related E/E/PE system includes a discussion of the regular preventative maintenance required on each E/E/PE system. Each E/E/PE also has associated operation, calibration (where required) and verification and validation procedures. As part of the routine preventive maintenance program each E/E/PE system is subject to periodic re-validation and verification.

4.8 OVERALL SAFETY VALIDATION PLANNING

“To develop a plan to facilitate the overall safety validation of the E/E/PE safety-related systems.” IEC 61508-1 Section 7.8.1

A verification and validation plan is under development for each E/E/PE system.

4.9 OVERALL INSTALLATION AND COMMISSIONING PLANNING

“To develop a plan for the installation of the E/E/PE safety-related systems in a controlled manner, to ensure the required functional safety is achieved; To develop a plan for the commissioning of the E/E/PE safety-related systems in a controlled manner, to ensure the required functional safety is achieved.” IEC 61508-1, Section 7.9.1

The hardware is installed by qualified electronics/electrical technologists following an installation plan. The software is designed and installed by qualified software developers. CID will verify the installation through the use of a ring-out procedure as required prior to turn-over of the system to HSE. HSE will conduct an independent verification and validation of the system.

4.10 SAFETY RELATED SYSTEM REALIZATION

“To create E/E/PE safety-related systems conforming to the specification for the E/E/PES safety requirements (comprising the specification for the E/E/PES safety functions requirements and the specification for the E/E/PES safety integrity requirements).” IEC 61508-1 Section 7.10.1 and part 1 and 2.

The E/E/PE Design Manual and associated drawing set will define the realization of the system.

4.11 OTHER TECHNOLOGIES SAFETY-RELATED SYSTEM REALIZATION

“To create other technology safety-related systems to meet the safety functions requirements and safety integrity requirements specified for such systems (outside the scope of this standard).” IEC 61508-1 Section 7.11.1

Other technologies and methods may be needed for the realization of the system. To the extent practical, these systems shall be developed to an adequate level of reliability. Specific requirements shall be identified on a case-by-case basis in the hazard analysis or system design manuals.

4.12 EXTERNAL RISK REDUCTION FACILITIES: REALIZATION

“To create external risk reduction facilities to meet the safety functions requirements and safety integrity requirements specified for such facilities (outside the scope of this standard).” IEC 61507-1 Part 7.12.1

To the extent practical in reducing risk, external risk reduction facilities are incorporated into the design of CLS safety systems.

4.13 OVERALL INSTALLATION AND COMMISSIONING

“To install the E/E/PE safety-related systems; To commission the E/E/PE safety-related systems.” IEC 61508-1 Section 7.13.1

CLS has developed procedures, where appropriate, to manage the installation and commissioning of safety systems. In most cases a final independent verification and validation is performed.

4.14 OVERALL SAFETY VALIDATION

“To validate that the E/E/PE safety-related systems meet the specification for the overall safety requirements in terms of the overall safety functions requirements and the overall safety integrity requirements, taking into account the safety requirements allocation for the E/E/PE safety-related systems developed according to 7.6.” IEC 61508-1 Section 7.14.1

For each safety system, verification and validation procedures are developed and executed. The procedures cover both white box (verification) and black box (validation) tests.

4.15 OVERALL OPERATION MAINTENANCE AND REPAIR

“To operate, maintain and repair the E/E/PE safety-related systems in order that the required functional safety is maintained.” IEC 61508-1 Section 7.15.1

Maintenance and modifications to the system are performed by trained staff under the same direction as the original installation. Each safety system is inspected on an annual basis by redoing the verification and validation tests.

4.16 OVERALL MODIFICATION AND RETROFIT

“To ensure that the functional safety for the E/E/PE safety-related systems is appropriate, both during and after the modification and retrofit phase has taken place”. IEC 61508-1 Section 7.16.1.

CLS has developed an ECR/ECO process (Lowe 2004) to manage changes to all of its systems, including the safety system.

4.17 DECOMMISSIONING AND DISPOSAL

“To ensure that the functional safety for the E/E/PE safety-related systems is appropriate in the circumstances during and after the activities of decommissioning or disposing of the EUC.” IEC 61508-1 Section 7.17.1

CLS has developed a decommissioning plan for the entire facility. Safety systems within the CLS are not expected to pose undue risk to the safety of workers or the environment and therefore decommissioning plans will be developed when required at the end of the useful life of the E/E/PE.

5.0 DOCUMENTATION PLAN

In addition to the system specific documentation listed in the following tables, the following common documents have also been developed:

- Safety System Ring-out Procedure CLS Doc. No. 7.7.52.1 - (Tanner 2008)
- Personnel Safety System Jumper Request Procedure CLS Doc. No. 11.7.52.4 – (Cubbon 2003)

5.1 ACCELERATOR SYSTEMS

Table 2 – Accelerator System Documentation Structure

System	Operation	Design	Verification
Linac (Existing)	Linac to LTB1 Lockup Procedure. (2.7.37.2)	Personnel Safety Lockup System (1.2.37.2) Personnel Safety Lockup System Micro 84 Program. (1.2.37.3)	See associated check-sheets on file.
Linac (Proposed)	Linac to LTB1 Lockup Procedure. (2.7.37.2)	Linac ACIS Upgrade Project Plan (1.12.52.1) Linac ACIS Design Manual (1.9.52.1)	Linac ACIS Verification and Validation Procedure (In Preparation) Linac ACIS Human Factors Validation Procedure (In Preparation)
LTB1	Linac to LTB1 Lockup Procedure. (2.7.37.2)	Access Control and Interlock System for Zone 6 & 7. (1.2.37.4)	See associated check-sheets on file.
BR1	Booster Ring Lockup Procedure (5.7.37.1)	Booster/Storage Ring/Beamlines Access Control and Interlock System. (7.9.39.4) CLS Lockup PLC Technical Specification. (7.4.37.1)	Booster Ring Verification Procedure (3.7.37.2) Booster/Storage Ring/Beamlines ACIS Verification and Validation Procedure (7.7.39.11)
SR1	Storage Ring Lockup Procedure (5.7.52.1)	Booster/Storage Ring/Beamlines Access Control and Interlock System. (7.9.39.4)	Storage Ring Verification Procedure (5.7.37.2)

System	Operation	Design	Verification
		CLS Lockup PLC Technical Specification. (7.4.37.1)	Storage Ring Verification Report (5.7.37.2) Booster/Storage Ring/Beamlines ACIS Verification and Validation Procedure (7.7.39.11)

5.2 BEAMLINER SYSTEMS

Table 3 – Beamline System Documentation Structure

System	Operation	Design	Verification
CMCF	08ID ACIS Lockup Procedure (6.7.52.10)	Booster/Storage Ring/Beamlines Access Control and Interlock System. (7.9.39.4) CLS Lockup PLC Technical Specification. (7.4.37.1)	08ID-1 (CMCF) ACIS Verification and Validation Procedure (6.7.52.7) V&V Reports – Issued annually in the 6.5.52.xx document series.
CMCF2	08B1-1 CMCF2 ACIS Lockup Procedure (6.7.52.21)	Booster/Storage Ring/Beamlines Access Control and Interlock System. (7.9.39.4) CLS Lockup PLC Technical Specification. (7.4.37.1)	08B1-1 (CMCF2) ACIS Verification and Validation Procedure (6.7.52.20) V&V Reports – Issued annually in the 6.5.52.xx document series.
Far-IR	Not applicable – This beamline does not require a radiation hatch.	Not applicable.	Not applicable.
HXMA	06ID-1 ACIS Lockup Procedure (6.7.52.9)	Booster/Storage Ring/Beamlines Access Control and Interlock System. (7.9.39.4) CLS Lockup PLC Technical Specification. (7.4.37.1)	06ID-1 ACIS Verification and Validation Procedure (6.7.52.8) V&V Reports – Issued annually in the 6.5.52.xx document series.
Mid-IR	Not applicable – This beamline does not require a radiation hatch.	Not applicable.	Not applicable.
OSR	Not applicable – This beamline does not require a radiation hatch.	Not applicable.	Not applicable.

PGM	11ID ACIS Lockup Procedure (6.7.52.1)	Booster/Storage Ring/Beamlines Access Control and Interlock System. (7.9.39.4) CLS Lockup PLC Technical Specification. (7.4.37.1)	11ID ACIS Verification and Validation Procedure (6.7.52.2) V&V Reports – Issued annually in the 6.5.52.xx document series.
REIXS	10ID ACIS Lockup Procedure (6.7.52.4) 10ID POE Training Form (11.11.52.12)	Booster/Storage Ring/Beamlines Access Control and Interlock System. (7.9.39.4) CLS Lockup PLC Technical Specification. (7.4.37.1)	10ID ACIS Verification and Validation Procedure (6.7.52.3) V&V Reports – Issued annually in the 6.5.52.xx document series.
SGM	<i>See PGM – shared safety system.</i>		
SM	<i>See REIXS – shared safety system.</i>		
SXRMB	06B1-1 ACIS Lockup Procedure (6.7.52.14)	Booster/Storage Ring/Beamlines Access Control and Interlock System. (7.9.39.4) CLS Lockup PLC Technical Specification. (7.4.37.1)	06B1-1 ACIS Verification and Validation Procedure (6.7.52.11) V&V Reports – Issued annually in the 6.5.52.xx document series.
SyLMAND	05-B2-1 ACIS Lockup Procedure (6.7.52.18)	Booster/Storage Ring/Beamlines Access Control and Interlock System. (7.9.39.4) CLS Lockup PLC Technical Specification. (7.4.37.1)	05B2-1 ACIS Verification and Validation Procedure (6.7.52.18) V&V Reports – Issued annually in the 6.5.52.xx document series.
VESPERS	07B2-1 ACIS Lockup Procedure (6.7.52.14)	Booster/Storage Ring/Beamlines Access Control and Interlock System. (7.9.39.4) CLS Lockup PLC Technical Specification. (7.4.37.1)	07B2-1 ACIS Verification and Validation Procedure (6.7.52.13) V&V Reports – Issued annually in the 6.5.52.xx document series.
XSR	02B2-2 ACIS Lockup Procedure (6.7.52.6)	Booster/Storage Ring/Beamlines Access Control and Interlock System. (7.9.39.4) CLS Lockup PLC Technical Specification. (7.4.37.1)	02B2-2 (XSR) ACIS Verification and Validation Procedure (6.7.52.5) V&V Reports – Issued annually in the 6.5.52.xx document series.

5.3 ALFT

Table 4 – ALFT System Documentation Structure

System	Operation	Design	Verification
ALFT	ALFT Enclosure ACIS Lockup Procedure (11.7.52.11)	<i>See detailed drawings.</i> - TST/ME/0107178 - TST/ME/0107179 - TST/EE/0107180 - TST/EE/0107184	ALFT Enclosure ACIS Verification and Validation Procedure (8.7.52.1) V&V Reports – Issued annually in the 6.5.52.xx document series.

5.4 BMIT

Table 5 – BMIT System Documentation Structure

System	Operation	Design	Verification
BMIT	Planning for Human Studies on BMIT (26.12.1.3) BMIT Operational Task Description (26.12.1.2) BMIT ACIS Lockup Procedure (6.7.52.16)	BMIT ID POE1 Three Position Safety Shutter Design (26.2.47.1) BMIT Hazard and Risk Analysis (26.2.37.1) BMIT ACIS System Design Manual (26.9.52.1)	BMIT ACIS Verification and Validation Procedure (6.7.52.17) V&V Reports – Issued annually in the 6.5.52.xx document series.

5.5 O₂ MONITORING

Table 6 – BMIT System Documentation Structure

System	Operation	Design	Verification
O ₂	Oxygen Monitoring System Alarm Response Procedure (11.7.52.3) Oxygen Sensor Calibration Procedure (11.7.56.2 Rev. 0)	Oxygen Monitoring and Liquid Nitrogen Distribution Component Manual (7.9.52.1)	Verification and Validation Procedure for the O ₂ Monitoring and LN ₂ Distribution System (7.9.52.2)

REFERENCES

- Benmerrouche, M. 2006. *CLS Safety Report*. Rev. 6.
- Carter, L. 2007a. *CLSI Ethics Guidelines: Involving Humans*. CLS Tech. Doc. 22.1.1.3, Rev. 2
- Carter, L. 2007b. *CLSI Ethics Guidelines: when animals are involved*. CLS Tech. Doc. 22.1.1.4 Rev. 1
- Cubbon, G. 2003. *Personnel Safety System Jumper Request Procedure*. CLS Tech. Doc. 11.7.52.4 Rev. 0.
- Cubbon, G. 2008. *Linac ACIS Hazard and Risk Analysis*. CLS Tech. Doc 11.18.52.1 Rev. 0.
- Fetch, N. 2004. *Organisation Management*. CLS Tech. Doc. 0.1.1.15 Rev. 0.
- Jackson, D. et. al. 2007. *Software for Dependable Systems: Sufficient Evidence?* Joint Committee on Certifiably Dependable Software Systems, National Research Council. The National Academies Press. Washington, D.C. ISBN 0-309-10857-8
- Interagency Secretariat 2005. *Tri-Council Policy Statement – Ethical Conduct for Research Involving Humans*. Interagency Secretariat on Research Ethics. Public Works and Government Services Canada. ISBN 0-662-40236-7. 2005.
- Leveson, N. 1995. *SAFWARE: System Safety and Computers*. Addison-Wesley Publishing Co. ISBN 0-201-11972-2
- Lowe, D. 2004. *Engineering Change Request & Engineering Change Order Procedure*. CLS Tech. Doc. 0.7.1.3 Rev. 0.
- Matias, E. 2001. *CLS Lockup PLC Technical Specification*. CLS Tech. Doc. 7.4.37.1. Rev. 0.
- Matias, E. 2006. *Control and Instrumentation Department Development Guide* CLS Tech. Doc. 7.1.39.1 Rev. 1.
- Matias, E. 2007. *System Engineering Guide*. CLS Tech. Doc. 0.1.69.1 Rev. 1.
- Matias, E. 2008. *BMIT Development, Commissioning and Operations Plan*. CLS Tech. Doc. 26.12.40.1 Rev. 3.
- Matias, E. 2008b. *BMIT ACIS Human Factors Validation Procedure* CLS Tech. Doc. 26.7.52.1 Rev. 0.
- McKibben, M. 2006. *Control System Common Specification*. CLS Tech. Doc. 7.4.39.1 Rev. 3.
- McKibben, M. 2008. *Human Factors Workscope*. CLS Tech. Doc. 0.1.1.1 Rev. 2.
- McKibben, M. and E. Matias 2008. *BMIT Human Factors Engineering Program Plan*. CLS Tech. Doc. 26.12.1.4 Rev. 1.
- Tanner, R. 2008. *Safety System Ring-out Procedure*. CLS Tech. Doc. 7.7.52.1 Rev. 4.
- West, F. T. 2001a. *Personnel Safety Lockup System* CLS Tech. Doc. 1.2.37.2. Rev. 0.
- West, F. T. 2001b. *Personnel Safety Lockup System Micro 84 Program*. CLS Tech. Doc. 1.2.37.3. Rev. 0.
- West, F. T. 2002. *Access Control and Interlock System for Zone 6 & 7*. CLS Tech. Doc. 1.2.37.4 Rev. 0.
- West, F. T. 2002. *Linac to LTB1 Lockup Procedure*. CLS Tech. Doc. 2.7.37.2 Rev. 2.

Zhang, H. and G. Cubbon 2008. *Linac ACIS Upgrade Project Plan*. CLS Tech. Doc. 1.12.52.1 Rev. 0.

Zhang, H. 2008. *LINAC ACIS Design Manual*. CLS Tech. Doc. 1.9.52.1 Rev. 0.

APPENDIX A: COMMITTEE TERMS OF REFERENCE



Canadian Light Source Inc.
University of Saskatchewan
101 Perimeter R.d.
Saskatoon SK
S7N 0X4 Canada
Tel: 306-657-3500
Fax: 306-657-3535
www.lightsource.ca

October 13, 2006

Dear Colleague:

Re: BMIT Human Studies Committee

As you know, I am setting up the BMIT Human Studies Committee. I am most grateful for your willingness to serve the Canadian Light Source Inc. as a member of this important committee. This letter is to inform you of the fundamental purpose and goals of the Committee. Beyond the fundamentals, what we do will be determined by what we learn as we meet and discuss the many issues surrounding human research studies at the BMIT facility at CLS.

Basically, within only a few years we anticipate that research programs involving human volunteers in both imaging and radiation therapy will commence at BMIT. In order to proceed to human studies, CLSI must ultimately have its operating license amended by the Canadian Nuclear Safety Commission. It will be necessary to inform the CNSC through a formal document of all the plans and agreements that we will undertake to meet all regulatory and ethical requirements.

Our starting point is this committee. We have members representing CLSI for HSE, QA, experimental facilities and senior management, the principal investigator for BMIT, the U of S College of Medicine, the U of S VP Research Office and Ethics Committee, and the Saskatoon Health Region. The membership may evolve as we better understand the issues that we will be dealing with. A membership list, with contact coordinates, is attached.

I have been involved in obtaining permission for human studies at synchrotron facilities three times in the past: Stanford Synchrotron Radiation Facility (DOE SLAC Laboratory), National Synchrotron Light Source (DOE Brookhaven National Laboratory), and the European Synchrotron Radiation Laboratory (Grenoble, France). The following is my starting point of issues that we will discuss, and go wherever we must to achieve the goal of CNSC permission to carry out the human studies:

1. Accreditation of the BMIT facility at CLS by appropriate provincial and other organizations (local, university, federal) if necessary
2. Ethics review process and authorizations
3. Radiation safety validation
4. Authority and responsibilities of medical, U of S, and CLSI staff at each phase of the research program, including the actual time of an imaging or therapy session at CLS
5. Liability issues

There will be other matters that arise as we move forward. I see the first meeting(s) focused on identifying as many issues as possible, and forming a strategy for action on the issues. We can also discuss the make-up of the committee for completeness and efficiency.

The time scale for completion of the work of the committee is not fixed, but we anticipate human studies commencing as early as July 2009. Thus we must have obtained all necessary permissions and licenses prior to that time.

Betty Harper will be contacting you to establish a meeting to be held at the CLS in November to further organize the committee agenda.

Thanks so much for participating on the committee.

Sincerely,

William Thomson

Enclosure

**Canadian Light Source Inc.
BMIT Human Studies Committee**

Membership – October 2006

Institution	Member	E-Mail	Phone
Canadian Light Source 101 Perimeter Road Saskatoon, SK S7N 0X4	Bill Thomlinson Executive Director (Committee Chair)	william.thomlinson@lightsource.ca cc: betty.harper@lightsource.ca	657-3600
Canadian Light Source 101 Perimeter Road Saskatoon, SK S7N 0X4	Tom Ellis Research Director	thomas.ellis@lightsource.ca cc: marie.knowles@lightsource.ca	657-3602
Canadian Light Source 101 Perimeter Road Saskatoon, SK S7N 0X4	Mo Benmerrouche Manager, HSE	mohamed.benmerrouche@lightsource.ca	657-3514
Canadian Light Source 101 Perimeter Road Saskatoon, SK S7N 0X4	Elder Matias Manager, Controls	elder.matias@lightsource.ca	657-3551
Canadian Light Source 101 Perimeter Road Saskatoon, SK S7N 0X4	Tomasz Wysokinski BMIT Beamline Scientist	tomasz.wysokinsky@lightsource.ca	657-3710
University of Saskatchewan College of Medicine B 103 Health Science Building 107 Wiggins Road Saskatoon SK S7N 5E5	Jim Thornhill Associate Dean, Research and Basic Sciences	jim.thornhill@usask.ca cc: sara.kjelshus@usask.ca	966-8119

University of Saskatchewan Anatomy & Cell Biology B303 Health Science Building 107 Wiggins Road Saskatoon, SK S7N 5E5	Dean Chapman BMIT Scientific Lead	dean.chapman@usask.ca	966-4111
University of Saskatchewan 110 Gymnasium Place Saskatoon, SK S7N 4J8	Tom Graham Health Research Facilitator	tom.graham@usask.ca cc: kimberly.porter@usask.ca	966-1733
University of Saskatchewan Room 302 Kirk Hall 117 Science Place Saskatoon, SK S7N 5C8	Susan Blum Ethics Unit Manager	susan.blum@usask.ca	966-8585
Saskatoon Health Region 3rd Floor 410-22nd Street East Saskatoon SK S7K 5T6	Sheldon Wiebe	sheldon.wiebe@saskatoonhealthregion.ca	655-2371
Saskatoon Health Region 3rd Floor 410-22nd Street East Saskatoon SK S7K 5T6	Bryan Witt	bryan.witt@saskatoonhealthregion.ca	655-1797

**Subsequent to the Original Formation of the Committee the Following
Changes were made as of July 2007.**

**BMIT Human Studies Committee
Membership – July 2007**

Institution	Member	E-Mail	Phone
Canadian Light Source 101 Perimeter Road Saskatoon, SK S7N 0X4	Bill Thomlinson Executive Director (Committee Chair)	william.thomlinson@lightsource.ca cc: betty.harper@lightsource.ca	657-3600
Canadian Light Source 101 Perimeter Road Saskatoon, SK S7N 0X4	Tom Ellis Research Director	thomas.ellis@lightsource.ca cc: marie.knowles@lightsource.ca	657-3602
Canadian Light Source 101 Perimeter Road Saskatoon, SK S7N 0X4	Mo Benmerrouche Manager, HSE	mohamed.benmerrouche@lightsource.ca	657-3514
Canadian Light Source 101 Perimeter Road Saskatoon, SK S7N 0X4	Elder Matias Manager, Controls	elder.matias@lightsource.ca	657-3551
Canadian Light Source 101 Perimeter Road Saskatoon, SK S7N 0X4	Tomasz Wysokinski BMIT Beamline Scientist	tomasz.wysokinski@lightsource.ca	657-3710
University of Saskatchewan College of Medicine B 103 Health Science Building 107 Wiggins Road Saskatoon SK S7N 5E5	Jim Thornhill Associate Dean, Research and Basic Sciences	jim.thornhill@usask.ca cc: sara.kjelshus@usask.ca	966-8119
University of Saskatchewan Anatomy & Cell Biology B303 Health Science Building 107 Wiggins Road Saskatoon, SK S7N 5E5	Dean Chapman BMIT Scientific Lead	dean.chapman@usask.ca	966-4111
University of Saskatchewan 110 Gymnasium Place Saskatoon, SK S7N 4J8	Tom Graham Health Research Facilitator	tom.graham@usask.ca cc: kimberly.porter@usask.ca	966-1733
University of Saskatchewan Room 302 Kirk Hall 117 Science Place Saskatoon, SK S7N 5C8	Susan Blum Ethics Unit Manager	susan.blum@usask.ca	966-8585
Saskatoon Health Region 3rd Floor 410-22nd Street East Saskatoon SK S7K 5T6	Sheldon Wiebe	sheldon.wiebe@saskatoonhealthregion.ca	655-2371
Saskatoon Health Region 3rd Floor 410-22nd Street East Saskatoon SK S7K 5T6	Bryan Witt	bryan.witt@saskatoonhealthregion.ca	655-1797
Saskatchewan Labour, OHS Division	Steve Webster, Health Physicist	swebster@lab.gov.sk.ca	933-7775
Saskatoon Cancer Centre/Oncology	Claude LaPointe	claudelapointe@saskcancer.ca	655-2693