



Design Requirement

FUEL HANDLING CONTROLS SYSTEM

ACR

108-63581-DR-001

Revision 1

Prepared by
Rédigé par

Popratnjak Branka

Reviewed by
Vérifié par

Francis Chris

Approved by
Approuvé par

Millard Julian W.F.

2003/04/07
**Controlled
Licensing**

©Atomic Energy of
Canada Limited

2251 Speakman Drive
Mississauga, Ontario
Canada L5K 1B2

2003/04/07
**Contrôlé
Licensing**

©Énergie Atomique du
Canada Limitée

2251 rue Speakman
Mississauga (Ontario)
Canada L5K 1B2



Design Requirement

Fuel Handling Control System

ACR

108-63581-DR-001

Revision 1

2003 April

Avril 2003

**CONTROLLED -
Licensing**

**CONTRÔLÉ -
Licensing**

This document and the information contained in it is made available for licensing review. All rights reserved by Atomic Energy of Canada Limited. No part of this document may be reproduced or transmitted in any form or by any means, including photocopying and recording, without the written permission of the copyright holder, application for which should be addressed to Atomic Energy of Canada Limited. Such written permission must also be obtained before any part of this document is stored in a retrieval system of any nature.

Le présent document et l'information qu'il contient sont disponibles pour examen en vue de l'obtention des permis. Tous droits réservés par Énergie atomique du Canada limitée. Il est interdit de reproduire ou de transmettre, par quelque procédé que ce soit, y compris de photocopier ou d'enregistrer, toute partie du présent document, sans une autorisation écrite du propriétaire du copyright obtenue auprès d'Énergie atomique du Canada limitée. De plus, on doit obtenir une telle autorisation avant qu'une partie du présent document ne soit intégrée dans un système de recherche documentaire de quelque nature que ce soit.

© Atomic Energy of
Canada Limited

© Énergie atomique du
Canada limitée

2251 Speakman Drive
Mississauga, Ontario
Canada L5K 1B2

2251, rue Speakman
Mississauga (Ontario)
Canada L5K 1B2



Design Requirement

Fuel Handling Control System

ACR

108-63581-DR-001

Revision 1

Prepared by
Rédigé par

B. Popratnjak
ACR Reactor & Fuel Handling Engineering

Reviewed by
Examiné par

D. Grossman
ACR Reactor & Fuel Handling Engineering

Approved by
Approuvé par

J. Millard
Manager, ACR Reactor & Fuel Handling

2003 April

**CONTROLLED -
Licensing**

© Atomic Energy of
Canada Limited

2251 Speakman Drive
Mississauga, Ontario
Canada L5K 1B2

Avril 2003

**CONTRÔLÉ -
Licensing**

© Énergie atomique du
Canada limitée

2251, rue Speakman
Mississauga (Ontario)
Canada L5K 1B2



Release and Revision History

Liste des documents et des révisions

0939B Rev. 13

Document Details / Détails sur le document

Title
Titre

Fuel Handling Control System

Total no. of pages
N^{bre} total de pages

CONTROLLED - Licensing / CONTRÔLÉ - Licensing

Release and Revision History / Liste des documents et des révisions

Release Document		Revision Révision		Purpose of Release; Details of Rev./Amendment Objet du document; détails des rév. ou des modif.	Prepared by Rédigé par	Reviewed by Examiné par	Approved by Approuvé par
No./N ^o	Date	No./N ^o	Date				
1		D1	02/09/23	Issued for review and comment.	B. Popratnjak	D. Grossman M. Leaker D. Duncan C. Francis J. Harber O. Hines R. Leger J. Yip	
2		0	02/11/12	Issued as "approved for use".	B. Popratnjak	See above	J. Millard / J.W. Love
3		1	03/04/07	Issued as "Approved for Use". Classification change from "Controlled" to "Controlled - Licensing".	B. Popratnjak	See above	J. Millard

DCS/RMS Input / Données SCD ou SGD

Rel. Proj. Proj. conn.	Project Projet	SI	Section	Serial Série	No. N ^o	Sheet Feuille	Of De	Unit No.(s) Tranche n ^o
	108		DR	001	1	1		

TABLE OF CONTENTS

SECTION	PAGE
1.	INTRODUCTION..... 1-1
1.1	Design Principles..... 1-1
1.2	Acronyms 1-2
2.	FUNCTIONAL REQUIREMENTS 2-1
2.1	Safety Functional Requirements 2-1
2.2	Operational Functional Requirements..... 2-1
2.2.1	Normal Operations 2-1
2.2.2	Abnormal Operations 2-2
2.2.3	Upset and Emergency Operations 2-2
2.2.4	FH DCS 2-2
2.2.4.1	Sequential Control..... 2-4
2.2.4.1.1	Structure of the Supervisory Sequential Control System..... 2-4
2.2.4.1.2	Modes of Supervisory Sequential Control 2-4
2.2.4.1.3	Operator Intervention During Supervisory Sequential Control 2-4
2.2.4.1.4	Mechanism Sequential Control 2-5
2.2.4.2	Logic Control 2-5
2.2.4.3	PID Control 2-5
2.2.4.4	Motion Control..... 2-6
2.2.4.4.1	Brushless DC Drive Motion Control..... 2-6
2.2.4.4.2	AC Drive Motion Control 2-7
2.2.4.4.3	Modes of Motion Control..... 2-7
2.2.4.4.4	Operator Intervention During Motion Control..... 2-7
2.2.4.5	Computational Functions 2-8
2.2.4.6	Control Execution 2-8
2.2.4.7	Monitoring Functions..... 2-9
2.2.4.8	I/O System..... 2-9
2.2.4.9	Communication System 2-10
2.2.4.10	Interface between the FH DCS and the EWS 2-10
2.2.4.11	Interface between the FH DCS and the FDS..... 2-11
2.2.4.12	Interface between the FH DCS and the Backup Control Panel..... 2-11
2.2.5	Protective Interlock System 2-11
2.2.6	Seismic Trip System..... 2-12
3.	PERFORMANCE REQUIREMENTS 3-1
3.1	Sequence Control Execution Time..... 3-1
3.2	Data Transfer between Sequential Controller and Subsystem/Motion Control Processors..... 3-1
3.3	Motion Control Loop Update Time for Brushless DC Drives 3-2
3.4	Motion Control Loop Update Time for AC Drives..... 3-2
3.5	PID Control Loop Update Time..... 3-2

TABLE OF CONTENTS

SECTION	PAGE
3.6	Position Data Transfer from FH DCS to FDS Interface 3-2
3.7	Transfer Time for Commands from FDS Interface to FH DCS..... 3-3
3.8	Data Transfer from FH DCS to FDS Interface (Excluding Position Data)..... 3-3
3.9	Analogue Input Conversion 3-4
3.10	Seismic Sensing Range 3-4
3.11	Seismic Sensing Accuracy 3-4
4.	SAFETY REQUIREMENTS 4-1
4.1	Applicable Requirements from Safety Design Guides 4-1
4.1.1	108-03650-SDG-001, Safety Related Systems 4-1
4.1.2	108-03650-SDG-002, Seismic Requirements 4-1
4.1.3	108-03650-SDG-003, Environmental Qualification 4-1
4.1.4	108-06350-SDG-004, Separation of Systems and Components 4-2
4.1.5	108-03650-SDG-005, Fire Protection 4-2
4.1.6	108-03650-SDG-006, Containment 4-2
4.1.7	108-03650-SDG-007, Radiation Protection 4-2
4.2	Specific Requirements from Applicable Canadian Nuclear Safety Commission (CNSC) Regulatory Documents 4-2
4.3	Protection Against Environmental Hazards 4-3
4.4	Protection Against Impact Forces 4-3
4.5	Fire Protection 4-3
4.6	Industrial Safety Requirements 4-3
4.7	Other Safety Requirements 4-3
4.8	Operational Safety Requirements..... 4-3
5.	APPLICABLE CODES, STANDARDS AND CLASSIFICATION 5-1
5.1	Classification and Quality Assurance Level 5-2
5.1.1	Classification 5-2
5.2	Quality Assurance 5-2
5.2.1	Hardware 5-2
5.2.2	Software 5-2
6.	ENVIRONMENTAL CONDITIONS 6-1
6.1	Normal Plant Operation 6-1
6.2	Abnormal Conditions 6-1
7.	OVERPRESSURE PROTECTION 7-1
8.	INSPECTION AND TESTING 8-1
8.1	Inspection 8-1
8.2	Testing 8-1
8.3	Commissioning..... 8-1

TABLE OF CONTENTS

SECTION	PAGE
9.	RELIABILITY AND MAINTAINABILITY 9-1
9.1	Reliability 9-1
9.2	Availability 9-1
9.3	Failure Detection 9-1
9.4	Redundancy Requirements 9-2
9.4.1	Redundancy for Shared Resources 9-2
9.4.2	Redundancy for Controllers 9-2
9.4.3	Redundancy for Seismic Trip System 9-2
9.5	Maintainability Requirements 9-2
10.	LAYOUT 10-1
11.	INTERFACING SYSTEMS 11-1
12.	DECONTAMINATION AND DECOMMISSIONING 12-1
13.	MATERIALS AND CHEMISTRY 13-1
14.	LOADS, LOAD COMBINATIONS AND SERVICE LIMITS 14-1
15.	HUMAN FACTORS AND OTHER DESIGN REQUIREMENTS AND CONSTRAINTS 15-1
15.1	Human Factors 15-1
15.2	Other Design Requirements 15-1
15.3	Constraints 15-1
15.3.1	Control System Configuration 15-1
15.3.1.1	FH DCS Hardware and Software 15-1
15.3.1.2	FH DCS Configuration 15-3
15.3.1.3	System Partitioning 15-3
16.	REFERENCE DOCUMENTS 16-1

TABLES

Table H-1	Human Factors Requirements (Operator and Maintainer Functions / Performance Requirements) H-1
Table H-2	Typical (Non-Mandatory) Human Factors Requirements (Operational and Maintenance Tasks) H-3

TABLE OF CONTENTS

SECTION	PAGE
FIGURES	
Figure 1 Functional Bubble Diagram for the ACR FCS	2-3
Figure 2 ACR FH Control and Operator Interface System	15-2
Figure 3 ACR FH DCS Configuration	15-4
 APPENDICES	
Appendix A Design Parameters.....	A-1
Appendix B Typical (Non-Mandatory) List of PID Loops	B-1
Appendix C Typical (Non-Mandatory) List of Motor Drives	C-1
Appendix D Typical (Non-Mandatory) List of I/O Signals.....	D-1
Appendix E Typical (Non-Mandatory) List of Interlocks.....	E-1
Appendix F Design Requirements	F-1
Appendix G List of Interfacing Systems	G-1
Appendix H Typical (Non Mandatory) Human Factors Requirements.....	H-1

1. INTRODUCTION

This document establishes the basis for the detailed design of the ACR™* Fuel Handling (FH) Control System. The main function of the FH Control System (FCS) is to control and monitor the major FH sub-systems. It monitors the state of the FH equipment and manipulates the equipment and process variables under the general supervision of the operator. Other than the exchange of data, the FCS shall be functionally independent from the rest of the Plant Control Systems (PCS) so its failure does not affect the PCS and vice versa.

The overall requirements of the FCS are covered in this document.

Since ACR uses the double-ended refuelling concept, separate sets of FH subsystems are proposed for each side of the reactor. It is proposed to provide physical and functional partitioning between the controllers handling separate sets of FH subsystems to the extent practicable.

The operator interface for monitoring and control of the FH System is provided by the FH Display System (FDS). The design requirements of the FDS will be covered by a separate document.

The FH instrumentation and the input and output signal conditioning are not included in the scope of this document.

This Design Requirements document includes a non-mandatory appendix (Appendix A – *Design Parameters*) that provides guidance on the application of the mandatory requirements. The values given are design parameters, not design requirements, and are for reference only.

The FCS is a subsystem of the FH System and is therefore subject to the general requirements of Reference 1.

1.1 Design Principles

The principles for the design of the FCS are that it will:

- a) Allow for a substantial reduction of control components (compared to CANDU 6) leading to improved reliability and reduced maintenance and construction costs.
- b) Reduce the different types of hardware and software platforms (e.g., by incorporating hardware/software which is used in other parts of the ACR plant) in the plant to the extent practicable to reduce the cost of inventory and maintenance.
- c) Use proven and commercially available hardware and software components to the extent practicable.
- d) Provide an increased level of automation and operability (e.g., with more automated sequences), building on the existing CANDU design features to free operating staff from tedious tasks, and thereby reduce the frequency and likelihood of operator error.
- e) Control the cost escalation of software development/maintenance by using high-level languages, and eliminating the need for specialist computer programming skills.

* ACR™ (Advanced CANDU Reactor™) is a trademark of Atomic Energy of Canada Limited (AECL).

- f) Based on the ACR design (refer to Reference [15]) the FH System shall utilize electric drives only. With this change the in-service performance will improve, the in-service period will be extended, and the maintenance required will be significantly reduced.

1.2 Acronyms

CANDU	CANadian Deuterium Uranium
CER	Control Equipment Room
CMRR	Common Mode Rejection Ratio
CNSC	Canadian Nuclear Safety Commission
CSA	Canadian Standards Association
DCC	Digital Control Computer
DCS	Distributed Control System
DBE	Design Basis Earthquake
EWS	Engineering Work Station
FH	Fuel Handling
FCS	Fuel Handling Control System
FDS	Fuel Handling Display System
FM	Fuelling Machine
HSI	Human-System Interface
HTS	Heat Transport System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
I/O	Input/Output
ISO	International Organization for Standardization
L-L	Line-to-Line
LVDT	Linear Variable Differential Transformer
MCR	Main Control Room
MTTR	Mean Time To Repair
NFT	New Fuel Transfer
PCS	Plant Control Systems
PDS	Plant Display System
PID	Proportional, Integral and Derivative
RAB	Reactor Auxiliary Building
RMS	Root Mean Square
RTD	Resistance Temperature Detector
SDG	Safety Design Guide
SFT	Spent Fuel Transfer
TBD	To Be Determined

TTL Transistor-Transistor Logic

VDU Video Display Unit

2. FUNCTIONAL REQUIREMENTS

2.1 Safety Functional Requirements

The FCS shall be designed so that any failure or spurious operation of the FCS does not lead to:

- LOCA caused by the Fuelling Machine (FM) damaging a reactor end fitting, or unclamping from a reactor end fitting while the closure is removed.
- Breach of the containment whether or not new or spent fuel is being transferred through the containment boundary.
- Loss of cooling to spent fuel bundles from the time they have been removed from the fuel channel until they are transferred into the spent fuel bay.

2.2 Operational Functional Requirements

The conceptual block diagram of the overall FH Control and Display System is shown in Figure 2 (refer to Section 15.3).

The overall FCS shall consist of three functional units:

- a) FH Distributed Control System (DCS)
- b) Protective Interlock System
- c) Seismic Trip System.

The functional requirements of these units are given in Sections 2.2.4, 2.2.5, and 2.2.6.

The functional requirements of the FCS are shown in Figure 1.

The FCS shall be designed to support the following normal, abnormal, upset and emergency operations (refer to Reference [1] for details).

2.2.1 Normal Operations

The FCS shall facilitate the following normal FH operations under automatic and/or operator control from the Main Control Room (MCR).

- a) Transfer new fuel into containment and load new fuel into the FM.
- b) Change fuel in the reactor at any stationary level of power.
- c) Unload spent fuel from the reactor and handle spent fuel up to, and including storage in the spent fuel storage bay.
- d) Rehearse all fuel changing and other on-reactor FM operations as required at the Rehearsal Facility.
- e) Replace defective fuel channel closure plugs and ram adaptors, and transfer them to an accessible area.
- f) Provide means of channel flow verification.
- g) Defuel and fuel a complete fuel channel with the reactor at power or in a shutdown state.

2.2.2 Abnormal Operations

The FCS shall facilitate the following abnormal FH operations under automatic and/or operator control from the MCR.

- a) Drain the light water from a fuel channel.
- b) Replace a faulty shield plug in a fuel channel, and using special tooling transfer the shield plug to the spent fuel storage bay.
- c) Refuel an empty fuel channel.

2.2.3 Upset and Emergency Operations

The FCS shall provide suitable monitoring and facilitate the following upset and emergency operations (under automatic and/or operator control from the MCR) without jeopardising the containment boundary or Heat Transport System pressure boundary.

- a) Release/recover stuck mechanisms.
- b) Stop unintentional operation of mechanisms.
- c) Initiate emergency cooling of fuel in the FM or Spent Fuel Port.
- d) Isolate water supply or return lines in the event of leakage or rupture.
- e) Minimise the possibility of inadvertent operation of mechanisms.

2.2.4 FH DCS

The FH DCS shall be the primary system that monitors and controls all FH operations during normal, abnormal and certain upset and emergency conditions.

The FH DCS shall perform the following types of control functions:

- a) Sequential Control
- b) Logic Control
- c) PID (Proportional, Integral and Derivative) Control
- d) Motion Control

Two levels of sequential controls are required: Supervisory Sequential Controls and Mechanism Sequence Controls (refer to Section 2.2.4.1).

In addition, some computational and monitoring capability is required. The requirements for each of these functions are discussed in the following sections.

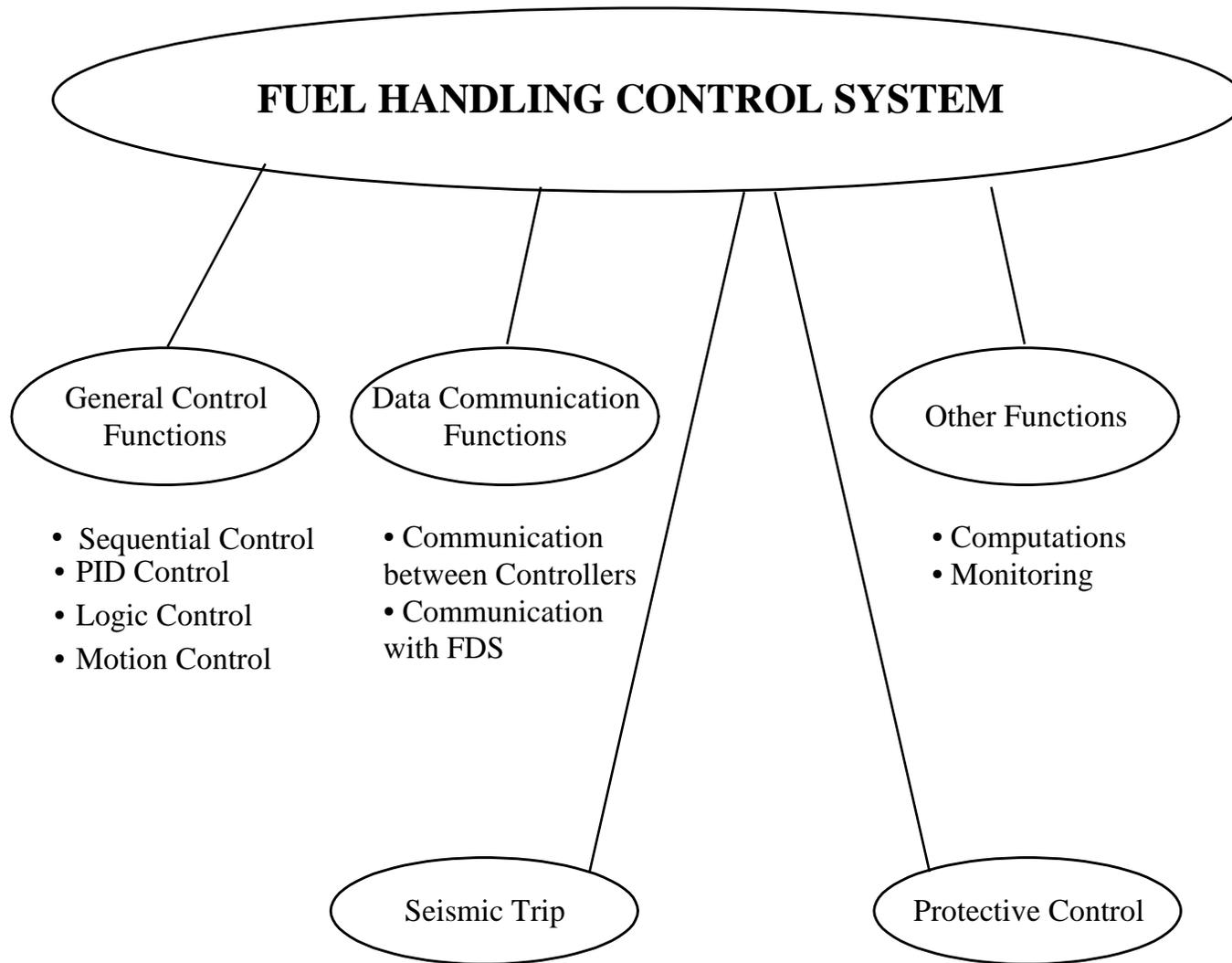


Figure 1 Functional Bubble Diagram for the ACR FCS

2.2.4.1 Sequential Control

FH system operations are sequential in nature. Two levels of sequential controls are required:

- a) Supervisory Sequential Control
- b) Mechanism Sequential Control

Requirements for these two levels of sequential control are specified in the following four subsections.

2.2.4.1.1 Structure of the Supervisory Sequential Control System

Supervisory sequential control manages all FH operations (as described in Sections 2.2.1, 2.2.2, and 2.2.3). This control function shall provide a hierarchical structure of Steps, Sequences and Jobs as given below:

- a) Step: A set of operations comprising a number of commands and feedbacks.
A feedback is either a database point, digital input, analogue input value or a position status of a mechanism from a motion control loop.
A command is either a digital output change or a new position required for a mechanism to be passed on to a motion control loop.
- b) Sequence: A set of steps.
- c) Job: A set of sequences.

Refer to Section 2 of Appendix A for more information.

It shall be possible to associate sets of data to some sequences (similar to recipes used in batch control), to avoid having a number of separate sequences that are similar except for changes in some data (e.g., setpoints etc.).

2.2.4.1.2 Modes of Supervisory Sequential Control

It shall be possible to execute supervisory sequential control in the following modes:

- a) Auto-Step: Following a start command by the operator, the selected job or sequence is executed without further operator intervention (unless an error condition arises or a feedback is not available or a “hold” is deliberately introduced to facilitate an operator permissive).
- b) Single-Step: Same as Automatic mode, except that operator intervention is required to proceed to the next sequence/step.
- c) Single-Operation: The sequential controller stays at the same step and the operator selects any individual commands from within the step of the sequence.
- d) Manual: The operator manually selects and executes the required command.

2.2.4.1.3 Operator Intervention During Supervisory Sequential Control

The FH DCS shall permit the operator to initiate and execute sequential control in a flexible manner, as warranted by the status of the FH system. The following facilities shall be provided:

- a) Start job/sequence (from the beginning or from an intermediate sequence/step)
- b) Pause job/sequence

- c) Resume job/sequence
- d) Abort sequence/job
- e) Change mode
- f) Skip steps
- g) Skip feedbacks
- h) Provide messages to the operator during critical operations and accept operator input data/commands.

Full details of the supervisory sequential control requirements will be provided in a separate design requirements document.

2.2.4.1.4 Mechanism Sequential Control

The mechanism sequential control function controls and manipulates individual mechanisms. The control involves both sequential operations and logic operations. Mechanism sequential control shall be executed in the individual subsystem controllers and involve commanding and monitoring of various FH mechanisms by direct manipulation of control elements and indirect control of mechanisms through motion controllers. It address situations where controlling an individual mechanism must be accomplished in an ordered manner (e.g. ram positioning. This is similar to the CANDU 6 loop control).

- a) The mechanism sequence control shall be executed in the individual subsystem controllers.
- b) The mechanism sequence control shall be a subset of supervisory control functions with the following limitations:
 - Job functionality is not required.
 - Skip step and Skip feedback functions are not required.

2.2.4.2 Logic Control

- a) The FH DCS shall be capable of logic control for the implementation of operational interlocks and device control (for mechanical devices, including pumps, valves, etc.).
- b) It shall be possible to start/stop/open/close the devices both in automatic and manual modes.
- c) All logic control functions and Boolean operations defined by IEC 61131-3 shall be supported.

2.2.4.3 PID Control

- a) The FH DCS shall be capable of performing PID control to control process parameters. Typical process loops are listed in Appendix B.
- b) Both Automatic and Manual control modes are required.
- c) The requirements of bumpless transfer for any specific loop shall be pre-definable for mode change from automatic to manual and vice-versa.
- d) The PID parameters shall be tuneable from the EWS.
- e) Each subsystem controller shall be capable of executing multiple PID loops simultaneously.

2.2.4.4 Motion Control

The FH DCS shall have the capability to perform motion control for the drives listed in Appendix C. The following types of motors will be used in the ACR FH system:

- a) Brushless DC motors
- b) AC motors (single or double speed)

2.2.4.4.1 Brushless DC Drive Motion Control

Most of the FH mechanisms are driven by brushless DC motors.

- a) The motion control system shall provide sinusoidal commutation for these motors in addition to performing the motion control. The power amplifiers and power supply to these motors shall be part of the motion control system package.
- b) The capability for closed loop servo motion control shall be provided to achieve accurate positioning of various mechanisms. The motion control system shall accept feedback signals from resolvers (both incremental and absolute types) and LVDTs.
- c) For point-to-point moves, the motion control loops shall follow a predefined motion profile with controlled speed, acceleration, torque and bump. The velocity profile shall facilitate smooth operation of the drive.
- d) The motion control system shall permit the motion to take place either in current mode or velocity mode, depending on the operational requirements. During certain operations, it shall be possible to switch between these two modes automatically. The required mode (i.e., current or velocity) shall be selectable by the operator during manual operations (independent of the motion controller) in certain situations (e.g., a mechanism is stuck).
- e) The motion control system shall be able to perform backlash compensation based on dual position feedback.
- f) During normal operations, the torque/force shall be maintained within the predefined limits for each drive. The motion control system shall be capable of exerting more torque than is normally required (selectable by the operator) to release a stuck mechanism or during abnormal operations.
- g) The capability shall be provided to move some mechanisms to stall with controlled torque.
- h) Simple on/off type motion control shall be provided for some mechanisms with electric drives.
- i) The motion control system shall communicate with the subsystem controller for exchanging command and feedback data.
- j) The motion control system shall monitor the motor's parameters and abort the motion if a fault condition is detected. The fault condition data shall be sent to the FDS or Engineering Work Station (EWS, refer to Section 2.2.4.10) as appropriate for annunciation.
- k) The motion control system shall fail safe during a Design Basis Earthquake based on a signal from a Seismic Trip System.
- l) The motion control system shall permit coordinated movements (synchronized) between multiple drives.

2.2.4.4.2 AC Drive Motion Control

The following capabilities of AC drive motion control shall be provided for AC motors:

- a) Start/stop/direction control
- b) Variable or fixed speed control

2.2.4.4.3 Modes of Motion Control

It shall be possible to perform motion control for electric drives in the following modes:

- a) Automatic: Upon receiving the position command from the sequential control system, the mechanism shall be moved to the selected position without operator intervention.
- b) Semi-automatic: Upon receiving the position command from the operator, the mechanism shall be moved to a selected pre-defined position without further operator intervention. Both incremental and absolute motions shall be possible in semi-automatic mode. In incremental motion mode, the operator shall be able to set the distance to be travelled relative to the current position. In absolute motion mode, the operator shall be able to enter an absolute setpoint and command the mechanism to move to that setpoint.
- c) Manual: In this mode, the operator shall be able to manually jog the mechanism (manually moving the mechanism either in small increments or in continuous motion) in either the forward or reverse direction and stop at any point. It shall be possible to perform the manual operations from the FH operators console and selected number of operations from the Backup Control Panel (refer to Section 2.2.4.12) that bypasses the FH DCS.

It shall be possible to set limits on the force/torque, speed, acceleration and bump/jerk in all of these modes as required.

Rationale: Jogging function is required to facilitate manual movement of a mechanism during non-routine/abnormal operations (e.g., move a stuck mechanism by gently nudging it or manually move a mechanism to a specific position). During this manual operation, the operator directly manipulates the control command signal to the motor bypassing the closed-loop motion control.

2.2.4.4.4 Operator Intervention During Motion Control

During normal operations in automatic mode, the sequential control system provides all the required motion commands to the motion controllers through the subsystem controller. The system shall enable the operator to initiate and execute motion control in a flexible manner as warranted by the specific FH system status in semi-automatic and manual modes. The following facilities shall be provided:

- a) Select/enter setpoints
- b) Start motion in semi-auto mode
- c) Jog/stop mechanisms in forward/reverse directions in manual mode
- d) Abort motion
- e) Change mode
- f) Change force/torque

- g) Change speed

2.2.4.5 Computational Functions

Numerical and logical computations shall be provided for achieving overall monitoring and control. These include the following:

- a) Engineering Unit Conversions
- b) Bit and byte manipulations
- c) Maintaining calibration setpoint tables
- d) Indexed selection of setpoints (lookup tables)
- e) Boolean logic
- f) Arithmetic
- g) Square root
- h) Automatic scaling
- i) Linearization
- j) Signal selection logic for duplicated signals
- k) Signal comparisons
- l) Floating point calculations
- m) Maintaining multiple timers with up and down counting.

For more information on computational functions refer to Section 2 of Appendix A.

2.2.4.6 Control Execution

- a) It shall be possible to execute the control programs only when required.

Rationale: Because FH operations are predominantly sequential; it is not required to execute certain control and computational functions continuously. It is safer to keep those control programs dormant until those specific control functions are required.

- b) Redundancy is provided for some of the FH devices and instrumentation. The system shall facilitate operator selection of the active devices/instruments and use the data from these devices for monitoring and control functions. Signals from standby devices/instruments shall be available for checking and confirmation purpose by the operators.
- c) The system shall allow changing of position/force setpoints (with appropriate authorization) whenever the FH mechanisms are re-calibrated.
- d) The system shall be able to handle multiple setpoints for each motion control loop (e.g., the same algorithm shall be executed with a different setpoint from a setpoint table each time a different position is required).

Rationale: Each of the fuel handling mechanisms has a number of predefined position setpoints (e.g., X-drive has a number of setpoints each corresponding to a column of fuel channels. Each time, the FM Carriage has to travel to a different fuel channel, which requires a different position setpoint. Once the FH operator selects the required channel, the control system is required to automatically select the required position setpoint).

- e) The system shall have the capability to compute and store data, and use this data at a later time to perform monitoring and control functions (e.g., once the mechanism is positioned, the current position/computed position error needs to be stored to detect slippage of the mechanisms).

2.2.4.7 Monitoring Functions

- a) In addition to conventional monitoring functions, the system shall be able to monitor against non-fixed/variable and dynamically selected/generated setpoints for some parameters.
Rationale: Each FH mechanism has several position and force/torque setpoints. These position/torque setpoints are selected depending on specific operational requirements. The alarm limits for the position/torque setpoints change as the setpoints themselves change in the course of mechanism movement. So the system shall be able to change the alarm limits dynamically as the position/torque setpoints change. In some cases, when the mechanism stops, the system is required to dynamically generate and monitor the alarm limits depending on the stopping point (required for slippage monitoring).
- b) It shall be possible to automatically enable and disable monitoring based on the current operational conditions/equipment status. When monitoring is disabled for a piece of equipment, no alarms shall be generated when the equipment is taken out of service for maintenance purposes. The control system shall have adjustable deadband zone, noise filters and “hold-in” times.
- c) In certain cases, if abnormal conditions are detected, it shall be possible to initiate automatic corrective action and provide data to the FDS for annunciation.
- d) All the annunciation data shall be made available to the FDS and the EWS. In addition, the operational status/health of the FH DCS shall be annunciated locally in each FH DCS station.
- e) All alarms shall be time stamped.
- f) The FH DCS shall monitor the following:
- Operational parameters of the FH System
 - Operational status of the FCS
 - Field signal integrity at the I/O system
 - Internal power supply parameters

2.2.4.8 I/O System

- a) The FCS shall have the capability to handle the quantity and types of inputs and outputs listed in Appendix D.
- b) In case there is a failure of the I/O module, the failure shall be annunciated locally on the module and the error code shall be sent to the EWS for fault identification and troubleshooting. Necessary information shall also be sent to the FDS for annunciation of the failure at the FH Console.
- c) The system shall be capable of providing I/O loop power from an internal source and accepting external I/O loop power source, as required. It shall be possible to time stamp the selected analogue and digital inputs.

For more information on I/O System refer to Section 2 of Appendix A.

2.2.4.9 Communication System

- a) An efficient communication system shall be provided within the FH DCS so that the commands from the operator or the sequential controller shall reach the motion controllers and/or the output modules complete and error free, and in a timely manner. Similarly the process data, mechanism operational data and feedback data shall be sent to the sequential controllers and the FDS complete and error free, and in a timely manner. The communication system shall meet the data transfer requirements specified in the performance requirement section (refer to Section 1).
- b) The communication system shall enable data exchanges between various subsystem controllers within each partition and between the sequential controllers of both partitions.
- c) The communication system shall enable data exchange between the EWS and all subsystems of both partitions.
- d) The communication system shall have built-in error checks. In addition, further communication error checking (e.g., when there is no reply for a data request) shall be implemented through other modules where possible. Communication errors and failures of communication modules shall be annunciated through the FDS/EWS as well as locally on the module.
- e) The communication system shall have redundant communication links and redundant processing modules.

2.2.4.10 Interface between the FH DCS and the EWS

The FH DCS maintenance functions, such as system configuration and programming tools, shall be provided through the interface between the FH DCS and the EWS, which shall permit the following:

- a) Display and recording of all I/O and communication data.
- b) Annunciation of system and I/O module faults.
- c) Calibration of FH mechanisms and creation of setpoint tables for each mechanism, and downloading of calibrated position/torque setpoint tables to various subsystem controllers and/or motion controllers.
- d) Configuration of all hardware modules, definition of inputs and outputs, configuration of the communication system and database/system variables etc.
- e) On-line and off-line program de-bugging and troubleshooting.
- f) Troubleshooting of system faults.
- g) Signal simulation.
- h) Tuning of control loops in the FH subsystem processors.
- i) Communication between all the controllers in the FH DCS and the EWS.

2.2.4.11 Interface between the FH DCS and the FDS

The interface between the FH DCS and the FDS shall be designed to ensure that the minimum performance and system response requirements are met at the FH Control Console. As a minimum, the following types of data are required to be exchanged between the control and display systems:

- a) Analogue and digital I/O signal data
- b) Analogue and digital calculated variables
- c) Control setpoints
- d) Control commands
- e) Control modes
- f) Mechanism calibration data
- g) System status and diagnostic information

2.2.4.12 Interface between the FH DCS and the Backup Control Panel

An interface shall be provided between the FH DCS and the Backup Control Panel to achieve the following functions:

- a) Annunciation of FCS faults for which the signals are available on the Backup Control Panel.
- b) Monitoring of the position of the Panel/Computer mode switches by the FH DCS (The Panel/Computer mode switches shall be mounted on the backup panel and shall be provided only for the safety related equipment for which manual control is available from the this panel).

2.2.5 Protective Interlock System

- a) The capability for Interlock/Protective control shall be provided to:
 - Minimise damage to the FH equipment and fuel bundles due to inadvertent operation.
 - Minimise the possibility of damage to safety related systems such as HTS and Containment which interface with the FH System.
- b) The protective interlock system shall be designed as per the IEC 61497 standard for nuclear safety interlocks (as applicable to a safety related system).
- c) The protective control function shall be immune to control system software failures. All the commands from the FH DCS with safety related functionality shall be checked by the protective interlock system and shall be sent to the field only if the safety conditions are met. The manual control commands from the Backup Control Panel shall also be routed through the Protective Interlock System.
- d) The interlocks shall be designed in such a way that they can be bypassed in a safe manner with appropriate authorization.

A tentative list of interlocks is provided in Appendix E.

2.2.6 Seismic Trip System

The primary purpose of this system is to protect against spurious operation of the FH system arising from DBE. It also serves to monitor low-level seismic activity below the severity of a DBE.

- a) During a DBE, the FCS shall ensure that no spurious control operation will take place resulting in potential damage to the HTS pressure boundary or containment. A Seismic Trip System shall be provided which will:
 - Continuously monitor the acceleration of the base slab of the reactor building to detect the onset of an earthquake.
 - Interrupt power to predefined drives (to be determined during detailed engineering) after detecting the onset of an earthquake, so that they fail safe before the intensity of the earthquake reaches a level that could damage the drives or cause them to malfunction.
- b) The Seismic Trip System shall be physically and functionally independent of the rest of the FCS. The outputs from the Seismic Trip equipment shall be directly connected to the circuit breaker circuitry and the breakers shall be seismically qualified to the extent that they will not re-energize under the influence of a DBE.
- c) The Seismic Trip System shall be immune to spurious trips (which could be caused by rotating equipment, vehicles, or blasts).
- d) The latching and resetting of the Seismic Trip System shall be immune to spurious operations during seismic activities.
- e) The Seismic Trip System shall be provided with a facility to record the seismic activity.
- f) The Seismic Trip System shall provide digital output signals, indicating its operating status/faults, to the FH DCS for monitoring.

3. PERFORMANCE REQUIREMENTS

The FCS shall be designed to enable the overall FH System to meet the performance requirements as defined in Reference [1].

It is expected that limitations on FH system performance and the speed of operation will generally be set by the operation of the mechanical equipment rather than by the speed of operation of the control system. However, the control system shall meet the following minimum requirements.

3.1 Sequence Control Execution Time

The time between execution of two consecutive steps in a sequence (i.e., the time between the finish of the current step and the start of the next step) shall satisfy the following conditions:

- a) The time between the execution of two consecutive steps in a sequence shall be short enough to accommodate the fuelling cycle time requirements (Reference [13]).
- b) The time between two consecutive steps in a sequence shall be long enough for the operator to be able to follow the sequence.

For the suitable time refer to Section 3 of Appendix A.

Note: The time required for completing the execution of commands by the subsystem controller or the motion controller is not considered, as that time depends on the control action to be performed.

3.2 Data Transfer between Sequential Controller and Subsystem/Motion Control Processors

- a) The feedback data from the subsystem controllers and motion controllers shall reach the sequential controllers within a time frame that satisfies the two conditions identified in Section 3.1. This time shall include the following:
 - Time to detect the feedback by the subsystem/motion control processors (i.e., controller cycle time etc.).
 - Time to transmit the feedback data from the subsystem/motion control processor through the communication network to the communication interface of the sequential controller.
 - Time to receive the feedback data by the sequential control processor from its communication interface.

For the suitable time frame refer to Section 3 of Appendix A.

- b) The commands from the sequential controllers shall reach the subsystem controllers and motion controllers within a time frame that satisfies the two conditions identified in Section 3.1. This time shall include the following:
 - Time to transfer the command data by the sequential control processor to its communication interface.
 - Time to transfer the command data through the communication network to the subsystem/motion control processor.

- Time to detect the command by the subsystem/motion control processors (i.e., controller cycle time etc.)

For the suitable time frame refer to Section 3 of Appendix A.

3.3 Motion Control Loop Update Time for Brushless DC Drives

The update time for each electric drive motion control loop (for a single axis) shall satisfy the two conditions identified in Section 3.1. It shall include the following:

- a) Reading of position data.
- b) Execution of servo control algorithm.
- c) Updating the output signal.

For the suitable update time refer to Section 3 of Appendix A.

Rationale: During motion control operations, the position, speed, acceleration, torque, and bump/jerk of the motor are required to be controlled. Some of the motors may have speeds exceeding 3000 rpm and the mechanisms have to be accurately positioned at the setpoint within the tolerances. Position adjustments are not permitted.

3.4 Motion Control Loop Update Time for AC Drives

The update time for the control loops of AC motor drives shall satisfy the two conditions from Section 3.1. It shall include the following:

- a) Control program cycle time.
- b) Contact debouncing or reading of position data.
- c) Input signal scan time at the input module.
- d) Data transmission from the input module to the control processor.
- e) Data transmission from the control processor to the output module.
- f) Generation of the output signal by the output module.

For the suitable update time refer to Section 3 of Appendix A.

Rationale: FH mechanisms need to be monitored and control action taken as soon as an event is detected. Failure to take the control action within the time frame that satisfies those conditions in Section 3.1 will result in potential damage to the mechanisms.

Note: The AC control loops include both sequential and logic control functions.

3.5 PID Control Loop Update Time

PID control loops shall be updated at intervals that satisfy the two conditions identified in Section 3.1.

For the suitable time intervals refer to Section 3 of Appendix A.

3.6 Position Data Transfer from FH DCS to FDS Interface

Position data of the mechanisms shall be updated and transferred to the FDS within a time frame that satisfies the two conditions identified in Section 3.1. It shall allow the operator to manually

jog and position the mechanisms using the VDU and data input devices of the FDS. In determining the communication speed and the frequency of data transfer, the following shall be considered where appropriate:

- a) Contact debouncing or reading and processing of position data.
- b) Input signal scan time at the input module.
- c) Time for data transmission from the input module to the control processor.
- d) Time to detect/compute the position status by the subsystem/motion control processors (i.e., controller cycle time etc.).
- e) Time to transmit the position status data from the subsystem/motion control processor through the communication network to the communication interface of the FDS interface.

For a suitable position data update time refer to Section 3 of Appendix A.

Rationale: In CANDU 6 plants, a full-fledged hardwired FH Control Panel was provided. The FH operators could perform manual jogging/positioning of the mechanisms from this panel. The FH Backup Control Panel in ACR plants will provide backup for safety related functions only. Therefore, it is necessary to provide functionality for manual jogging and positioning of the other mechanisms from the FH Operator's Console using the VDU and data input devices of the FDS.

3.7 Transfer Time for Commands from FDS Interface to FH DCS

The FH DCS shall be able to transfer the operator commands received from FDS interface to the controllers and I/O within a time frame that satisfies the two conditions identified in Section 3.1. In determining the communication speed and the frequency of data transfer, the following shall be considered where appropriate:

- a) Time to transfer the command data from the FDS interface through the communication network to the communication interface of the subsystem/motion control processor.
- b) Time to detect the command by the subsystem/motion control processor (i.e., controller cycle time etc.).
- c) Time for data transmission from the control processor to the output module.
- d) Generation of the output signal by the output module.
- e) Time for output signal conditioning (e.g., interposing relays etc.).

For a suitable command transfer time refer to Section 3 of Appendix A.

Rationale: Same as Section 3.6

3.8 Data Transfer from FH DCS to FDS Interface (Excluding Position Data)

- a) During the execution of a sequence in automatic mode, the FH DCS shall be able to update and transfer the data required for sequence monitoring and alarm monitoring by the FDS at least once within a time frame that satisfies the two conditions identified in Section 3.1. This time shall include the following:
 - Contact debouncing or reading and processing of position data.
 - Input signal scan time at the input module.

- Time for data transmission from the input module to the control processor.
- Time to compute the data by the subsystem/motion control processors, if necessary.
- Time to transmit the data from the subsystem/motion control processor through the communication network to the communication interface of the sequential controller/FDS.
- Time to receive the data by the FDS interface.

For a suitable transfer time of data required for sequence and alarm monitoring by the FDS refer to Section 3 of Appendix A.

- b) The rest of the system data (for inactive mechanisms and process parameters) shall be transferred to the FDS in a time interval that will satisfies the two conditions identified in Section 3.1.

For a suitable data transfer time refer to Section 3 of Appendix A.

3.9 Analogue Input Conversion

Suitable analogue input conversion accuracies are listed in Section 3 of Appendix A.

3.10 Seismic Sensing Range

The Seismic Trip System (Section 2.2.6) shall be able to monitor the ground acceleration in the range that encompasses the ACR DBE level (Reference [3]). Furthermore, it shall be able to record low-level seismic activity.

It shall be able detect and distinguish between the non-damaging Primary Wave (P-Wave) and the damaging Secondary Wave (S-Wave).

For numerical requirements refer to Section 3 of Appendix A and Appendix F.

3.11 Seismic Sensing Accuracy

The sensing accuracy and response time of the Seismic Trip System (Section 2.2.6) shall be adequate to enable tripping of circuit-breakers and putting the FH system in a safe state upon detection of the non-damaging Primary Wave (P-Wave), and before the arrival of the damaging Secondary wave (S-Wave).

For a suitable sensing accuracy and response time refer to Section 3 of Appendix A.

4. SAFETY REQUIREMENTS

4.1 Applicable Requirements from Safety Design Guides

The FH System is a safety related system and therefore the FCS shall be designed to meet the relevant safety requirements as per the applicable safety design guides. Compliance with Safety Design Guides (SDG) is mandatory.

4.1.1 108-03650-SDG-001, Safety Related Systems

As identified in SDG-001, the Safety Design Guide for Safety Related Systems (Reference [2]) the FH System is a safety related system. Therefore the FCS controls several safety related operations.

Reference [2] does not treat the FCS as a separate system, but indicates that the general safety requirements of the FH system are applicable to the FCS. Most of the requirements stated in the above design guide are applicable to the mechanical structures of the FH system. The requirements that are specifically applicable to the FCS are identified in the following sections.

4.1.2 108-03650-SDG-002, Seismic Requirements

As per Reference [3], there are no specific seismic qualification requirements for the overall FCS. However, as part of the overall FH system, the FCS shall satisfy the requirement that failure of non-qualified controls shall not compromise the safety related functionality of the FH system. Refer to Section 2.2.6 for the requirements of the Seismic Trip System to achieve this objective.

The Seismic Trip System shall be seismically qualified as a category B component per Reference [3].

Note: The FH Backup Control System (including Backup Control Panel) is not part of the FCS and its design requirements are identified in the Design Requirements document for the Fuel Handling Display System (FDS).

4.1.3 108-03650-SDG-003, Environmental Qualification

The FCS (excluding the Seismic Trip System) shall be located in a controlled environment in the Control Equipment Room (CER). The environment of the CER is classified as mild (Reference [4]). The Seismic Trip System shall be located in the Reactor Auxiliary Building (RAB) which is, also, subject to a mild environment (Reference [4]).

During and following a Design Basis Accident (DBA), the Seismic Trip System and the FM Emergency Water System shall remain functional. Furthermore, the containment boundary shall be maintained, the FM shall not unclamp from a fuel channel if the channel closure is removed, and the FM and its support equipment shall not damage an end fitting. Therefore, the fuel handling controls for the above safety related functions shall be environmentally qualified.

4.1.4 108-06350-SDG-004, Separation of Systems and Components

The FCS is not a safety system and does not require duplicated or triplicated components to meet any safety requirements. Therefore, the separation requirements as per Reference [5] are not applicable to the FCS.

The FCS shall be provided with limited redundancy where required for operational/economic reasons only.

Note: The FH Backup Control System (including Backup Control Panel) is not part of the FCS and its design requirements are identified in the Design Requirements document for the Fuel Handling Display System (FDS).

4.1.5 108-03650-SDG-005, Fire Protection

The design of the FCS shall meet the relevant requirements specified in Reference [6] as follows:

- a) The cables shall be routed as far away as practical from equipment identified as having a fire hazard.
- b) Only cables that meet the flame spread rating and do not exceed the allowable corrosive gas releases shall be used.
- c) Protection against localised fires shall be provided in areas of significant fire hazard.
- d) Non-combustible materials for systems and components shall be specified as far as practical.
- e) The design shall minimise the spread of fire from one equipment cabinet to another.
- f) Provision shall be made for “quick-open” doors on equipment cabinets to minimise the time required to extinguish a fire inside a cabinet.

4.1.6 108-03650-SDG-006, Containment

The FCS does not form part of any containment extension. However, the SFT System and the NFT System have containment extensions. Both of these systems are controlled by the FCS. Therefore, the FCS shall be designed so that any failure or spurious operation of the FCS does not lead to a breach of the containment boundary. Refer to Reference [7].

4.1.7 108-03650-SDG-007, Radiation Protection

The FCS shall be located in an area of negligible radiation levels. Therefore the maintenance staff of the FCS will not be exposed to any significant radiation.

To minimize radiation exposure (Reference [8]) for FH maintenance personnel, the FCS shall be designed to minimize the possibility of the FM getting stranded in the reactor vault and requiring manual recovery due to any hardware or software failures.

4.2 Specific Requirements from Applicable Canadian Nuclear Safety Commission (CNSC) Regulatory Documents

There are no specific Canadian Nuclear Safety Commission requirements in effect at this time. The general CNSC requirements for Quality Assurance, Safety, Reliability and Maintainability are addressed in the relevant sections of this document.

4.3 Protection Against Environmental Hazards

Refer to Section 1.

The Seismic Trip System shall withstand the ACR DBE conditions (Refer to Appendix F). It shall be seismically qualified as a category B component as per Reference [3].

4.4 Protection Against Impact Forces

Not applicable to the FCS.

4.5 Fire Protection

See Section 4.1.5.

4.6 Industrial Safety Requirements

Not applicable to the FCS.

4.7 Other Safety Requirements

Not applicable to the FCS.

4.8 Operational Safety Requirements

- a) The FH DCS shall be designed and shall be capable of being configured such that specific critical functions shall have a demonstrated unsafe failure rate as outlined in CNSC Consultative Document C-006. (For more details refer to Appendix F). Both the FH DCS hardware and software shall be designed to meet this target. Refer to Reference [11] for the software categorization of the FH DCS to meet the safety objectives of the overall FH system. The following safety design requirements shall be implemented.
- b) In situations where asynchronous or inadvertent operation of the equipment will compromise nuclear safety or have a significant economic impact, interlocks are required to minimize risk. Note that the “interlock” can be an electrical circuit or a piece of mechanical hardware.
- c) In case of any system faults, the outputs of the FH DCS, the Protective Interlock System and the Seismic Trip System shall fail to a safe state/value (to be determined during detailed engineering for each control loop).
- d) The FCS shall also be designed to minimize spurious operations of the FH mechanisms, especially those that could compromise nuclear safety, such as breaching the containment boundary, unclamping the FM from a fuel channel if the channel closure is removed, or damaging an end fitting.

5. APPLICABLE CODES, STANDARDS AND CLASSIFICATION

The following are the applicable codes and standards:

- a) CSA N286.1 Procurement Quality Assurance for Nuclear Power Plants
- b) CSA N286.2 Design Quality Assurance for Nuclear Power Plants
- c) CSA N286.3 Construction and Installation Quality Assurance for Nuclear Power Plants
- d) CSA N286.4 Commissioning Quality Assurance for Nuclear Power Plants
- e) CSA Q396 1.1 Quality Assurance Program for the Development of Software Used in Critical Applications
- f) CSA Q396 1.2 Quality Assurance Program for Previously Developed Software Used in Critical Applications
- g) CSA N289.5 Seismic Instrumentation Requirements for CANDU Nuclear Power Plants
- h) IEC 61131-3 Programmable Controllers - Part 3: Programming Languages
- i) IEC 61000-4-2 Electrostatic Discharge Immunity test –(Level A4, air discharge, 15 V)
- j) IEC 61000-4-3 Radiated, Radio-frequency, Electromagnetic Field Immunity Test - (Class 3 severe radiated electromagnetic field)
- k) IEC 61000-4-4 Electrical Fast Transient/Burst Immunity test – (Level 3, typical industrial electrical fast transient environment)
- l) IEC 61000-4-5 Surge Immunity Test – (Class 4, surge environment featuring poor separation between surge sources and electronic equipment)
- m) IEC 61000-4-6 Immunity to Conducted Continuous Disturbances – (Class 3, severe electromagnetic radiation environment)
- n) IEC 61497 Nuclear Power Plants - Electrical Interlocks for Functions Important to Safety – Recommendations for Design and Implementation
- o) IEEE C62.41 Recommended Practice for Surge Voltages in Low-Voltage AC Power Circuits
- p) IEEE C62.45 Guide on Surge Testing for Equipment Connected to Low-Voltage AC Power Circuits
- q) ISO 9000-3¹ Guidelines for the Application of ISO 9001 to the Development, Supply and Maintenance of Computer Software
- r) ISO 9001¹ Quality Management Systems - Requirements Third Edition
- s) ISO 9002¹ Quality Systems - Model for Quality Assurance in Production, Installation and Servicing Second Edition
- t) CNSC C-006 (REV. 1) (E) Draft Regulatory Guide: Safety Analysis of CANDU Nuclear Power Plants

Code requirements will be updated when the project code effective date is decided.

¹ The manufacturing QA Standard (Z299.0 or Equivalent ISO 9000 shall be established and documented in the Technical Specification and/or EQR).

5.1 Classification and Quality Assurance Level

5.1.1 Classification

Not applicable to FCS.

5.2 Quality Assurance

The overall FCS shall meet the Project Quality Assurance Plan (Reference [9]).

For Quality Assurance level, see footnote on Page 5-1.

5.2.1 Hardware

Standard, pre-produced system components shall be manufactured in accordance with Quality Program Category 3 (ISO 9002). Design, manufacture and testing of custom components, assembly, wiring and testing of the complete system, shall be performed in accordance with Quality Program Category 2 (ISO 9001).

In cases where the manufacturer cannot demonstrate meeting the above quality assurance requirements, the hardware components shall be tested by AECL or by an independent testing agency to verify that those components meet the specified quality assurance requirements.

5.2.2 Software

The level of software quality assurance required shall be determined based on the category of the FH control software as determined in Reference [11]. The software development shall be carried out as per the Quality Program Plan for FCS software.

6. ENVIRONMENTAL CONDITIONS

6.1 Normal Plant Operation

The FCS (except for the Seismic Trip System) shall be located in the CER, where the temperature is controlled within a range specified in Section 6 of Appendix A. However, to provide immunity to failures in the building temperature control system, the FCS shall be designed to meet the functional and performance requirements in the environment identified in Section 6 of Appendix A.

The Seismic Trip System shall be located in the RAB and shall be designed to meet the functional and performance requirements in the same environment as the above (see Section 6 of Appendix A). Refer to Section 4.3.

The FCS shall be designed to be unaffected by the electromagnetic environment (with cabinet doors open) likely to be experienced in the plant, including walkie-talkie transmitters, cellular telephones or other personal communication devices. The electrostatic discharge testing and radiated electromagnetic susceptibility testing shall be performed as per the IEC 61000 standards (refer to Section 1).

6.2 Abnormal Conditions

Because the FCS will be located in the CER, it will not be directly affected by environmental conditions resulting from Class 1 and Class 2 events as indicated in the Licensing Basis Document (Reference [10]). In the event of a power failure (Class 1 event), the FH system shall fail safe and the FH operations shall be suspended. The FCS is not required to be operational during Class 3, 4 or 5 events. The FCS is not required to provide safety or mitigating functions, therefore no specific protection is required for the FCS against the environmental hazards resulting from abnormal conditions.

- a) The FCS shall be designed and located so that its functions are not affected by the following:
 - Failures in the building temperature control system (up to the temperature limits specified in Section 6 of Appendix A)
 - Steam leaks
 - Water leaks (spray)
- b) Electrical power disturbances (e.g., due to severe electrical power distribution upset or severe electrical storms) may cause transient data errors of very short duration (<20 ms). The FCS shall be designed and implemented so these transient data errors are detected and accommodated to have a negligible effect on the systems controlled by FCS.
- c) Suitable monitoring and annunciation shall be provided to sense high temperatures in the FCS cabinets to alert the maintenance staff.

Note: The FH Backup Control System (including Backup Control Panel) is not part of the FCS and its design requirements are identified in the Design Requirements document for the Fuel Handling Display System (FDS).

7. OVERPRESSURE PROTECTION

Not applicable to the FCS.

8. INSPECTION AND TESTING

Equipment inspection, testing and commissioning shall be carried out as specified by the equipment manufacturers.

8.1 Inspection

All FCS wiring/cabling terminations including grounding terminations shall be inspected periodically during normal operation.

8.2 Testing

- a) The application software shall be tested in accordance with the Quality Program Plan for FH Control System Software. Consideration shall be given to site and development feedback regarding flexibility and versatility of the application software.
- b) The FCS hardware and software shall be integrated and full integration testing shall be carried out at the individual controller level, at the subsystem control level and at the fully integrated system level with the FM, rehearsal facility, new and spent fuel ports before dispatching the system to site.
- c) After the system is in-service, it shall be possible to verify the operation of the following in an off-line mode:
 - Each individual interlock in the Protective Interlock System.
 - Seismic Trip operation.
- d) The Seismic Trip System shall facilitate testing of the system in an off-line mode by the application of an appropriate signal source to test points.

8.3 Commissioning

The FCS shall be designed to facilitate commissioning. Adequate test points/terminals shall be provided for testing and calibration during commissioning.

9. RELIABILITY AND MAINTAINABILITY

9.1 Reliability

a) The FH DCS shall be designed and shall be configurable such that no global failure (any loss greater than 1 station (a control rack that may contain I/O modules and processors) or a communication failure between stations) shall:

- Compromise its and any interfacing system's safety related function
- Prevent meeting the lifetime target capacity factor

b) The FH DCS shall be designed and configurable such that any local failures (a station or important single I/O module and processors) shall be repairable within the time specified in Appendix F (this time shall include the time required for detection, diagnosis and repair).

Rationale: Even though these failures may not cause reactor de-rating or shutdown, the failures can lead to the inability to fuel and possible de-rating of the reactor. It is essential to limit them to avoid:

- *lag in fuelling schedule*
- *loss of reactivity*
- *increased maintenance costs*
- *consequential damages to the FH equipment as a result of FH DCS failures*
- *loss of confidence in the system*
- *probability of an eventual catastrophic failure of the FH DCS.*

9.2 Availability

The availability of the FCS must support the overall plant availability target (refer to Appendix F). The FCS is not required to operate continuously to meet this requirement as the plant can be operated continuously for up to seven days without de-rating even if the FH system is not available. See "Reliability" section of Appendix F for an estimated failure rate.

The FCS shall be considered as failed if any of the major systems (e.g., FH DCS or Protective Interlock System) are not available. The failure of the Seismic Trip System shall be considered as a minor failure where upon discovery of the Seismic Trip System failure, the FH operation in progress (if any) shall be completed.

9.3 Failure Detection

a) The system shall have continuous self-diagnostic capability, and the system faults shall be annunciated as they occur. Indicator lights shall be provided on all the hardware modules, to indicate the system health and annunciate faults.

b) FCS system faults shall also be annunciated to the operator through the FDS as well as through the Backup Control Panel. It shall be possible to obtain adequate information regarding the system faults through the EWS, to be able to identify the fault and the affected module.

9.4 Redundancy Requirements

9.4.1 Redundancy for Shared Resources

The FCS shall be based on a configuration of redundant components for equipment which has a shared function or which contributes significantly to the overall system unavailability (e.g., communication network). These redundant components shall be simultaneously active all the time or automatic switching to the standby component shall be provided in the case of failure of an active component.

9.4.2 Redundancy for Controllers

Controller redundancy is not required to meet the safety requirements.

- a) Some of the FH mechanisms are provided with redundant electric motors for operational reasons (e.g., to retrieve the FM without shutting down the reactor, should the FM become stranded in the reactor vault due to a motor failure). In such cases, full redundancy shall be provided for the control loop (from motion controller to the motor) for that mechanism.
- b) Wherever motion control loop redundancy is provided, it shall be possible for the operator to manually switch between the active and standby motion control loops in the case of a motion controller fault or any other component failure in the control loop.
- c) Control processor redundancy shall be provided for the FM Fluid Systems controller. Automatic switching shall be provided between the active and standby control processors.

9.4.3 Redundancy for Seismic Trip System

The Seismic Trip System shall be provided with full redundancy with respect to sensors, I/O, processors and power supplies to reliably detect the onset of seismic activity and interrupt power supply to the specified drives.

9.5 Maintainability Requirements

To facilitate a reasonable Mean Time to Repair (MTTR) period the FCS shall meet the following requirements::

- a) The FCS shall be located so that there is good accessibility and adequate clearance to carry out inspection, testing and maintenance tasks (refer to Reference [14]).
- b) The design of the cabinets, mounting of hardware modules, terminals, terminal strips and wiring shall be such that they are uniquely identifiable and accessible for maintenance.
- c) The FCS shall permit on-line maintenance and program changes whenever/wherever it is safe and feasible.
- d) Clear annunciation shall be provided to identify failed modules.
- e) The FCS shall be modular in design so that the failed modules can be replaced easily without affecting the rest of the system. It shall be possible to complete module replacements within an hour (excluding administration time).
- f) The number of types of modules used in the system shall be minimised. The hardware shall be standardised to the extent practicable.
- g) All the hardware shall be labelled and located to support unique identification.

- h) Where practical, designs must avoid components that could become obsolete within the life of the plant and/or be flexible enough to allow retrofit.

Refer to Appendix F for the required MTTR.

10. LAYOUT

Most of the FCS (excluding the Seismic Trip System) along with its I/O modules shall be installed in the CER. Some FCS equipment may be located in other areas of the plant to ensure maximum recommended distances between FCS components are not exceeded. Such areas shall offer a similar environment to that found in the CER.

- a) The FCS shall have no adverse effect on other equipment operating in the room or in the same area.
- b) The Seismic Trip System shall be located outside of the containment in the RAB avoiding the localised areas that may be subject to high temperature and humidity for short periods due to failure of piping containing limited amounts of high energy (Reference [4]).
- c) The layout shall be designed to achieve the following:
 - Meet the maintainability requirements identified in Section 9.5.
 - Meet the relevant fire protection requirements identified in Section 4.1.5.
 - Meet project objectives of reducing the construction and commissioning schedule while minimising the overall cost.
 - Provide additional space to support maintenance-related tasks.
 - Improve the system operability.

11. INTERFACING SYSTEMS

The FDS provides the Human-System Interface (HSI) for control of the FH system through the FCS. Therefore the FCS shall be interfaced to the FDS, the EWS and the FH System.

- a) The interface between the FCS and the FDS shall be designed such that a single interface failure will not lead to loss of the FDS and/or FCS. The data identified in Section 2.2.4.11 shall be exchanged between the FCS and the FDS. The communication interface shall be designed so that any faults in the FDS shall not affect the FCS, and vice versa.
- b) The FCS shall be interfaced to the Backup Control Panel as identified in Section 2.2.4.12.
- c) The FCS shall be interfaced to the FH mechanisms and process systems through various sensors and control elements connected to the I/O system (Section 2.2.4.8).
- d) The FCS shall be interfaced to the Electrical Power System that will provide power necessary for the FCS operation.
- e) The Seismic Trip System shall be provided with a highly reliable and uninterruptible power supply.
- f) The FCS shall be interfaced to the EWS as identified in Section 2.2.4.10.

The list of systems interfacing to the FCS is provided in Appendix G.

12. DECONTAMINATION AND DECOMMISSIONING

Not applicable to the FCS.

13. MATERIALS AND CHEMISTRY

Not applicable to the FCS.

14. LOADS, LOAD COMBINATIONS AND SERVICE LIMITS

Not applicable to the FCS.

15. HUMAN FACTORS AND OTHER DESIGN REQUIREMENTS AND CONSTRAINTS

15.1 Human Factors

The overall FCS design shall comply with the ACR Human Factors Engineering Program Plan. The FCS function diagram is shown in Figure 1.

The tables in Appendix H summarize the Human Factors requirements from various sections of this document.

Table H-1 summarizes the Human Factors requirements, operator and maintainer functions, and performance requirements as outlined in various sections of this document.

Table H-2 summarizes the Human Factors requirements in support of the operational and maintenance tasks.

15.2 Other Design Requirements

- a) The control software shall be designed to automate as many FH operations as practicable. Detection and mitigation techniques for operator errors shall be implemented during the detailed design phase.
- b) The system software, application software, control configuration data and critical system data shall be stored in non-volatile memory and shall be secure against power outages or power removal for hardware maintenance. Refer to the Quality Program Plan for FH Control System Software for details of configuration management for the FCS software.

15.3 Constraints

15.3.1 Control System Configuration

The conceptual block diagram of the overall FH Control and Operator Interface System is shown in Figure 2. The overall FCS shall consist of three functional units:

- a) FH DCS
- b) Protective Interlock System
- c) Seismic Trip System.

15.3.1.1 FH DCS Hardware and Software

The FH DCS shall be based on proven hardware and software and the configuration shall be designed to meet the following criteria:

- a) The control functions shall be distributed by both subsystem and function to reduce the consequence of failure of any subsystem control or a specific control function on the rest of the system.
- b) Fast, reliable and efficient data transfer to the FDS shall be provided to meet the annunciation, control and display requirements.

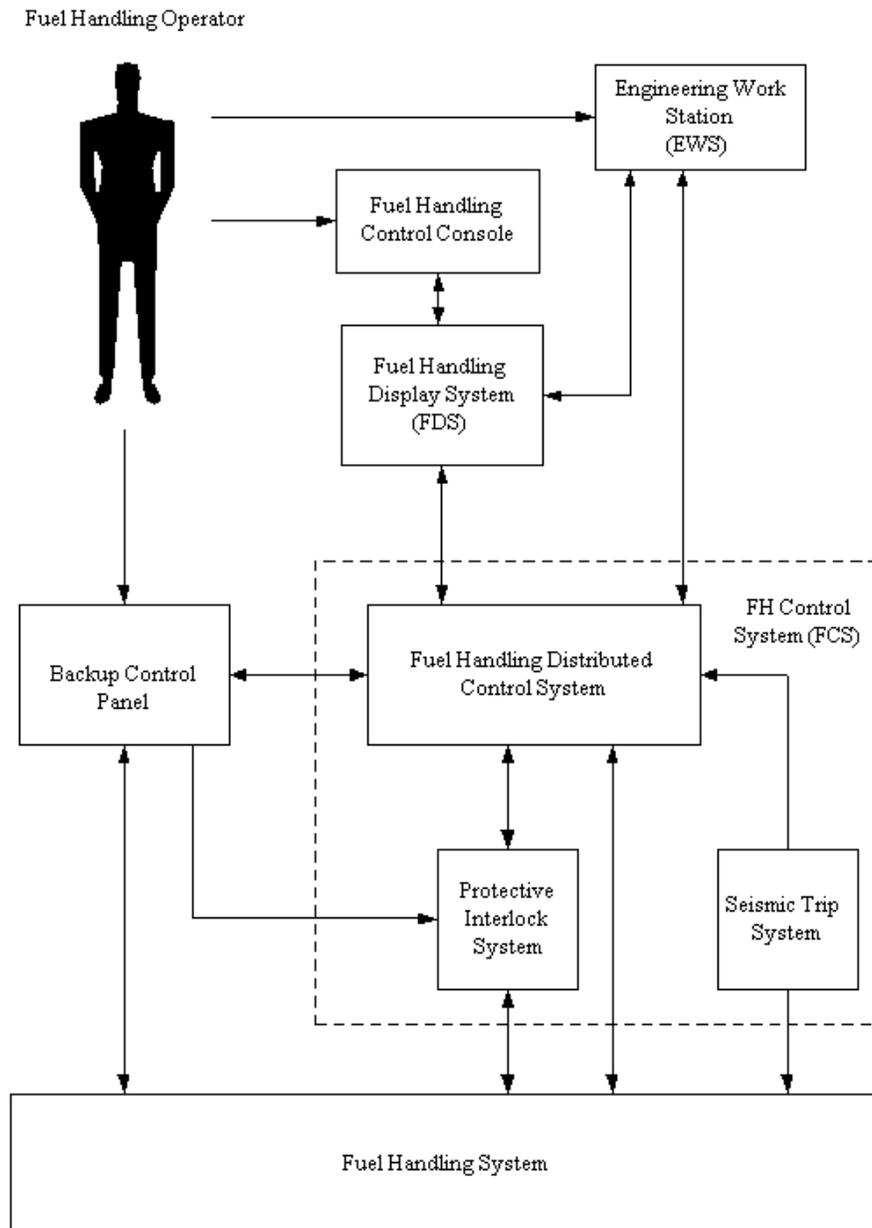


Figure 2 ACR FH Control and Operator Interface System

15.3.1.2 FH DCS Configuration

The conceptual system configuration of the FH DCS shall be as shown in Figure 3. Each side of the FH System shall be controlled by an independent partition of the DCS with the following requirements.

- a) A separate supervisory sequential controller shall be provided for each FH DCS partition to perform supervisory control of that side of the FH system. The supervisory sequential controllers of FH systems of both sides shall be interconnected to co-ordinate the operations between the two systems.
- b) Each FH DCS partition shall handle a separate set of FH subsystems, which shall be controlled by dedicated subsystem controllers.
- c) All subsystem controllers of each side shall be connected to a communication network for data exchanges between them as well as with the sequential controller.
- d) The controller at the subsystem level shall be able to perform any necessary computations, motion control co-ordination for electric drives, mechanism sequence control, PID control, and general operational logic/interlock functions. The subsystem level controllers shall be provided with suitable input/output (I/O) to perform the required functions.
- e) Individual electric drives of each subsystem shall be controlled by dedicated motion controllers of that subsystem. The motion controllers shall be able to communicate with the sequential and subsystem controllers.
- f) The FH DCS shall communicate with the FDS for exchange of command and feedback data.
- g) The FH DCS shall communicate with the EWS (one EWS common to both partitions) to perform functions as specified in Section 2.2.4.10.

15.3.1.3 System Partitioning

- a) The FH DCS system shall be partitioned as A and C sides, with limited communication between the two sides.

Rationale: The two sides of the FH system function independently except for limited co-ordination during refuelling operations.

- b) Within each side of the FH DCS the controls for each subsystem should be made independent of controls of other subsystems with facility for data exchanges between them. Failure of any subsystem control in one part of the FH DCS should not lead to a failure or potentially unsafe action by another subsystem of the FH DCS.

Rationale: Within each side of the FH system, various FH subsystems function independently, except for the FM Head which interacts with other FH subsystems (i.e., FM Head is required for all FH operations), but the operation of other subsystems are independent of each other.

- c) Physical separation of sequence control functionality from other control functions (e.g., motion control and process control) shall be provided.

Rationale: Physical separation between sequence control, process control and motion control enables certain control function to be carried out even when other control functions are not available (e.g., it shall be possible to complete the on-going FH operation in semi-automatic mode through the motion controller when the sequential controller fails).

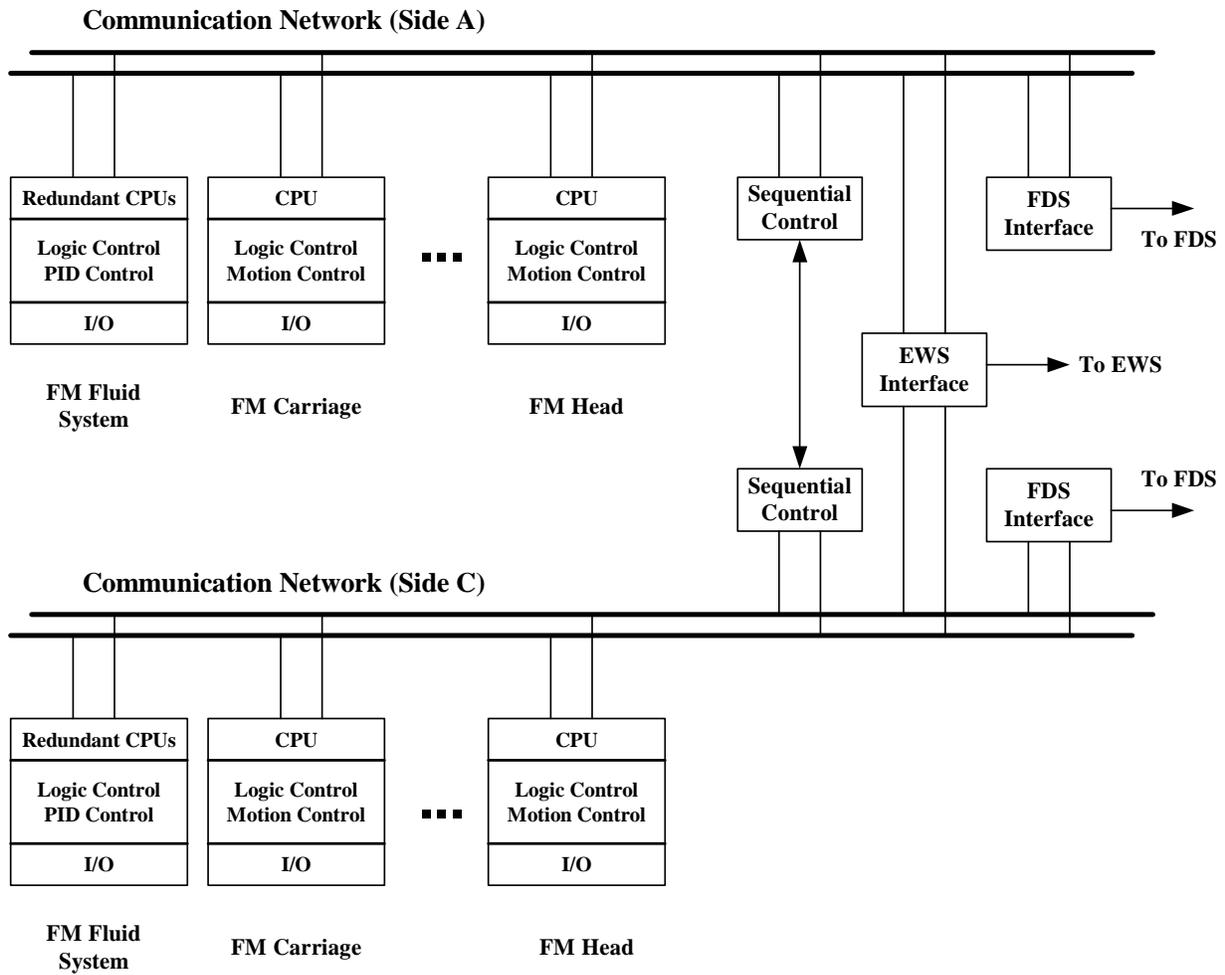


Figure 3 ACR FH DCS Configuration

16. REFERENCE DOCUMENTS

- [1] 108-35000-DR-001, Fuel Handling and Storage System, Design Requirements
- [2] 108-03650-SDG-001, Safety Design Guide, Safety Related Systems
- [3] 108-03650-SDG-002, Safety Design Guide, Seismic Requirements
- [4] 108-03650-SDG-003, Safety Design Guide, Environmental Qualification
- [5] 108-03650-SDG-004, Safety Design Guide, Separation of Systems and Components
- [6] 108-03650-SDG-005, Safety Design Guide, Fire Protection
- [7] 108-03650-SDG-006, Safety Design Guide, Containment
- [8] 108-03650-SDG-007, Safety Design Guide, Radiation Protection
- [9] 108-01913-QAM-001, Quality Assurance Manual
- [10] 108-00580-130-002, Licensing Basis for NG CANDU Concept, Licensing Basis Document
- [11] 108-63582-ASD-002, Assessment of Software Category for the Fuel Handling Control System (to be issued)
- [12] AECL Operating Instruction 933.4.2, Equivalent Quality Program Standards.
- [13] 108-35000-DCD-002, NG CANDU Refuelling Method
- [14] 108-03800-SPS-002, ACR Maintenance Basis (to be issued)
- [15] 10810-01372-TED-001, ACR-700 Technical Outline

Appendix A

Design Parameters

The values given in the following table are design parameters, not design requirements. They are non-mandatory and are provided for reference only.

	SECTION	DESIGN PARAMETERS	REFERENCE
1	Introduction	No numerical data.	
2	Functional Requirements	<p>Sequential Control</p> <p>Approximately 40 jobs are required, each consisting of up to 20 sequences. Approximately 200 sequences are required, each typically consisting of 10 to 150 steps. Step is a set of operations comprising up to 5 commands and 10 feedbacks.</p> <p>Computational Functions</p> <p>Arithmetic function should have a precision of at least 24 bits. The subsystem controllers should be capable of handling 16 bit position data (including sign) obtained from resolvers and or motion controllers.</p> <p>I/O Systems</p> <p><u>Analogue Inputs</u></p> <p>a) The analogue process signals should be converted to numerical engineering values.</p>	

	SECTION	DESIGN PARAMETERS	REFERENCE
		<p>b) The subsystem controller should be able to handle the following types of analogue inputs:</p> <ul style="list-style-type: none"> • 0 - 20 mA at 24 Vdc (minimum) • 4-20 mA at 24 Vdc (minimum) • 0 - 5 Vdc (able to withstand a 170 mA over-current) • 0 - 10 Vdc and +/-10 Vdc (able to withstand a 170 mA over-current) • 3 and 4 wire Resistance Temperature Detectors (RTD) (adjustable 1 to 10 mA excitation per channel) • Linear Variable Differential Transformers (LVDT) (minimum excitation range: 50 Hz to 10 kHz; input signals: 11.8VRMS L-L, 26VRMS L-L, and 90VRMS L-L; capable of being connected in a master/slave relationship (to minimize beat frequencies) with other LVDTs, incremental resolvers and multi-turn resolvers) • Incremental Resolvers (minimum excitation range: 50 Hz to 10 kHz; input signals: 11.8VRMS L-L, 26VRMS L-L, and 90VRMS L-L; capable of being connected in a master/slave relationship (to minimize beat frequencies) with other LVDTs, incremental resolvers and multi-turn resolvers) • Multi-turn Absolute Resolvers (minimum excitation range: 50 Hz to 10 kHz; input signals: 11.8VRMS L-L, 26VRMS L-L, and 90VRMS L-L; capable of being connected in a master/slave relationship (to minimize beat frequencies) with other LVDTs, incremental resolvers and multi-turn resolvers) • Binary Word Inputs (parallel data bits, 5 to 48 Vdc and TTL logic) <p>c) In addition to the signals with zero bias and standard offsets (i.e., 4-20 mA, 1-5 Vdc etc.), the system should be able to handle signals with non-standard offset.</p>	

	SECTION	DESIGN PARAMETERS	REFERENCE
		<p>d) Low pass filtering should be provided for all analogue inputs. The filter time constant should be selectable (between 5 ms and 200 ms) to handle slow process signals and fast varying mechanism position signals as required. The filter time constants should be selectable individually for each analogue input.</p> <p>e) Each analogue input signal should be checked for rationality/loss of signals due to open/short circuit, ground faults or signal source failure. The loss of signal integrity should be flagged for appropriate processing by the application programs.</p> <p>f) Filtering or signal hysteresis should be provided for all binary words and analogue signals (e.g., resolver signals)</p> <p>g) The motion control system should be able to handle inputs from the following types of position sensors:</p> <ul style="list-style-type: none"> • Incremental Resolvers • Multi-turn Absolute Resolvers • Quadrature encoders <p>h) The subsystem controllers and motion controllers should be capable of handling high speed position signals from absolute resolvers as binary word data.</p> <p><u>Digital Inputs</u></p> <p>a) The subsystem controller should be able to handle the following types of digital inputs:</p> <ul style="list-style-type: none"> • 24 Vdc • Potential Free Contacts. 	

	SECTION	DESIGN PARAMETERS	REFERENCE
		<p>b) The motion control system should be able to handle the following types of digital inputs:</p> <ul style="list-style-type: none"> • TTL-compatible • Potential Free Contacts. <p>c) Contact debouncing should be provided for all digital inputs.</p> <p>d) Input signals should be checked to detect signal faults and detected errors should be flagged for appropriate processing by the application programs.</p> <p><u>Analogue Outputs</u></p> <p>a) The subsystem controller should provide an analogue output of 4-20 mA (load of 0-250 Ω, to be confirmed during detail design).</p> <p>b) The motion control system should provide a differential analogue output of ±10 Vdc for current/velocity command signals.</p> <p>c) In case of a module fault, the last value of the output should be set to a predefined fail-safe value (0%, 50%, 100%, “as is”, or 0V clamp (digital tie)).</p> <p>d) For certain critical output signals, it should be possible to monitor the analogue output value.</p> <p><u>Digital Outputs</u></p> <p>a) The subsystem controller should provide the following types of digital outputs:</p> <ul style="list-style-type: none"> • 24 Vdc (current rating of 500 mA) • Relay Contacts (240 Vac at 3.0A inductive for solenoids and 30 Vdc at 2.0A inductive for solenoids and indicator lamps) 	

	SECTION	DESIGN PARAMETERS	REFERENCE
		<p>b) The motion control system should provide at least one of the following types of digital outputs:</p> <ul style="list-style-type: none"> • TTL-compatible • 24 Vdc (current rating of 100 mA maximum) • 24 Vdc isolated output at 100 mA (either relays or opto-isolated outputs) <p>The digital outputs should fail to a pre-defined safe state (open, close, or “as is”) in case of a module fault. For certain critical output signals, it should be possible to monitor the output value.</p>	

	SECTION	DESIGN PARAMETERS	REFERENCE
3	Performance Requirements	<p>Sequence Control Execution Time</p> <p>The time between execution of two consecutive steps in a sequence should be configurable between 100 ms and 500 ms, with 500 ms as the default.</p> <p><i>Rationale: The FH operation is a series of tasks carried out under the supervision of the sequential controller. Any delay by the sequential controller in processing and issuing the necessary commands will delay the refuelling cycle. In CANDU 6, this time was an average of 500 ms and a maximum of one second. Since reduction in the fuelling cycle times is important for ACR, a shorter time has been adopted as the maximum allowed time delay for ACR.</i></p> <p>Data Transfer between Sequential Controller and Subsystem/Motion Control Processors</p> <p>a) The feedback data from the subsystem controllers and motion controllers should reach the sequential controllers within 100 ms.</p> <p><i>Rationale: Certain control operations can be completed almost instantaneously (i.e., opening a solenoid valve). Any delay in providing this feedback to the sequential controller will unnecessarily delay the execution of commands in the next step and results in increase in the fuelling cycle time. The allowable time between the consecutive steps is identified in " Sequence Control Execution Time" paragraph above, and obtaining the feedback within this time will ensure that the commands of the next step are executed without additional delay. In CANDU 6 this time is 100 ms (program execution cycle time of the DCC).</i></p> <p>b) The commands from the sequential controllers should reach the subsystem controllers and motion controllers within 50 ms.</p>	

	SECTION	DESIGN PARAMETERS	REFERENCE
		<p><i>Rationale: A maximum of 50 ms command transfer time (especially for stop commands) ensures that the mechanisms are controlled without leading to potential damage.</i></p> <p>Motion Control Loop Update Time for Brushless DC Drives The update time for each electric drive motion control loop (for a single axis) should not exceed 1 ms.</p> <p><i>Rationale: To achieve the required mechanism positioning tolerance and ensure system stability, a 1 ms control loop update time is required.</i></p> <p><i>Note: Most commercially available motion controllers have loop update period in the order of 50 to 100 μs per axis.</i></p> <p>Motion Control Loop Update Time for AC Drives The update time for the control loops of AC motor drives should not exceed 100 ms.</p> <p><i>Rationale: 100 ms control program update has been arrived at based on the travel speed and positioning accuracy required for the mechanisms.</i></p> <p>PID Control Loop Update Time PID control loops should be updated at intervals of 50 to 150 ms.</p> <p><i>Rationale: Dedicated PID Loop controllers are being used in Wolsong 2/3/4 with loop update times between 50 and 150 ms depending on the loop. The same update times are adopted for ACR and are adequate considering the much slower FH process systems.</i></p>	

	SECTION	DESIGN PARAMETERS	REFERENCE
		<p>Position Data Transfer from FH DCS to FDS Interface</p> <p>Position data of the mechanisms should be updated and transferred to the FDS within 50 ms, so that the operator can manually jog and position the mechanisms using the VDU display and data input device.</p> <p>Transfer Time for Commands from FDS Interface to FH DCS</p> <p>The FH DCS should be able to transfer the operator commands received from FDS interface to the controllers and I/O within 50 ms.</p> <p>Data Transfer from FH DCS to FDS Interface (Excluding Position Data)</p> <p>a) During the execution of a sequence in automatic mode, the FH DCS should be able to update and transfer the data required for sequence monitoring and alarm monitoring by the FDS at least once every 100 ms.</p> <p><i>Rationale: The maximum 100 milliseconds sequence data update interval at the FDS matches the sequence control execution speed and enables the operator to monitor the sequences in real time.</i></p> <p>b) The rest of the system data (for inactive mechanisms and process parameters) should be transferred to the FDS every 500 ms.</p>	

	SECTION	DESIGN PARAMETERS	REFERENCE
		<p>Analogue Input Conversion</p> <ul style="list-style-type: none"> a) The analogue input conversion resolution for inputs from the process systems and most of the mechanisms should be a minimum of 13 bits (excluding sign) over the signal ranges of 0-20 mA, 0-5 Vdc, 0-10 Vdc, 4-20 mA, and 1-5 Vdc. The maximum error over the operating temperature ranges (refer to Section 6 of this Appendix) should not exceed 0.05% of full scale with a CMRR of 80 dB over 0-60 Hz. b) It should be possible to resolve the position of some mechanisms using resolvers for position measurement (i.e., Positioning Ram) to 15 bits plus sign with a maximum error of 0.003% of full scale. c) The analogue outputs (for non-motion control applications) should have a minimum 12 bit resolution and the error should not be more than 0.5% of full scale over the operating temperature range specified in Section 6 of this Appendix. Current analogue outputs will be capable of supplying maximum current (typically 20 mA) at 24 Vdc. d) The analogue outputs for motion control applications should have a minimum 16 bit resolution and the error should not be more than 0.05% of full scale over the operating temperature range specified in Section 6 of this Appendix. <p>Seismic Sensing Range</p> <p>The Seismic Trip System should be able to monitor the ground acceleration within a frequency range of 0.5 Hz to 15 Hz.</p>	

	SECTION	DESIGN PARAMETERS	REFERENCE
		<p>Seismic Sensing Accuracy</p> <p>The sensing accuracy of the Seismic Trip System (Section 2.2.6) should be $\pm 1\%$ of full scale and the response time should a maximum of 100 ms.</p> <p><i>Rationale: During an earthquake, the P-Wave arrives first followed by the Secondary Wave (S-Wave). The major damage is caused by the S-wave. The minimum time delay between a P-Wave and an S-Wave is one second. A 100 ms response time enables tripping of circuit-breakers and putting the FH system in a safe state within one second.</i></p>	
4	Safety Requirements	No numerical data.	
5	Applicable Codes, Standards and Classification	No numerical data.	
6	Environmental Conditions	<p>Operating conditions within CER: Temperature = 20°C to 26°C Design Condition within CER: Temperature = 0°C to 55°C Relative Humidity = 5% to 95% Pressure = atmospheric</p>	
7	Overpressure Protection	Not applicable to FCS.	
8	Inspection and Testing	No numerical data.	

	SECTION	DESIGN PARAMETERS	REFERENCE
9	Reliability, Unavailability and Maintainability Requirement	No numerical data.	
10	Layout	No numerical data.	
11	Interfacing Systems	<p><u>Electrical Power System:</u></p> <p>The design should be based on 240 Vac, 50 Hz power source ($\pm 5\%$ variations in voltage, 4 ms interruption duration).</p> <p>The design should facilitate the change to 120 Vac, 60 Hz power source ($\pm 5\%$ variations in voltage, 4 ms interruption duration).</p>	
12	Decontamination and Decommissioning	Not applicable to the FCS.	
13	Materials and Chemistry	Not applicable to the FCS.	
14	Load, Load Combinations and Service Limits	Not applicable to the FCS.	
15	Human Factors and other Design Requirements and Constraints	No numerical data.	

Appendix B**Typical (Non-Mandatory) List of PID Loops**

GSI	Subsystem	Drives
63523	FM Water System	Magazine Pressure Control (see Note 2) FM Water System Temperature Control
63526	FM Emergency Water System	FM Emergency Water System Pressure Control
63530	SFT	SFT Temperature Control SFT Flow Control
63560	Rehearsal Facility	Channel Water Pressure Control Channel Flow Control

Notes:

- 1. Except for the Rehearsal Facility, process loops are required for each side of the FH System.*
- 2. Magazine Pressure Control requires redundancy.*

Appendix C

Typical (Non-Mandatory) List of Motor Drives

ASI	Subsystem	Drives
63510	NFT	^{1,3} NFT Magazine ^{1,3} NFT Ram ^{1,3} NF Loading Ram
63521	FM Head	^{1,3} Snout Clamp – main ^{1,3} Snout Clamp – alternate ^{1,3} Positioning Ram drive #1 ^{1,3} Positioning Ram drive #2 ^{1,3} Latch Ram – main ^{1,3} Latch Ram – alternate ^{1,3} Magazine – main ^{1,3} Magazine – alternate ^{1,3} Separator drive #1 ^{1,3} Separator drive #2 ^{1,4} Magazine Level Lowering Pump – main ^{1,4} Magazine Level Lowering Pump – alternate
63522	FM Bridge & Carriage	^{1,3} Bridge Elevator #1 – main ^{1,3} Bridge Elevator #1 – alternate ^{1,3} Bridge Elevator #2 – main ^{1,3} Bridge Elevator #2 – alternate ^{1,3} Bridge Elevator #3 – main ^{1,3} Bridge Elevator #3 – alternate ^{1,3} Bridge Elevator #4 – main ^{1,3} Bridge Elevator #4 – alternate ^{1,3} Carriage – main ^{1,3} Carriage – alternate ^{1,3} Fine Y – main ^{1,3} Fine Y – alternate ^{1,3} Z – main ^{1,3} Z – alternate ^{1,3} Rotation – main ^{1,3} Rotation – alternate
63523	Water Supply System	^{2,4} FM Water Supply Pump – main ^{2,4} FM Water Supply Pump – alternate ^{2,4} Low Pressure Recirculation Pump ^{2,4} Emergency Cooling Supply Pump – main ^{2,4} Emergency Cooling Supply Pump – alternate

ASI	Subsystem	Drives
63530	SFT	^{2,4} Circulation Pump – main ^{2,4} Circulation Pump – alternate ^{1,3} SFT Fuel Bundle Decelerating Ram ^{1,3} Separator drive #1 ^{1,3} Separator drive #2 ^{1,3} SFT Magazine ^{1,3} SF Discharge Ram ^{2,3} SFT Inter-bay Conveyor – main ^{2,3} SFT Inter-bay Conveyor – alternate
21602	Shielding Doors & Misc. Systems	^{1,4} Reactor Vault Shielding Door – main ^{1,4} Reactor Vault Shielding Door – alternate ^{1,4} Maintenance Lock Door

Notes:

1. *Drives preceded by ¹ are required on both sides (A and C) of the FH system.*
2. *Drives preceded by ² are common to both sides of the FH system. That is, only one is required per unit.*
3. *Drives preceded by ³ are brushless DC drives with motion controllers.*
4. *Drives preceded by ⁴ are AC drives (single or two speed)*

Appendix D

Typical (Non-Mandatory) List of I/O Signals

The following table provides a typical list of I/O signals to be connected to the FH DCS. An additional 25% (minimum) of spare capacity is required for each subsystem.

Subsystem	Analogue Inputs	Analogue Outputs	Digital Inputs	Digital Outputs	RTD	Encoders	Single-turn Resolvers	Multi-turn Resolvers	LVDTs	Motion Controllers for Brushless DC Drives (see Note)
Bridge & Carriage A	16	0	84	30	0	0	16	16	4	16
Bridge & Carriage C	16	0	84	30	0	0	16	16	4	16
Catenary System A	0	0	4	0	0	0	0	0	0	0
Catenary System C	0	0	4	0	0	0	0	0	0	0
FM Head A	15	0	70	40	3	0	10	10	8	10
FM Head C	15	0	70	40	3	0	10	10	8	10
NFT A	5	0	30	20	0	0	6	6	0	3
NFT C	5	0	30	20	0	0	6	6	0	3
Shielding Doors A	0	0	10	5	0	0	0	3	0	0
Shielding Doors C	0	0	10	5	0	0	0	3	0	0
SFT A	12	0	30	20	3	0	10	10	0	6
SFT C	12	0	30	20	3	0	10	10	0	6
FM Process A & C	80	16	100	60	12	0	0	0	0	0
Grand Total	176	16	556	290	24	0	84	90	24	70

Note:

It is assumed that a motion controller is used for each drive. In this table, the motion controller is considered to be part of the FH DCS.

Appendix E

Typical (Non-Mandatory) List of Interlocks

The following table provides a typical list of interlocks to be provided by the Protective Interlock System.

Interlock	Drive/Action Affected	Pre-Requisite	Action Prevented	Consequence Avoided
1a	Carriage drive	Snout not clamped.	Prevents FM carriage motion while on reactor or attached to transfer ports.	End fitting damage / containment at fuel ports.
		Catenary free to move.	Avoids overstressing hoses and cables.	Damage to hoses and cables.
		Carriage in normal window of operation (direction sensitive).	Overtravel.	Damage to carriage and bridge supports.
1b	Carriage drive from either side, when carriage is in region of shielding door.	Shielding door open.	Prevents collision with shielding door.	Damage to FM.
		FM rotated to line up with maintenance lock.	Prevents collision with shielding door, bridge columns or structures in maintenance lock.	Damage to FM.
		Bridge rails and maintenance lock rails aligned.	Prevents transfer between misaligned structures.	Damage to FM and carriage
1c	Carriage drive, when carriage is in maintenance lock.	FM rotated to line up with maintenance lock	Prevents collision with shielding door or structures in maintenance lock.	Damage to FM.
1d	Carriage drive, when carriage is on bridge.	FM rotated to face reactor with Z drive retracted, or line up with maintenance lock.	Prevents interference with reactor end fittings	Damage to end fittings and FM.

Interlock	Drive/Action Affected	Pre-Requisite	Action Prevented	Consequence Avoided
1e	Carriage high speed	Z drive retracted.	Prevents high speed during homing.	End fitting damage / containment at fuel ports.
2a	Bridge Drive	Carriage not in region of shielding door.	Prevents bridge operation while FM is traversing between the bridge rails and maintenance lock rails.	Damage to FM and carriage.
		Catenary free to move.	Avoids overstressing hoses and cables.	Damage to hoses and cables.
		Bridge in normal window of operation (direction sensitive).	Overtravel	Damage to end fittings, FM, carriage and bridge.
2b	Bridge drive (when carriage is on bridge)	Z drive retracted.	Prevents bridge operation while on reactor.	End fitting damage.
		FM rotated to face reactor or line up with maintenance lock.	Prevents interference with reactor end fittings	Damage to end fittings and FM.
2c	Bridge brakes release.	Z drive retracted.	Prevents release of bridge brakes with snout over end fitting.	End fitting damage.
3a	Z drive advance, when carriage is on bridge	Bridge brakes engaged.	Prevents Z motion towards the reactor while there is any possibility of bridge motion.	End fitting damage.
3b	Z drive retract	Snout unclamped and snout safety lock disengaged.	Prevents Z motion while FM is clamped to end fitting.	End fitting damage / containment at fuel ports.

Interlock	Drive/Action Affected	Pre-Requisite	Action Prevented	Consequence Avoided
4	Rotary drive	Z drive retracted.	Prevents rotary motion with snout over end fitting.	End fitting damage / containment at fuel ports. Damage to the Y drive and support columns. End fitting damage / containment at fuel ports.
		FM within the defined locations for rotation.	Prevents rotary motion in restricted areas: in region of shielding door and bridge columns.	Damage to the bridge columns and FM.
5a	NF magazine valves - open	NF port valves closed.	Prevents loss of containment.	Breach of containment.
5b	NF port valves - open	NF magazine valves closed.	Prevents loss of containment.	Breach of containment.
6a	SF bay valves - open	SF port valves closed.	Prevents loss of containment.	Breach of containment.
6b	SF port valves -open	SF bay valves closed.	Prevents loss of containment.	Breach of containment.
7a	Reactor vault shielding door - close	FM carriage fully in maintenance lock and bridge raised out of the way of the door.	Prevents shielding door from damaging the catenary or the bridge.	Loss of control, interlocks, and cooling, when FM is in the reactor vault.
7b	Reactor vault shielding door - open	Maintenance lock door closed	Operator access.	Dose to operator.
7c	Maintenance lock door - open	Reactor vault shielding door closed	Operator access.	Dose to operator.
8	Power supply to bridge and carriage drives.	Snout unclamped and snout safety lock disengaged.	Prevents any bridge or carriage drive operation while on end fitting.	End fitting damage.

Appendix F

Design Requirements

Plant life = 60 years (Reference [15])

Capacity factor = 90% (Reference [15])

Peak Horizontal Ground Acceleration = 0.30g (Reference [15])

Seismic Sensing Range

The Seismic Trip System shall be able to monitor the ground acceleration in the range of at least ± 0.35 g.

Rationale: The DBE level for ACR plant is 0.30 g (Reference [15]). The selected acceleration range encompasses the DBE level and will be able to record low-level seismic activity. The selected frequency range corresponds to the frequency of the Primary Wave (P-Wave). Early detection of the non-damaging P-wave is required to trip the FH drives before the arrival of the damaging Secondary wave (S-Wave).

Safety Requirements

The FH DCS shall be designed and shall be capable of being configured such that specific critical functions shall have a demonstrated unsafe failure rate of less than 1 in 100 years.

Rationale: The overall FCS is a process system which can lead to Class 1 and Class 2 events (as per CNSC Consultative document C-6) with initiating frequency limits as given below:

<u>Event type</u>	<u>Initiating Event Frequency Limit</u>
Class 1 events	$f > 10^{-2}/\text{yr}$
Class 2 events	$10^{-2}/\text{yr} \geq f > 10^{-3}/\text{yr}$

Due to the provision of the Protective Interlock System, the Seismic Trip System and other design features, it is unlikely that a failure of FH DCS hardware or software can directly lead to these events. A failure of the FH DCS can increase the probability of a plant system failure that can lead to systematic fuel failures or release of radioactivity.

Considering this fact, a minimum allowable initiating event frequency limit of $10^{-2}/\text{yr}$ has been imposed on the FH DCS, which leads to 1 allowable unsafe failure once every 100 years.

Reliability

- a) The FH DCS shall be designed and shall be configurable such that any global failure (any loss greater than 1 station (a control rack that may contain I/O modules and processors) or a communication failure between stations) exceeding a repair time of 8 (preliminary) hours and less than 32 (preliminary) hours (including the time required for failure detection, diagnosis and repair) shall not occur more than once in 25 (preliminary) years.

Rationale: The overall FH system contributes 10% (see Reference [1]) of the plants allowable minor outages and de-ratings. Considering a lifetime capacity factor of 90% (Reference [15]) for an ACR plant, the allowable minor outages and de-ratings is 4 days (96 hours) per year (Reference [12]). The allowable overall FH system contribution (10%) is

9.6 hours/year. Out of these 9.6 hours, based on relative complexities of various FH subsystems, the FH control system is assumed to contribute 1.2 hours (12.5%). The allowable failure rate is $1.2/30 = 0.04$ or one failure in 25 years.

Notes:

- Failure of the partition on one side is equivalent to the whole system failing. The reactor cannot be fuelled with only one fuelling machine running.*
 - Under ideal conditions the reactor can operate up to 7 days without refuelling before it is de-rated. In reality, the reactor may not always have 7 days of time. For this reason the requirement refers to faults taking more than 8 (preliminary) hours to repair.*
 - 8 (preliminary) hours is the duration of a shift. Any repair that cannot be completed within a shift is perceived to be a major failure.*
- b) The FH DCS shall be designed and configurable such that any local failures (a station or important single I/O module or processor) shall be repairable within 8 (preliminary) hours (this time shall include the time required for detection, diagnosis and repair). These failures shall not occur more than once a year (over the entire system).

Availability

The availability of the FCS must support the overall plant availability target of 90% (Reference [15]).

Maintainability

The Mean Time to Repair (MTTR) shall not exceed [TBD] days for any major failure.

Appendix G

List of Interfacing Systems

The following table summarizes the list of systems that interface with the FCS.

ASI	System
21602	Shielding Doors & Other Miscellaneous Systems
35000	Fuel Handling and Storage
35100	New Fuel Transfer and Storage
35210	Fuelling Machine Head
35220	Fuelling Machine Bridge and Carriage
35230	Fuelling Machine Water System
35250	Fuelling Machine Gas Auxiliary Systems
35260	Fuelling Machine Emergency Water System
35300	Spent Fuel Transfer and Storage
35730	Hose and Cable Management System
53000	Distribution System
60000	Instrumentation and Control
63510	New Fuel Transfer (NFT) System
63521	Fuelling Machine Head Controls
63522	Fuelling Machine Bridge and Carriage
63523	Fuelling Machine Water System
63525	Fuelling Machine Gas Auxiliary System
63526	Fuelling Machine Emergency Water System
63530	Spent Fuel Transfer (SFT) and Storage Controls
63570	Fuelling Machine Transfer
63583	Fuel Handling Display System
63594	Engineering Work Station
	Backup Control Panel
65000	Control of Electric Power Systems
66200	Control Equipment Room

Appendix H

Typical (Non Mandatory) Human Factors Requirements

Table H-1

Human Factors Requirements (Operator and Maintainer Functions / Performance Requirements)

The following table summarizes the Human Factors requirements, operator and maintainer functions and performance requirements as outlined in various sections of this document.

Function Type	Function Description	DR Reference	Plant Operating Regions and System State for Function	Function Automated or Performed Manually	Information Required to Perform Function
System Supervision	Selection of modes of sequential control.	2.2.4.1.2	All	Operator	Current status of the FH system and the specific operational requirement.
	Operator intervention during sequential control.	2.2.4.1.3	All	Operator	Current status of the FH system and the specific operational requirement.
	Device control commands and control mode selection.	2.2.4.2	All	Operator	Status of the device under control and the specific operational requirement.
	Selection of modes of motion control.	2.2.4.4.3	All	Operator	Status of the mechanism under control and the specific operational requirement.
	Operator intervention during motion control.	2.2.4.4.4	All	Operator	Status of the mechanism under control and the specific operational requirement.
	Transfer of I/O module failure data to the EWS and FDS.	2.2.4.8	All	Automated	Failed module identification and error data.
	Monitoring of abnormal temperature conditions.	6.2	All	Automated	Temperature inside the FCS cabinets.

Function Type	Function Description	DR Reference	Plant Operating Regions and System State for Function	Function Automated or Performed Manually	Information Required to Perform Function
	Automatic detection of FCS failures.	9.3	All	Automated	System fault information.
	Automating FH operations to the extent practicable.	15.2	All	Automated	Status of the total FH system.
Corrective Action and Control	Action on fault conditions during motion control.	2.2.4.4.1	All	Automated	Status of mechanisms and motion parameters.
	Monitoring and automatic corrective action.	2.2.4.7	All	Automated	Status of FH system.
	Analogue output fault handling.	Appendix A Section 2 (Analogue Outputs)	All	Automated	Type and location of fault.
Corrective Action	Digital output fault handling.	Appendix A Section 2 (Digital Outputs)	All	Automated	Type and location of fault.
	Switching between active and standby controllers.	9.4.2	All	Automated	Failure indication for the controller or any other component in the control loop.
Inspection	Periodic inspection of FCS terminations during normal operation.	8.1	All	Maintainer	None
Testing	Periodic testing of Protective Interlock System and Seismic Trip System.	8.2	All	Maintainer	None

**Table H-2
Typical (Non-Mandatory) Human Factors Requirements (Operational and Maintenance Tasks)**

The following table summarizes the Human Factors requirements in support of the operational and maintenance tasks.

Requirement Type	Description	DR Reference	Human Factors Rationale
Accessibility	Provision of test points/terminals for testing and calibration.	8.3	The test points/terminals will improve the accessibility of internal hardware test points.
	Layout of FCS equipment.	9.5 a) & 1 a) b)	Adequate accessibility is required to carry out inspection, testing, and maintenance tasks.
	Design of cabinets.	9.5 b)	Hardware modules and wiring are required to be clearly visible and accessible for maintenance.
Maintenance	Annunciation of failed modules.	9.5 d)	Clear annunciation required to identify the failed modules.
	Modular design.	9.5 e)	Modular design facilitates quick and easier replacement of failed hardware.
	Labelling of hardware.	9.5 g)	Clear labelling reduces the possibility of using incorrect hardware during maintenance.
	Editing of software.	2.2.4.10 e)	Display of blocks of code minimizes scrolling through screens and allows operator to see more than a small segment of the program.