CONTROL OF CANDU 3 FUEL HANDLING OPERATIONS USING A DEDICATED DISTRIBUTED CONTROL SYSTEM

D.Arapakota, J.A.Yip and R.Anderson
AECL CANDU
Sheridan Park Research Community
Mississauga, Ontario

INTRODUCTION

The Fuel Handling (F/H) System in existing CANDU 6 plants was designed in the early 1960's, utilizing the technology available at that time, including the use of oil hydraulic motors for driving some of the mechanisms. Position control for these mechanisms was implemented using on/off control. The system was designed to be operated in full automatic mode through a single centralized computer system, which performs both the control and display functions. The F/H control computer system is shared with only one of the main plant control computers (DCC-Y) and in order to ensure continuity of F/H operations during the possible unavailability of the control computer system, full manual back-up control and operator interface was provided using discrete hardware (such as relays, current alarm units,analog controllers, panel indicators, switches etc.). The control software was written in Assembly language and highly skilled computer engineering staff are required to maintain the F/H control software. This design has proven to be adequate in meeting the basic control requirements, however, the sharing of the F/H control computer with the main plant control system has resulted in some operational limitations for enhancing the operation of the F/H system.

The design of the CANDU 3 F/H system is based on the latest available technology utilizing standard off-the-shelf equipment to the maximum possible extent. All the mechanisms in the F/H system are driven by brushless d.c servo motors with resolver position sensors, which facilitate accurate closed loop position control. The control system design is based on the following primary design decisions:

(a) Totally decouple the F/H control system from the main plant control system to provide for maximum operational flexibility for the F/H system. This is in line with the current design practice at multi-unit CANDU stations such as Bruce and Darlington.

(b) Separate control and display functions so that systems most suitable for each function can be utilized.

(c) Provide an independent hardwired protective logic control system to minimize the consequence of software failure and to avoid safety critical categorization of F/H control software.

(d) Take advantage of currently available distributed control technology.

Based on the above primary design philosophy, it was decided to implement a dedicated Distributed Control System (DCS) for the CANDU 3 F/H system. Accordingly, a generic system configuration has been designed meeting certain pre-defined detailed design criteria.

CONTROL SYSTEM CONFIGURATION

Control of the F/H system involves mainly logic control operations (configured either for interlocks or for sequential control) and motion control operations together with a small amount of conventional process control. These control operations are ideally suited to the functionality and capability of Programmable Logic Controllers (PLC's). It was therefore decided to base the F/H control system configuration on PLC's.

The control system configuration proposed to be implemented for the CANDU 3 F/H system is shown in Figure-1. This is a generic configuration, whose design requirements can be broadly met by most of the commercially available systems, with minor variations specific to each system architecture.

The control system configuration contains functional controller units for the following major subsystems and functions:

(a) Fuelling Machine (F/M) Carriage system
(b) F/M Head system
(c) New Fuel Transfer system
(d) Irradiated Fuel Transfer system
(e) F/M Fluid system
(f) Sequential Control system

Each of the above systems is controlled by an individual PLC. These PLC's are connected through a peer level communication network exclusively for data exchanges between them.

The first four functional control units have a number of sub-functional units (Motion Controllers) connected to each of them to perform motion control for individual mechanisms.

A separate communication path (data highway) is provided for data transfers between the display computer system and the distributed PLC network.

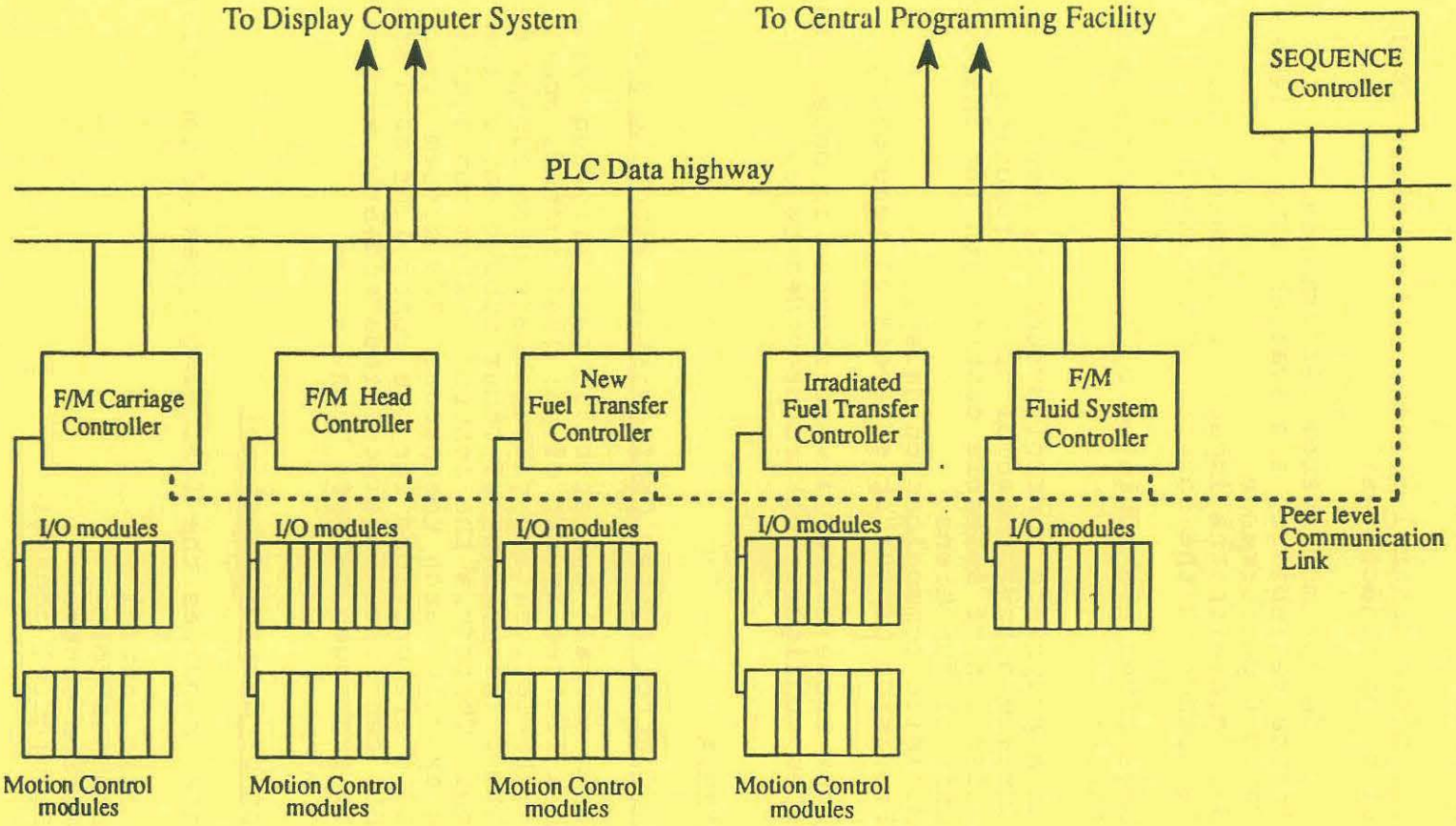

Figure – 1

Distributed Control System configuration for CANDU–3 Fuel Handling System

A centralized programming facility is also provided for all the control units.

DESIGN OBJECTIVES

The F/H distributed control system configuration is designed to meet the following objectives:

(a) Provide optimum system performance.
(b) Ensure reliability and availability at least equal to CANDU 6 performance.
(c) Help minimize the impact of Software Quality Assurance on the control system design.

The above objectives are achieved by adopting the following design criteria:

(a) An appropriate control system structure.
(b) Optimum distribution of control functions.
(c) Selection of suitable controllers for the required control functions.
(d) Minimize communication delays.
(e) Provision of suitable levels of redundancy.

Details on how these criteria were adopted in developing the F/H control system configuration are provided below.

DESIGN CRITERIA

Matching of Control System Configuration with the F/H system

The F/H system overall operation is basically sequential in nature with a limited amount of parallel control operations. It is divided into logical subsystems where each subsystem can function almost independent of other subsystems in the sequence of operations. Therefore the control system configuration was selected to exactly match the natural F/H system structure and separate PLC's are provided for the control of each subsystem so that each PLC can function almost independently with only limited data exchanges between them.

Distribution of Control Functions

The F/H system requires the following types of controls:

(a) Logic control
(b) PID control
(c) Motion control
(d) Sequential control

Once the distributed control system functions are determined at the subsystem level, further functional distribution is carried

out based on the type of required control functions to achieve the optimum system performance.

The logic and/or PID control for each subsystem are localized and specific to each subsystem. Any medium level PLC can handle these functions. Therefore for each subsystem, both logic and PID control functions are allocated to their respective PLC units.

The motion control function is highly specialized and needs extensive processing and very fast loop updates. Therefore individual motion controllers are used for the control of each mechanism. Motion co-ordination and supervision of motion control is carried out by the respective PLC's to which the motion controllers are connected.

The responsibility for overall operation of the F/H system is allocated to a separate supervisory sequential controller, again using a PLC for control. This PLC communicates with each subsystem PLC via a peer level communication link for downloading operation commands and receiving feedbacks. This sequential control PLC does not require any direct field I/O connections.

Selection of Suitable Control Hardware

The PLC's for the control of subsystems F/M Carriage, F/M Head, New Fuel Transfer and Irradiated Fuel Transfer Systems handle predominantly logic control and supervise motion control. They also need only limited arithmetic processing capability and do not need large memory.

The PLC for the F/M Fluid System predominantly handles conventional process control including PID control. Therefore it does not require any special control function modules.

The PLC for Sequential Control needs a large amount of memory to handle the large number of jobs (about 20) and sequences (about 100). Therefore a PLC with large memory is required for the sequence controller.

In the CANDU 3 F/H application, except for motion control, there are no time critical control response requirements. Therefore medium level PLCs are suitable for all subsystem level controls. Only motion control functions need very fast loop update (less than 1 ms) and response times. Therefore separate motion control modules are provided and connected to their respective subsystem level control PLC's. These motion controllers have their own microprocessors and I/O and communicate to their respective PLC's by a serial communication link (see Figure-1).

Present day PLC's are highly modular and this enables the user to customise the system from the same family of hardware and software compatible modules. Therefore it will not be necessary for a station to maintain a large inventory of various types of modules.

Minimization of Communication Delays

In a distributed system it is essential to minimize communication delays. Communication takes place within the different PLC's of the control system as well as between the control system and the display computer system which provides the Human-Machine Interface.

Communication within the Control System. In F/H application, the following types of communication takes place between the PLC's:

> Communication between subsystem control PLC's. This communication is infrequent and data exchanges are limited to permissives for operational interlocks.
>
> Communication between subsystem control PLC's and the Sequential control PLC. This communication takes place continuously during the system operation in both full automatic and semi-automatic modes, but with only one of the PLC's at a time, depending on the specific task being performed. The data basically consists of sequence commands and feedbacks and therefore does not have any timing constraints.

A peer level communication link is provided for exclusively handling both the above types of communication.

Communication with the Display Computer System. Unlike in a process control environment, the mechanical status of the equipment is continually changing in the F/H environment. Therefore it is important to provide the F/H operator with the most up-to-date status of the F/H system. This requires minimization of communication delays between the control system and the display computer system.

Appropriate communication between the distributed control system and the display computer system can be achieved in a number of ways and is to some extent control system vendor specific. In the generic system configuration shown in Figure-1 a redundant communication path is provided which assumes a simple command/response type communication protocol. This system enables the display computer system to control the communication and obtain control data simultaneously via both the communication paths and from different PLC's in each path. Depending on the task being performed, the display computer can optimally schedule communication to minimize the communication delays.

Redundancy in the Control System

The following factors were considered in providing appropriate redundancy in the F/H control system:

(a) The station can tolerate unavailability of the F/H system for up to three days without the need for de-rating the reactor output.

(b) In a distributed control system, the possibility of a total system failure is remote. If failures occur they are likely to be localized and affect only the limited functionality of the system.

It is a well recognized fact that the overall reliability of a distributed control system is relatively high compared to that of a single centralized computer control system.

(c) Modern PLC's are highly modular and have extensive self diagnostics with a typical MTTR (Mean Time To Repair) of less than an hour.

(d) An appropriate amount of hardwired protective logic control will be provided, such that failure of the control system will not affect the safety related functions of the F/H system.

(e) A back-up manual control panel is proposed to be provided with limited functionality for critical control and indications in case of total failure of control system and/or display system.

Based on the above rationale, it is planned that the F/H controllers will not be provided with any redundancy, i.e., single PLC's without back-ups will be used for each subsystem control. However, redundancy is planned to be provided for the communication system which functions across the total distributed control system.

SELECTION OF A SUITABLE SYSTEM

Most of the PLCs available from established vendors in the market have almost identical control capabilities with minor variations. All of them support Relay Ladder Logic (RLL) programming. Even though RLL is widely used in regular industrial applications, it is not well suited for use in nuclear reactor on-line control operations where Software Quality Assurance (SQA) is of utmost importance. The cost of control hardware is relatively small when compared to the total cost of SQA.

Therefore it was felt that the selected system must support a programming environment which is suitable for F/H application and also helps in reducing the impact of SQA.

The following criteria was used in selecting PLC hardware with a suitable programming environment, for use in a pilot system evaluation:

(a) As the F/H operations are predominantly sequential in nature,the programming environment should support SEQUENTIAL FUNCTION CHARTS (preferably based on the GRAFCET standard) for sequential control.

(b) The programming language should be a high level language and support both logic and arithmetic processing in a similar and integrated fashion.

(c) The programming language should facilitate structured software design and preferably support Object Oriented Programming concepts.

(d) The programming environment should support on-line and off-line debugging and troubleshooting.

(e) The programming environment should support software test tools and system simulation tools.

(f) The programming environment should support automatic documentation.

EXPERIENCE WITH A PILOT CONTROL SYSTEM

Early in the CANDU 3 conceptual design phase it was decided to carry out evaluation tests on some PLC hardware and software. We selected one of the commercially available PLC's which broadly met our F/H control system requirements. This system is currently being used for the control of the Fuelling Machine used in a laboratory demonstration of single ended refuelling operations. As this particular Fuelling Machine had conventional oil hydraulic drives, we did not use Motion Controllers for drive position control. The hydraulic drive position control was implemented in the main PLC itself.

The PLC was used for performing the following functions:

(a) Sequential control of the Fuelling Machine.
(b) Position control for B Ram, Latch Ram, C Ram and the Magazine.
(c) B Ram force control.
(d) Control of Feelers, Retractors, Stops and all process valves.
(e) Some of the logic interlocks.

(f) Monitoring of the status of the Fuelling Machine and its Fluid system.

A remote I/O system was used with both analog and digital signals. An IBM compatible PC-AT used to provide the Human-Machine Interface, was connected to the PLC via a RS-232 communication link. The control software was developed on a PC-AT and then down loaded to the PLC. The vendor supplied CASE (Computer Aided Software Engineering) tool was used for software development.

Most of the control software was based on Sequential Function Charts (SFCs) using a high level language (similar to state logic control languages). An example of a SFC structure for a typical F/H sequence with Latch Ram position control is shown in Figure-2.

The pilot system evaluation has demonstrated that Sequential Function Chart based programming is ideally suited to programming sequential operations (Jobs, Sequences and Steps) which are a cornerstone of the automatic control of F/H operations.

Considering the fact that a single PLC was used for performing all the above control functions, the performance of the system was found to be quite satisfactory. We were able to demonstrate good position control of the Fuelling Machine drives. The PLC scan time for performing the total control is about 50 milli seconds which is shorter than the position control loop update times in current CANDU 6 control computers.

Our experience has shown that by using suitable CASE tools, the program coding time can be substantially reduced (almost to 25% of the time taken for a CANDU 6 system). This also considerably reduces the time required for program review, verification and validation functions. Experience to date has also confirmed that with a PLC based system, F/H control system software development can be carried out by staff who may not be highly skilled in computer software techniques.

APPLICABILITY OF CANDU 3 DESIGN CONCEPT TO EXISTING STATIONS

The dedicated distributed control system concept designed for the CANDU 3 F/H system is equally applicable to any existing CANDU 6 F/H system with minor changes to accommodate the current CANDU 6 use of oil hydraulic drives. In this case the subsystem PLC can also handle the respective drive controls directly (as in the pilot control system).

The software for the most important control functions such as sequential control and drive position controls for the Fuelling Machine have already been tested and proven in the pilot control system. This proven software is directly applicable to existing CANDU 6 F/H systems.

SFC for a typical F/H Sequence

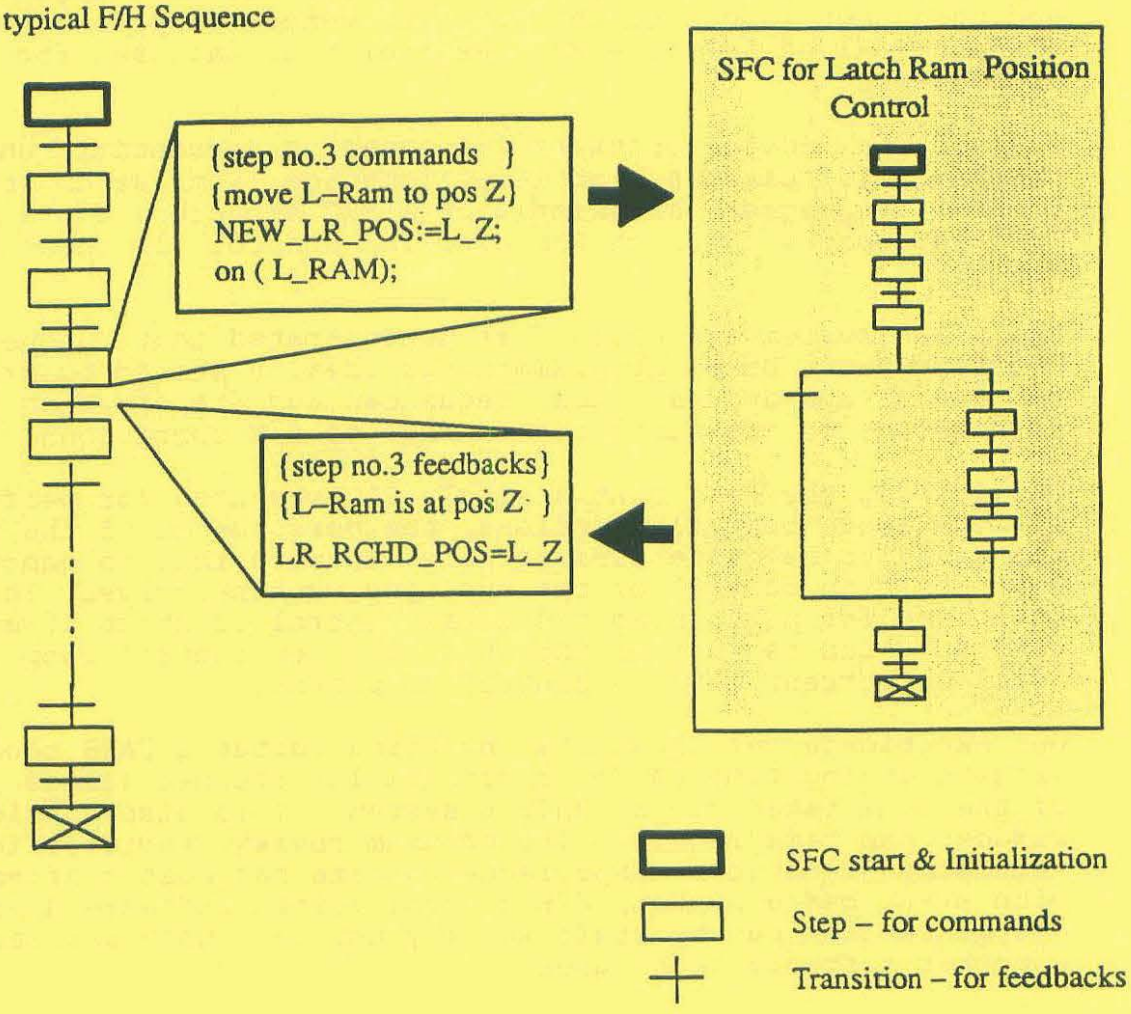

Figure – 2

Examples of Sequential Function Charts for a typical F/H sequence and Latch Ram Position Control

When a distributed control system configuration is used for an existing CANDU 6 F/H system, the scan time for each PLC is expected to be less than 25 milliseconds, which can provide excellent system response.

Current experience during Wolsong II detail design has shown that equipment such as control relays and current alarm units are no longer available from our traditional suppliers. Because replacements involve extensive design activity to accommodate changes such as terminal numbers and physical size, the use of a PLC based dedicated distributed control system becomes more and more desirable as a retrofit into existing CANDU-6 stations.

CONCLUSION

The CANDU 3 F/H control system design described in this paper provides the following advantages when compared to earlier CANDU 6 systems.

(a) Elimination of full back-up control panel and the associated discrete hardware for controls and indications. This results in saving in capital, engineering, construction and site operation costs.

(b) Elimination of backup control hardware and panels results in saving of space in the control room as well as in the control equipment room.

(c) The selected distributed control system architecture can facilitate geographical distribution of PLC and motion control hardware resulting in additional savings in the cost of cabling.

(d) By providing highly functional distribution of controls, the cost of overall software quality assurance can be reduced by applying higher level of SQA only to those functions which require it, rather than to the whole F/H system.

(e) By selecting a suitable programming environment and software engineering tools, the implementation of SQA becomes relatively easier.

(f) By using a higher level programming language, the person-years required for control program development is considerably reduced.

This also facilitates better software maintenance, quicker software modifications and improvements by the station operating staff.

(g) Enhanced operational flexibility due to independence from station computer control system.

The pilot system evaluation has shown that the F/H control system can be implemented with PLC based hardware. The use of a dedicated distributed system for control of F/H operations has been shown to be both feasible and desirable for enhancing F/H operational flexibility. In addition, the use of a PLC based system can provide design flexibility for accommodating changes due to design revisions and/or obsolescence of equipment.

The F/H system design and configuration developed for CANDU 3 is generic in nature and can be adopted as a standard for future CANDU stations.

SFC for a typical F/H Sequence

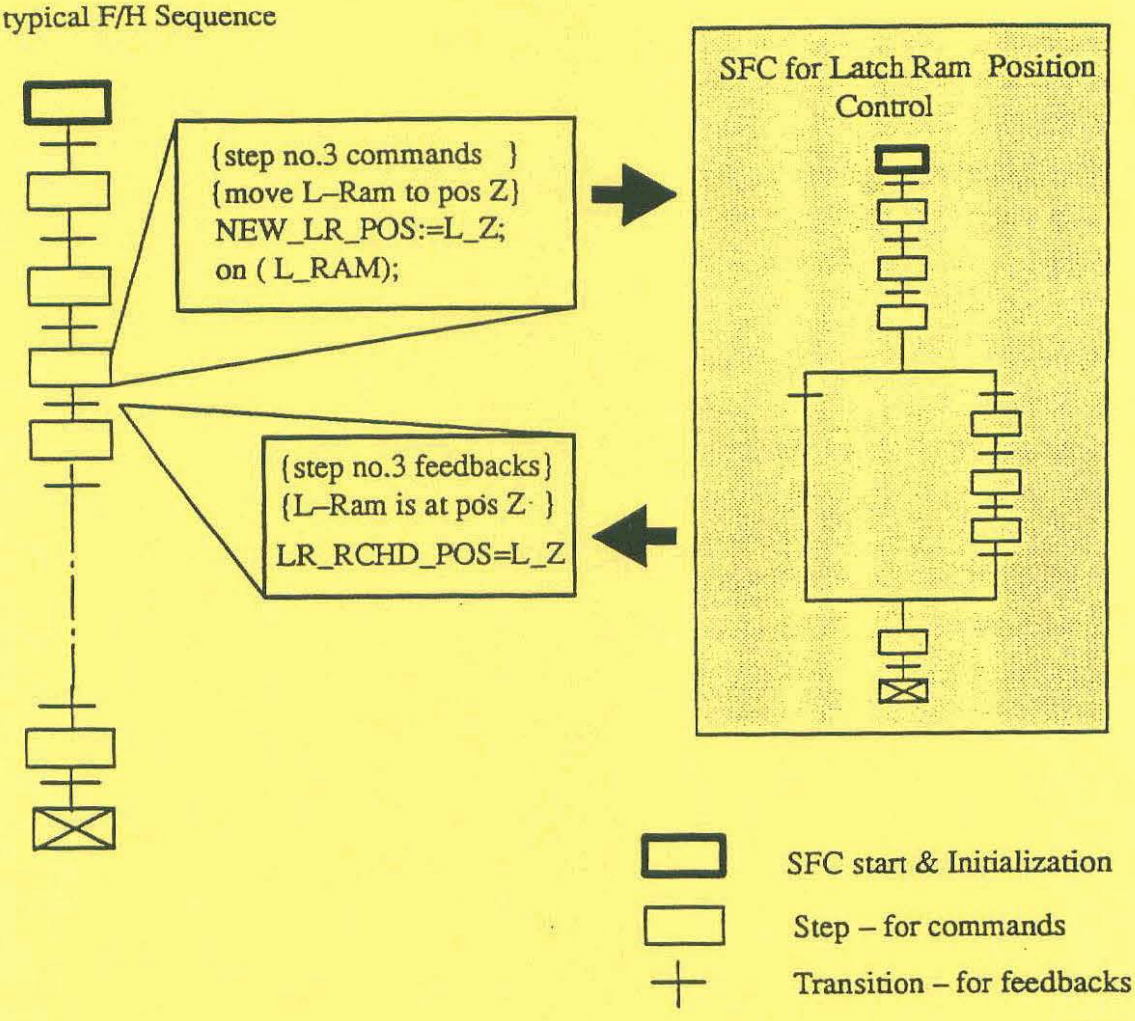

Figure – 2

Examples of Sequential Function Charts for a typical F/H sequence and Latch Ram Position Control

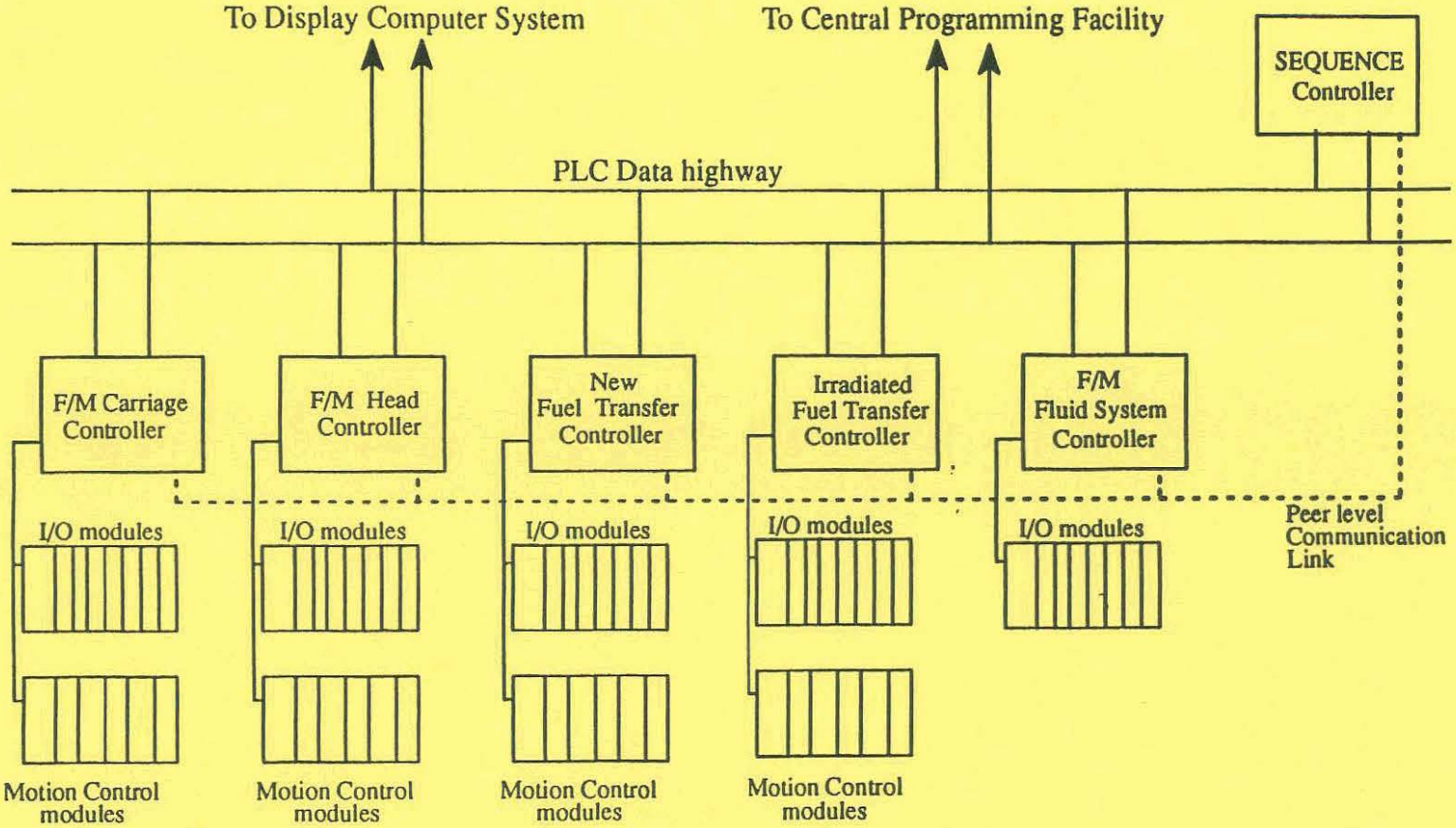

Figure – 1

Distributed Control System configuration for CANDU–3 Fuel Handling System