VVER NPPs
Fuel Handling Machine Control System

G. Mini, G. Rossi, *Ansaldo Nucleare*

M. Barabino, M. Casalini, *ABB*

I. INTRODUCTION

In order to increase the safety level of the fuel handling machine on VVER NPPs, Ansaldo Nucleare was asked to design and supply a new Control System.

Two FHM Control System units have been already supplied for Temelin NPP and others supply are in process for the Atommash company, which has in charge the supply of FHMs for NPPs located in Russia, Ucraina and China.

The Fuel Handling Machine (FHM) Control System is an integrated system capable of a complete management of nuclear fuel assemblies.

The computer-based system takes into account all the operational safety interlocks so that it is able to avoid incorrect and dangerous manoeuvres in the case of operator error.

Control system design criteria, hardware and software architecture, and quality assurance control, are in accordance with the most recent international requirements and standards, and in particular for electromagnetic disturbance immunity demands and seismic compatibility.

The hardware architecture of the control system is based on ABB INFI 90 system. The microprocessor-based ABB INFI 90 system incorporates and improves upon many of the time proven control capabilities of Bailey Network 90, validated over 14,000 installations world-wide [1].

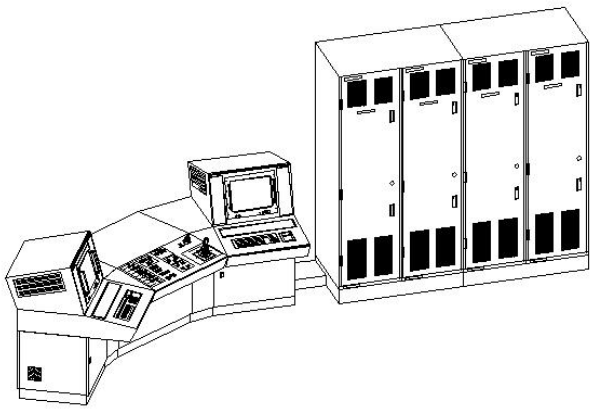

Figure 1 - This figure represents a typical configuration of the Fuel Handling Machine Control System

The control system complies all the former designed sensors and devices of the machine and markedly the angular position measurement sensors named "selsyn" of Russian design. Nevertheless it is fully compatible with all the most recent sensors and devices currently available on the market (for ex. Multiturn absolute encoders).

All control logic were developed using standard INFI 90 Engineering Work Station, interconnecting blocks extracted from an extensive SAMA library by using a graphical approach (CAD) and allowing and easier intelligibility, more flexibility and updated and coherent documentation [3], [4].

The data acquisition system and the Man Machine Interface are implemented by ABB in co-operation with Ansaldo. The flexible and powerful software structure of 1090 Work-stations (APMS - Advanced Plant Monitoring System, or Tenore NT) has been successfully used to interface the operator with the control of the fuel handling machine [2].

II. AUTOMATION LEVEL

The degree of automation of the control system is basically addressed to improve the automation level of the performed tasks helping the operator in the machine management. A workstation based operator interface basically allows the following functions:

- real time control of all the functions of the refuelling machine, by means of graphic displays depicting a synthetic representation of the refuelling machine current status in harmony with the physical reality;
- management of a predefined refuelling strategy by means of graphical maps depicting the fuel assemblies inside the reactor, the pools and the container, and software tools for the history of all the actions performed;
- management of the control system diagnostic and alarms.

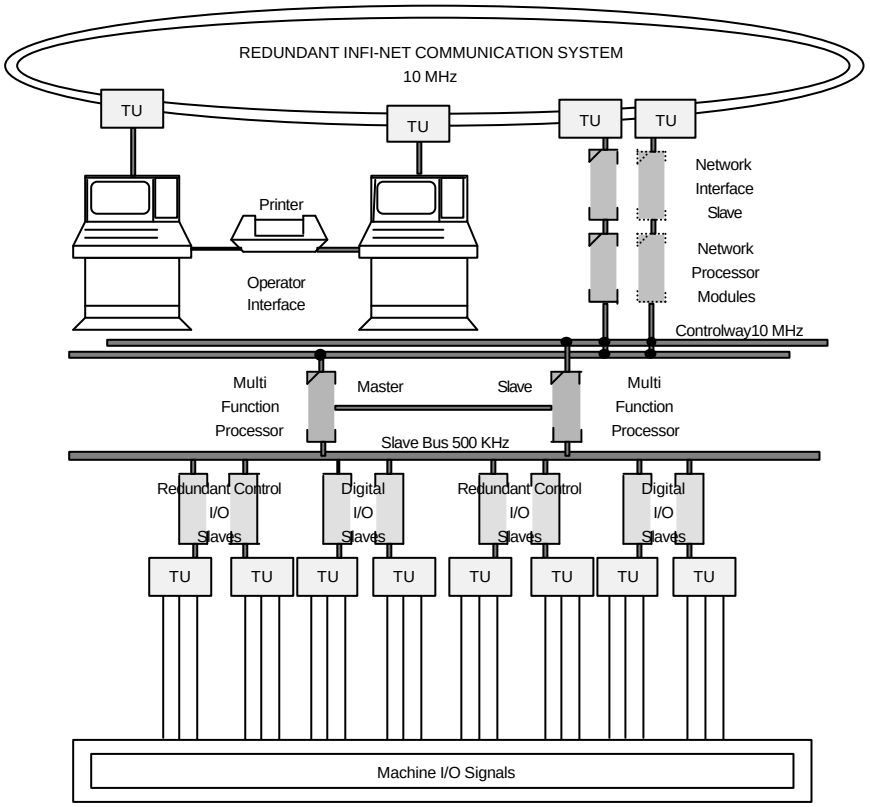

Fig. 2 Control System Architecture for Temelin Plant.

III. SAFETY AND AVAILABILITY

Automation strategies are implemented by means of microprocessors, which are in redundant configuration: the first one performs control strategies, while the other one follows and updates itself ("hot backup"). If the system diagnostic detects a failure in the master controller, the second one takes over the process control without waiting time since it is perfectly in phase.

Input security is provided by the Multi-Function Processor module to handle the cases of bad or unavailable input points. Both on board inputs and inputs acquired over the bus have a status associated with them. This point status is used to provide security based on the good quality of the input points. This logic may activate various alarm conditions and control backup strategies.

If both Multi-Function Processor modules fail, these additional safeguards are present: analog control outputs go to 0%, 100%, or hold; digital control outputs go to default values; this logic may activate the trip block to cause a module switch-off.

The system also performs self-diagnostics at the various system levels (i.e., module, process control unit, communication system, and operator interface). When a failure is detected by the control system this latter safely stops the machine, then it localises the failure allowing a board substitution for maintenance if needed, checks if it is possible a restart and allows the operator to restart the machine.

The control system is able to avoid incorrect and dangerous operations both in the case of operator error and in the case of single failure event. The maintenance of the control system requires, in the worst case, the substitution of the electronic boards, or of the power driver boards. The set of the possible spare boards is little and there is no need of personalizations and adjustments: all is done automatically by the computers at the power-up.

Each cabinet of the control system is equipped with fully redundant power supply system. Each supply module is backed up by another stand-by module having the same power. The commutation is performed without affecting the control functions being power supplied.

The system architecture involves the use of highly rationalised information transfer channel in order to guarantee the necessary information transfer speed: the concentration in well defined control systems portions of all the strategies concerning a complete functional unit minimises the information flow from and to the other system portions which control other functional units.

Message transmission over the data way is byte-oriented, and checks such as byte parity and message checksums ensure message security. Module bus communications are capable of transferring messages with less than one undetected error per 100 years of operation.

Configuration and tuning parameters which customise the controllers for specific applications are stored in non volatile RAM Memory (NVM) battery backed. BATRAM memory also eliminates the need for reloading configurations from a core central processor on power up of a distributed controller.

All the equipments have been selected to be compatible with the environmental conditions specified (normal and emergency) and among high quality level products (technology proven by similar successful applications).

A seismic analysis of the control system has been performed in order to ensure that no damage could be caused to fuel or any other safety grade equipment.

IV. CONROL SYSTEM HARDWARE ARCHITECTURE

According to the INFI 90 general description explained in the above paragraphs, the Figur 3 represents the general scheme of the FHM control system architecture.

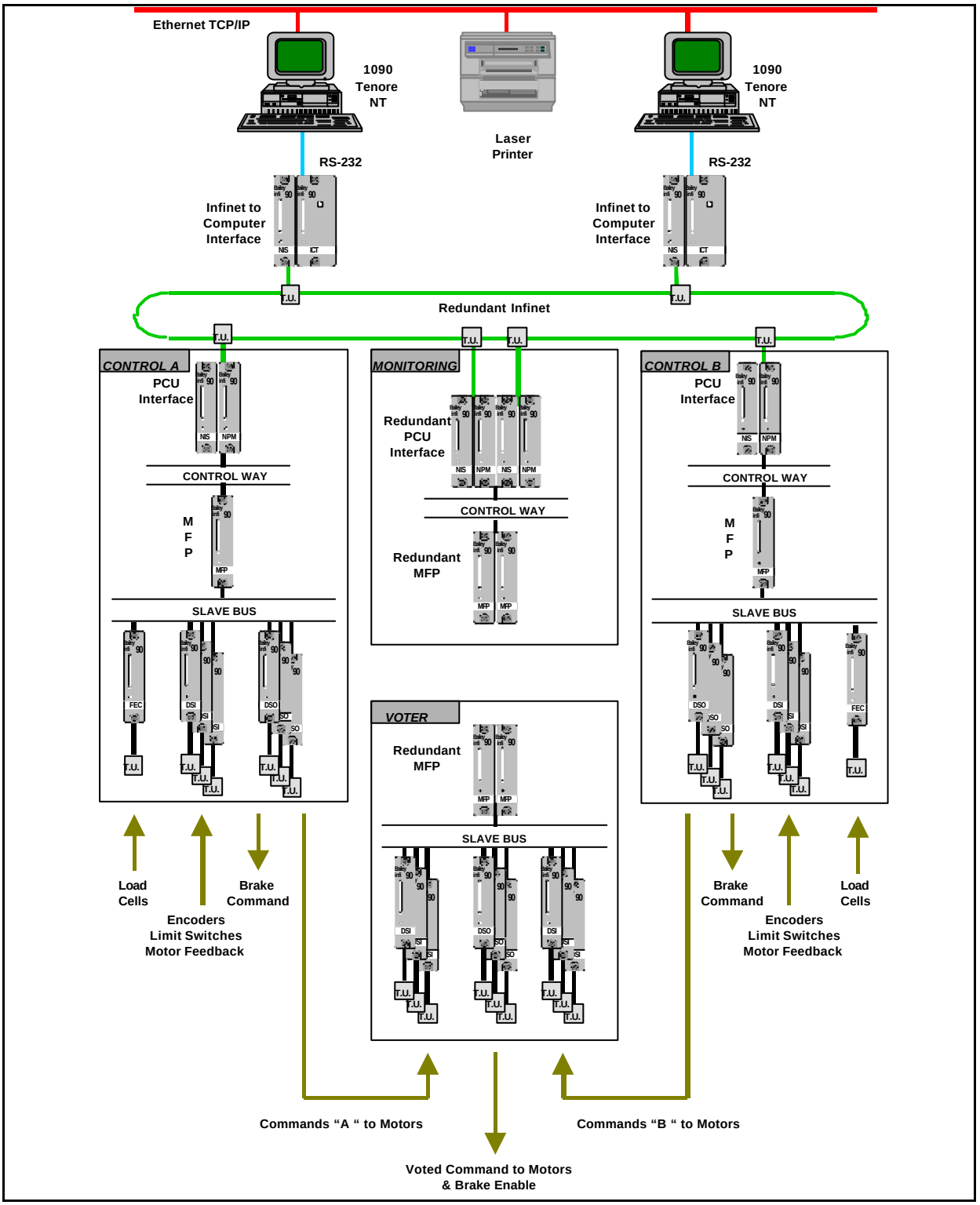

Figure 3 - Control System Architecture – New generation

It is based on a couple of MFP, in master-slave configuration (hot backup), which manages the I/O sub-system and the Man Machine Interface, both in redundant configuration.

The automation is based on INFI 90 Open ***Process Control Units (PCU).*** Physically, these consist of cabinets housing power supplies, controller modules, I/O slaves and field termination units. Functionally, the PCU is the location where all modulating (analog) and sequential control is performed. Data acquisition, i.e., multiplexing of analog and digital signals, is also accomplished here.

Internally in a PCU the controller module ***Multi Function Processors (MFP)*** gather data from I/O devices via I/O slaves across the Slave Bus. Field I/O signals are terminated on either ***Termination Units***.

To transmit data to/ from Operator Interfaces, a redundant high speed digital communication system is used, called ***Infinet***.

This is a loop-ring type architecture that permits extensive geographic distribution.

There is no traffic director needed to run the system. The nodes form an all master system, eliminating single points of failure that can take a system off-line. Any node can transmit and receive simultaneously, even in a two-node system. Since there is no mastership, node start-up/shut-down is strictly localized and can be done without affecting the balance of the system.

The ***Network Process Module (NPM)*** and the ***Network Interface Slave Module (NIS)*** are the interface between the Controlway and the Infinet. They can be implemented as a redundant pair. The Infinet consists of dual redundant fiber-optic cables connected to the NIS termination unit.

Data is reported by exception in the system. Each process input has associated with it a set of exception reporting limits. Whenever a signal change by more than a designated dead-band, its new value is reported to all parts of the system which require the information.

A maximum reporting time is specified to ensure that data is reported periodically even if there is no change. Also, a minimum reporting time is specified to ensure that a single rapidly changing input does not saturate the system with exception reports. This process reduces the repetitive transmission of unchanging data while increases response time to data that are changing.

The Infinet system provides to data exchange via serial RS-232 interface to the Operator Stations ***1090 Tenore NT*** based on PC. The 1090 Tenore NT stations are linked via Ethernet.

V. MAN MACHINE INTERFACE

A fundamental feature of the control system is the availability of a sophisticated operator interfaces located at the various control hierarchy levels. In case of malfunction, these interfaces enable a diagnostic and soft system degrading, always under the operator's control and in high safety conditions.

The Man Machine Interface is based on a couple of Industrial PC Work Stations in redundant configuration. The MMI allows communication with the whole system or a particular process module. The Software **Tenore NT** runs on each PC Work Station to perform data acquisition from the field, to store information onto data bases, to process data for MMI displaying, to send commands towards the field.

MMI monitors process activities, displays diagnostic, alarm and trend information and produces system documentation. Combined with a printer, the MMI generates logic control drawings, configuration drawings, module lists, specification lists, and system variable trends. While on-line, connected to the process system, the MMI provides real-time tuning and troubleshooting.

The MMI manages the following operational modes for the machine.

Graphical Operator Interface

Several graphical pages are designed to accomplish the three above mentioned tasks. In particular the following representations are included.

Top View

This page displays a representation of the entire area involved in movements (zoom is possible on pools and reactor areas). It is composed by some fixed parts (i.e., the drawing of the serviced area outline) and a window containing the values, continuously updated, of all the motion variables (i.e. bridge-trolley and Main Mast coordinates, etc.).

During the handling phases the following "dynamic" information are displayed and updated on the screen:

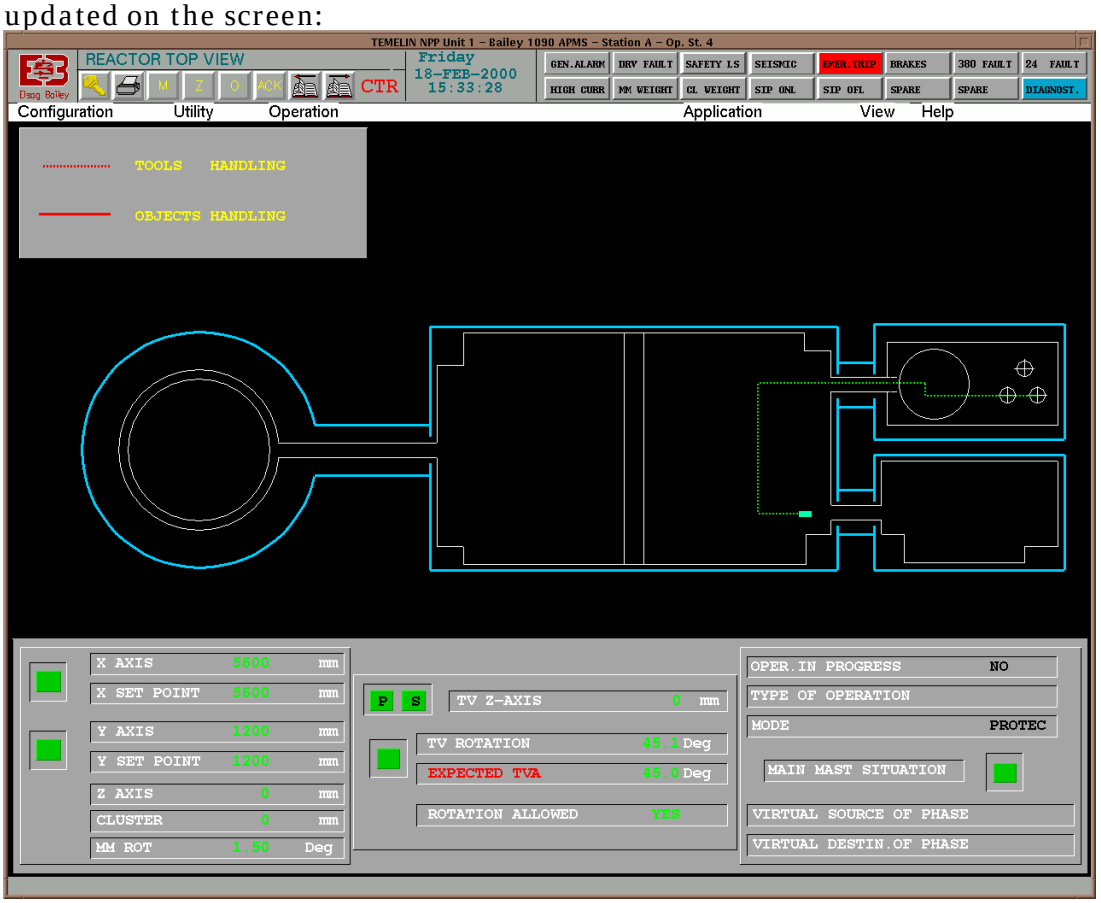

Figure 4 – Operator display Top View

- *At the beginning of each handling operation, the trajectory that the bridge-trolley will follow in order to perform the required operation (in the form of segments).*

- *During handling operations, it will be shown the bridge-trolley position inside the serviced area according to the real movement (following the x, y coordinates acquired by the system).*

Z View

This page contains the following data:

- *Load cell: the updated values of Main Mast, Fixing, Cluster, Tearing load cells are shown in digital and bar chart format.*
- *Main Mast: coordinates on Z axis is displayed and updated in digital format; rotation angle is displayed and updated in digital and pie chart format.*
- *TV Mast: coordinate on Z axis is displayed and updated in digital format; rotation angle is displayed and updated in digital and pie chart format*
- *A drawing of Main Mast is updated, showing the movement along Z axis of the two mobile elements and of the object which is actually hooked.*

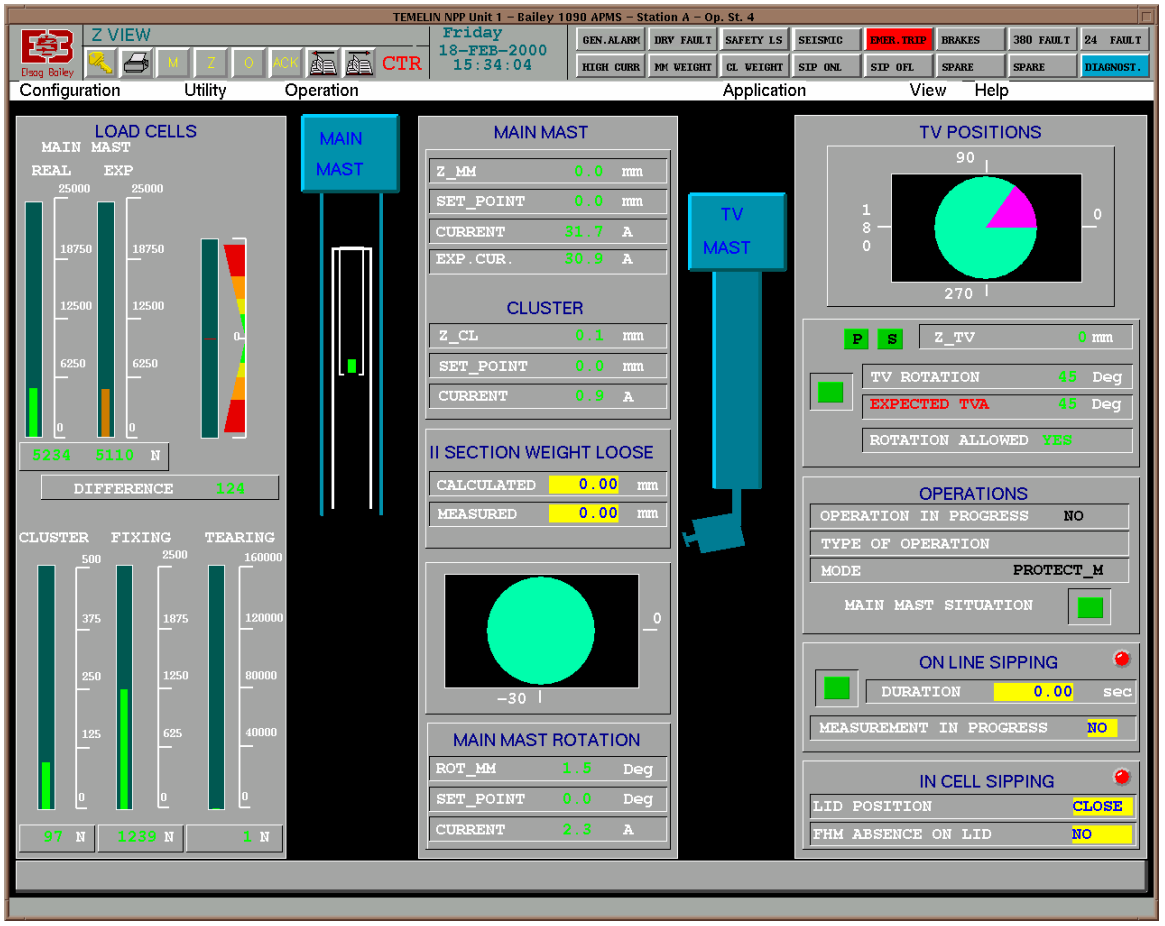

Figure 5– Operator display Z View

Detailed Pages

From the TOP VIEW page it is possible to zoom-in on any specific working area:

- *Reactor*
- *Pool 1*
- *Pool 2*

In these pages the objects placed in every working position and their relative status are shown for every coordinate.

In particular it is shown the possible status for the cassettes containing fuel element using one color for each different working feature (i.e. empty, fresh, damaged, exhausted, in-use).

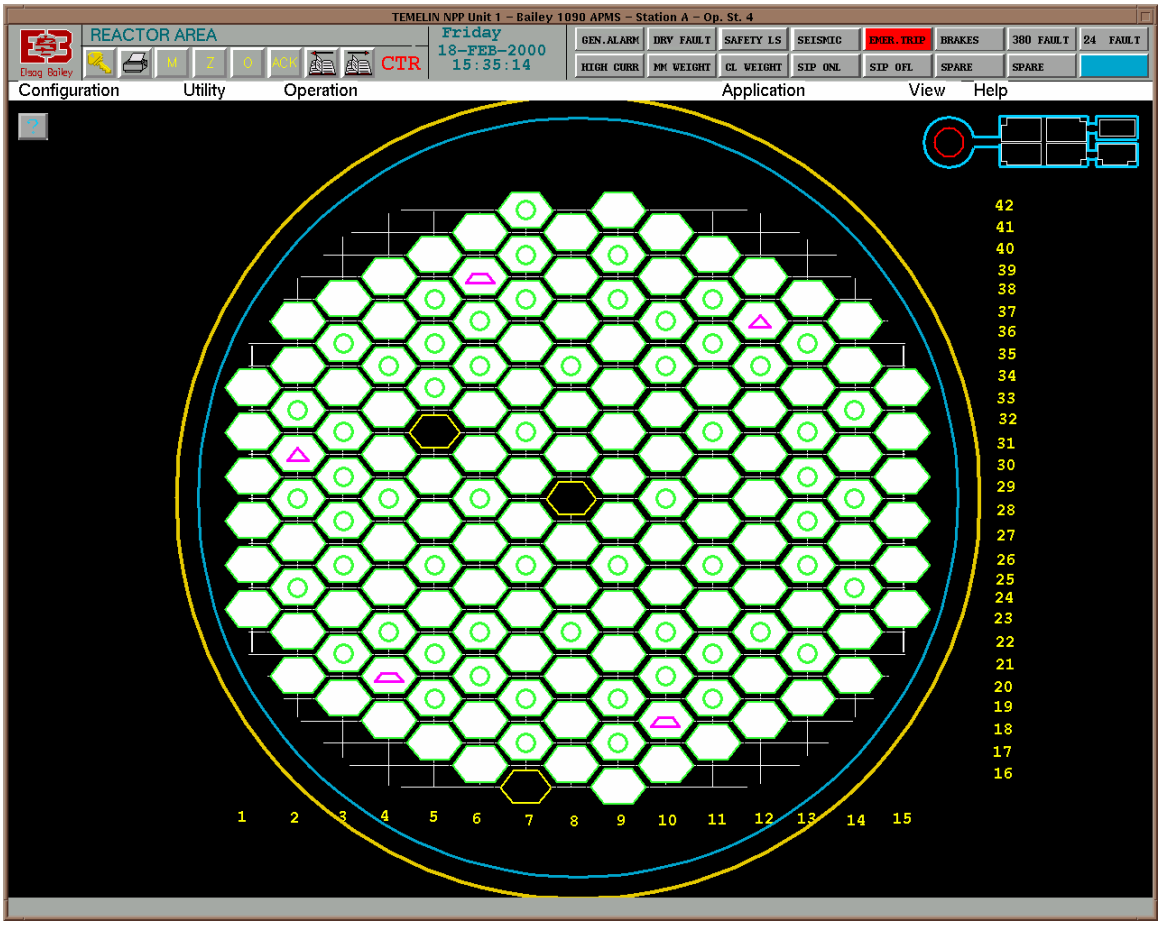

Figure 6 – Operator display for the Reactor working area

Movement Pages

It is present one page for each movement.

Typically the following information are shown:

- *Position (value, set point).*
- *Movement variables (motor current, brake energised, maximum speed, actual speed, reference speed).*
- *Limit switches (safety, forward, back).*

The following variables are displayed in trend format:

- *Motor current.*
- *Reference and actual speed.*
- *Position set-point and actual position.*
- *Load cells values.*

VI. OPERATING MODES

The control of the machine is performed in all the below described operating modes.

A definition of the terms hereinafter used is preliminary reported.

The **manoeuvre** consists in:

- **Static consents** *predetermined constraints based on values coming from the field, which have to be fulfilled for starting the manoeuvre*
- **Dynamic consents** *predetermined constraints based on values coming from the field, which have to be fulfilled during the manoeuvre*
- **Stop conditions** *constraints on the operating conditions of the control system hardware*
- **Starting command** *action performed by the manoeuvre for starting the actuator*
- **Stop command** *action performed by the manoeuvre for stopping the actuator*
- **Maximum execution time** *maximum allowable time for manoeuvre completion both in automatic and semiautomatic operating modes; after this time slice the manoeuvre shall be stopped in any case*

The **sequence** consists in a set of maneuvers in chronological order of execution. The start form of the maneuvers depends on the operating modes.

The **phase** consists in all the sequences for picking-up and depositing.

The **campaign** consists in a set of sequence necessary for the refueling operation. The control system will record a campaign to perform in a specific file: **phases file**. This file contains an header showing database status and several records containing the data of each phase.

Automatic Operating Mode

This operating mode is the standard one of operation. The operator manages the machine by means of predetermined sequences. In the same time the control system performs:

1. *The check on the right course of the sequences and the control of the*

consistency between the operator requests and the data recorded in the phases file. If any negative results come out, the requested sequence is refused or interrupted.

2. *The expansion of the sequence in a orderly set of elementary manoeuvres.*

3. *The check for each manoeuvre of the existence of the necessary consents to start the manoeuvre itself.*

4. *The execution of the commands for each manoeuvre.*

5. *The real time check during the execution of each manoeuvre of the existence of the necessary consents; in case of error the manoeuvre shall be stopped and the control shall wait an operator decision.*

6. *The update of the phases file if the phase is ended without any errors.*

Semiautomatic Operating Mode

The operator manages the machine by sequences: each sequence consists in the same manoeuvres performed in the automatic operating mode with the same chronological order, however for each manoeuvre is requested the operator consent. In the same time the control system performs:

7. *The check of the sequences right course and of the consistency between operator requests and data recorded on the phases file. If any negative results come out, the requested sequence is refused or interrupted.*

8. *The expansion of the sequence in a orderly set of elementary manoeuvres.*

9. *The proposal to the operator for the next manoeuvre, waiting his consent.*

10. *The check for each manoeuvre of the existence of the necessary consents to start the manoeuvre itself.*

11. *The execution of the commands for each manoeuvre.*

12. *The real time check during the execution of each manoeuvre of the existence of the necessary consents; in case of error the manoeuvre shall be stopped and the control shall wait an operator decision.*

13. *The update of the phases file if the phase is ended without any errors.*

Protected Manual Operating Mode

The operator manages the machine by elementary manoeuvres chosen by himself. In this case the operator can bypass the adequacy with the phases file. In the same time the control system performs:

14. *If the adequacy with the phases file is requested, the check of the sequences right course and of the consistency between operator requests and data recorded on the phases file. If any negative results come out, the requested sequence is refused or interrupted.*

15. *Waiting for the operator choice and his next request of execution.*

16. *The check for each manoeuvre of the necessary consents, before its starting.*

17. *The execution of the commands relevant to the single requested manoeuvre, until the operator maintains the request or failure happens; In case of error the control system waits for an operator decision.*

The operator will update the phases file.

Simulator Mode for Training

The FHM control system is improved with a full replica training simulator. Control logic that is developed for the real machine is downloaded unchanged into simulator. The operator work station is equipped with hardware dedicated to the simulator. Simulator design will ensure high fidelity and profitable operator training. Furthermore, because the simulation system uses the actual plant control logic, processor and operator interface, it can easily be upgraded to match the real plant throughout its life.

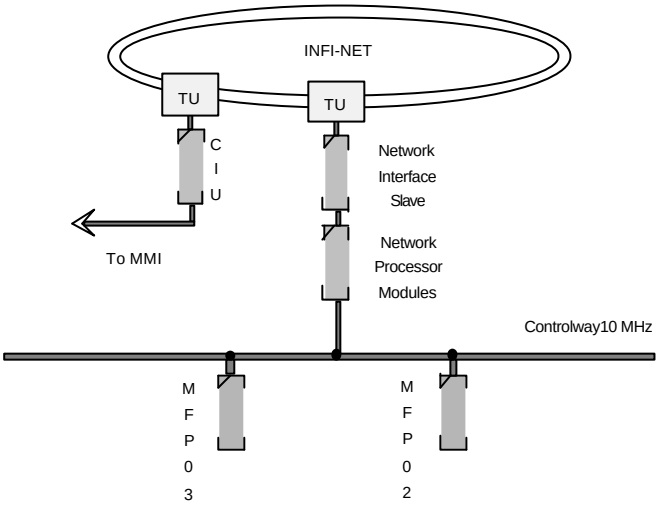

Fig. 7 Simulator hardware architecture.

VI. FUNCTIONAL AND ENVIRONMENTAL FEATURES SUMMARY

The following table summarizes some functional and environmental features of the fuel handling machine control system.

Electromagnetic Compatibility	**EN 61000-4-1** **EN 61000-4-2** **EN 61000-4-4** **EN 61000-4-5** **EN 61000-4-8** **EN 61000-4-9** **EN 61000-4-10** **EN 61000-4-11** **EN 61000-4-12**	**CEI** **55022** **CEI** **55011** **ENV 50140** **ENV 50204** **ENV 50141**	**EN** **EN** **EN** **IEC 255-5** **IEC 60**
Power supply requirements	**196¸264 VAC**	**47¸63 Hz**	**5% total harmonic distortion**
Period between failures	**10⁸ hours**		

VI. QUALITY ASSURANCE

The Quality Assurance Program of ANSALDO established to enforce the quality policy of the Division in relation to the activities of design, fabrication, installation, testing, start-up, operation, maintenance and commissioning of plants, system and components relevant to safety and/or to operational reliability, has been defined in a way which satisfies the prescription of the following documents:

- *ENEA Technical Guides on GQ matters issued up to the date of the revision of this Manual and in particular Guide N.os 8, 22, 25 inclusive;*
- *ANSI/ASME NQA1 Ed. 1986 - Quality Assurance Program Requirements for Nuclear Facilities;*
- *ISO 9001 (UNI EN29001) - Quality systems - Model for quality assurance in design/development, production, installation and servicing;*
- *UNI N. 8450 - Criteria prescriptions and recommendations for a Quality Assurance Program;*
- *CS N. 50-C-QA - Code pour la Sureté des Centrales Nucleaires. Assurance de la Qualité;*

and it periodically re-examined and updated.

.