ESTABLISHMENT OF A CONTROL PHILOSOPHY FOR THE PEBBLE BED MODULAR REACTOR

FJE Laubscher*, HA Grobbelaar**

** Pr.Eng, MSAIEE, Software Systems Engineer, PBMR (Pty) Ltd.*
*** Pr.Eng, Systems Engineer, PBMR (Pty) Ltd.*

Abstract: PBMR (Pty) Ltd. is in the process of developing a demonstration module of a new generation high-temperature gas-cooled nuclear power plant. This paper discusses the overall software structure for the Operational Control System as well as the development of the Operational Control System Software Specification from the User Requirement Specification.

The functions of the Pebble Bed Modular Reactor demonstration module are divided into logical and functional structures according to the development specifications for the plant subsystems. The control specification follows the same structure, but with the emphasis on the operational aspects, in order to ensure efficient integration of the Human-systems Interface and to enhance operational benefits. *Copyright © 2003 IFAC.*

Keywords: Process control, Plant automation, Control system architecture

1. INTRODUCTION

A substantial part of the intellectual property of the Pebble Bed Modular Reactor (PBMR) Demonstration Module will be captured in the functional design of the Operational Control System (OCS). For this reason, the OCS software is developed internally by PBMR (Pty) Ltd.

During the project design phase, the control specifications provide outlines for the control of all plant systems and subsystems, using a common methodology. This methodology establishes a control hierarchy with clearly defined levels of functionality, and it simplifies the development and Verification and Validation (V&V) processes.

After implementation, in the operation and maintenance phases of the PBMR Demonstration Module, the control system structure as well as the tested control modules and functions should be maintainable with ease in order not to jeopardize the integrity of other parts of the system.

2. DEVELOPMENT PROCESS

The PBMR Automation System (AS) consists of the Operational Control System (OCS), the Equipment Protection System (EPS), the Reactor Protection System (RPS) as well as other systems used for information, control and protection purposes.

The AS specification is derived from the PBMR Demonstration Module Specification, from which the OCS hardware and software specifications are derived. Functionally, the Subsystem Development Specifications are used to develop functional control specifications for plant subsystems. These functional Control requirements are implemented on the OCS.

The OCS control philosophy is based on the following main statements within the AS Specification:

- *Requirement #1*: 'The plant shall be automated as far as practically possible, to ensure all plant production goals can be met with a minimum number of operators, taking due consideration of safety, investment protection and human factors.'
- *Requirement #2*: 'The control and automation system shall be designed primarily in terms of structure and interaction based on a functional viewpoint of the plant, and not physical systems.'
- *Requirement #3*: 'No single random fault in the entire instrumentation, control & automation system shall cause a load loss, forced outage or unit trip.'

In order to satisfy *Requirements #1 and #3*, reliability and availability requirements were used to allocate control functionality to Distributed Controllers, called Automation Units (AU).

Requirement #2 is satisfied via a design of a functional hierarchy of group controllers. This hierarchy of group controllers also minimizes operator interaction, which implies less operational staff (*Requirement #1*).

The OCS is not classified as a nuclear safety system, but it is nevertheless important to minimize the risks arising from challenges to the EPS and RPS. The principles described in the references, are used in the software development process in order to satisfy *Requirement #3*.

The adequacy of the functional design is confirmed during Hazard and Operability (HAZOP) studies, where initiating events are identified and the resultant OCS actions analysed for automated mitigating action on the detection of unacceptable deviations from operating points.

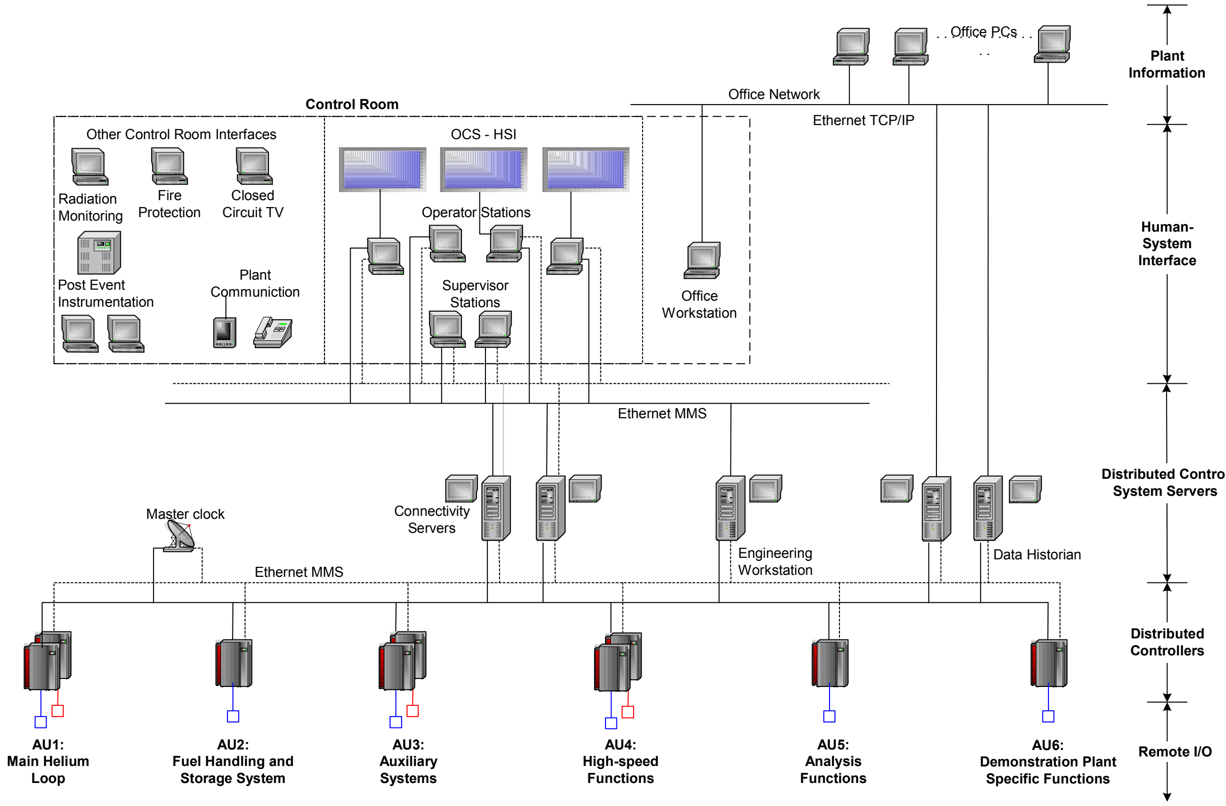

Fig. 1: OCS hardware architecture for the PBMR Demonstration Module.

In general, 1) The operator should be able to recover the operation successfully after the failure of a single control system element; 2) No single failure within the OCS should initiate a request for the EPS or RPS to react; and 3) The OCS should be able to maintain reactor cooling at all times (a power plant production requirement and not a safety requirement).

The implementation of the plant functions is finally validated on an engineering simulator against approved Acceptance Test Procedures (ATP).

3. HARDWARE ARCHITECTURE

3.1 Overview

The OCS hardware structure is divided into the following levels, as given in Fig. 1:

a. *Plant Information*: Provision is made to provide plant information to management and engineering staff by means of an open standard via the intranet to their computer systems (e.g. Maintenance system).

b. *Human-system Interface:* The Human-system Interface (HSI) is situated in the control room and includes an operator Task Support System (TSS).

c. *Distributed Control System Servers and Controllers*: An industrial Distributed Control System (DCS) was chosen for plant control. Apart from the AS Requirements, mentioned above, another criterion for the choice of DCS was for the DCS to have a software emulation package available. The emulation package, running on a personal computer, is used for software development as well as for the training simulator, where the same software used for the OCS, is used for simulating the OCS.

d. *Remote Input/Output Units*: Conventional analogue and digital input and output signals are wired to the Remote Input/Output (I/O) Units, which are placed as close to the source as possible, to reduce cabling. The Remote I/O is connected to the AUs with Profibus-DP networks, as shown in Fig. 2.

e. *Fieldbus*: Profibus-DP, an international open standard, is the chosen fieldbus. Profibus-DP connects AUs with distributed I/O, intelligent field devices and Motor Control Interface Units (MCIUs). Modbus is used for communication with protection relays, not supporting Profibus-DP. Fig. 2 shows these connections.

3.2 Automation Units (AU)

The AU design is based on the single failure criterion as well as processor speed requirements. The following AUs are defined:

- *Automation Unit 1 - Main Helium Loop*: All plant functions necessary for continuous operation of the reactor and power conversion unit, and for which normal processor cycle times are required, reside under this AU.
- *Automation Unit 2 - Fuel Handling and Storage System*: The Fuel Handling and Storage System (FHSS) does not have to run continuously. It also does not have an immediate effect on the plant performance in real time. A stand-alone AU is proposed with a non-redundant controller

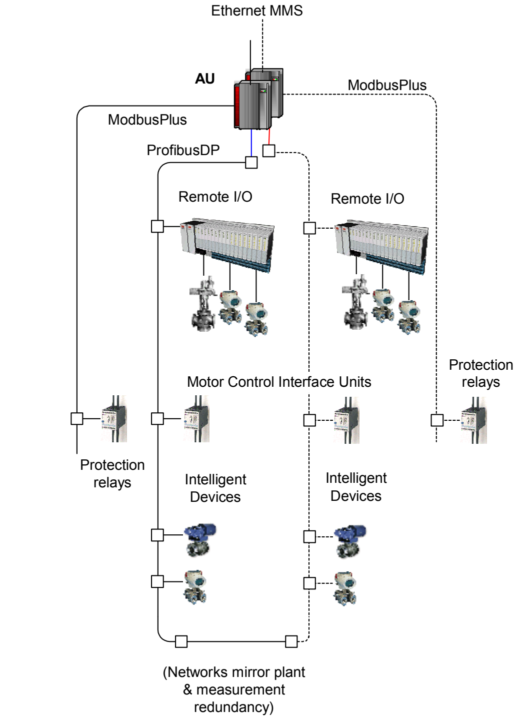

Fig. 2: Distributed I/O and fieldbus configuration.

- *Automation Unit 3 - Auxiliary Systems*: All auxiliary functions, including the Helium Inventory Control System (HICS), are controlled with this AU. From an operational revenue perspective, redundant controllers are proposed for this AU, as the HICS plays an important function in the load-following and Automatic Generation Control functions, supplying electricity to the national grid.
- *Automation Unit 4 – High-speed Functions*: The PBMR Demonstration Module has a few high-speed control functions (e.g. Compressor control, Turbine control, etc.) The aim is to standardize on AU controllers throughout the design – a separate AU for the high-speed functions makes it possible to use the same controller with a minimum set of control functions at a much higher cycle time.

  Redundant controllers are proposed for the high-speed AU.
- *Automation Unit 5 - Analysis Functions*: Analysis functions within the PBMR Demonstration Plant have the following characteristics: a) Special interfaces to analysers and b) Sampling at different points, utilizing changeover valves. The analysis functions are not critical for the operation of the plant, and the software functions associated with it reduce the main controller performance. A separate stand-alone AU is thus proposed with no redundancy.
- *Automation Unit 6 - Demonstration Module Specific Functions*: The PBMR Demonstration Module is fitted with additional instrumented in order to characterize the plant and to validate performance as accurately as possible. The Demonstration Module specific functions will not be included in subsequent plants, and are not critical for plant operation. If implemented in the main controller, these functions would reduce main controller performance, thus a stand-alone controller with no redundancy is used for these functions.

4. OCS SOFTWARE FUNCTIONS

4.1 Overview

The OCS software for a given plant subsystem consists of:

- Sequential control;
- Continuous closed-loop and open-loop control;
- Interlocking, trip and permissive logic;
- Limitation functions;
- Alarm logic and annunciation;
- Calculation functions; and
- Monitoring functions.

Fig. 3 gives an overview of the OCS software functions, for plant function 'AAA'. It also includes the interfacing to other software systems.

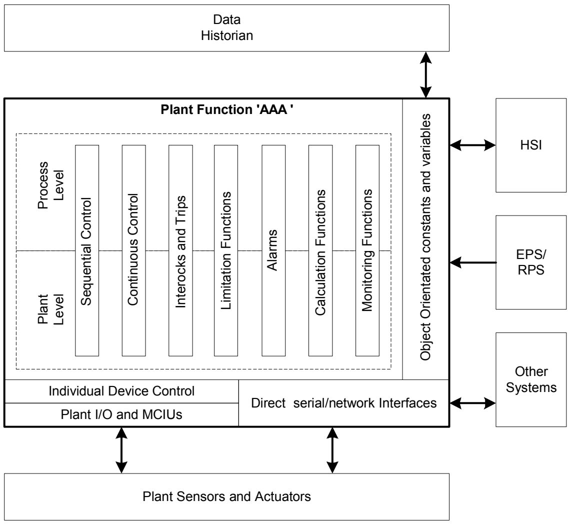

Fig. 3: OCS software functions.

4.2 Software Hierarchy

The OCS software for each of the AUs is organized in a hierarchy of super- and subordinate group controllers in order to execute the OCS functionalities in a structured manner.

The main advantages of the group controller structure are:

a. Operators have control over process functions as well as over physical plant functions.

b. The software architecture allows for the execution of process functions instead of managing plant entities.

c. It provides a consistent structure, with a single production objective, for the implementation of the control functions by multiple contactors.

Fig. 4 shows the software hierarchy for the OCS.

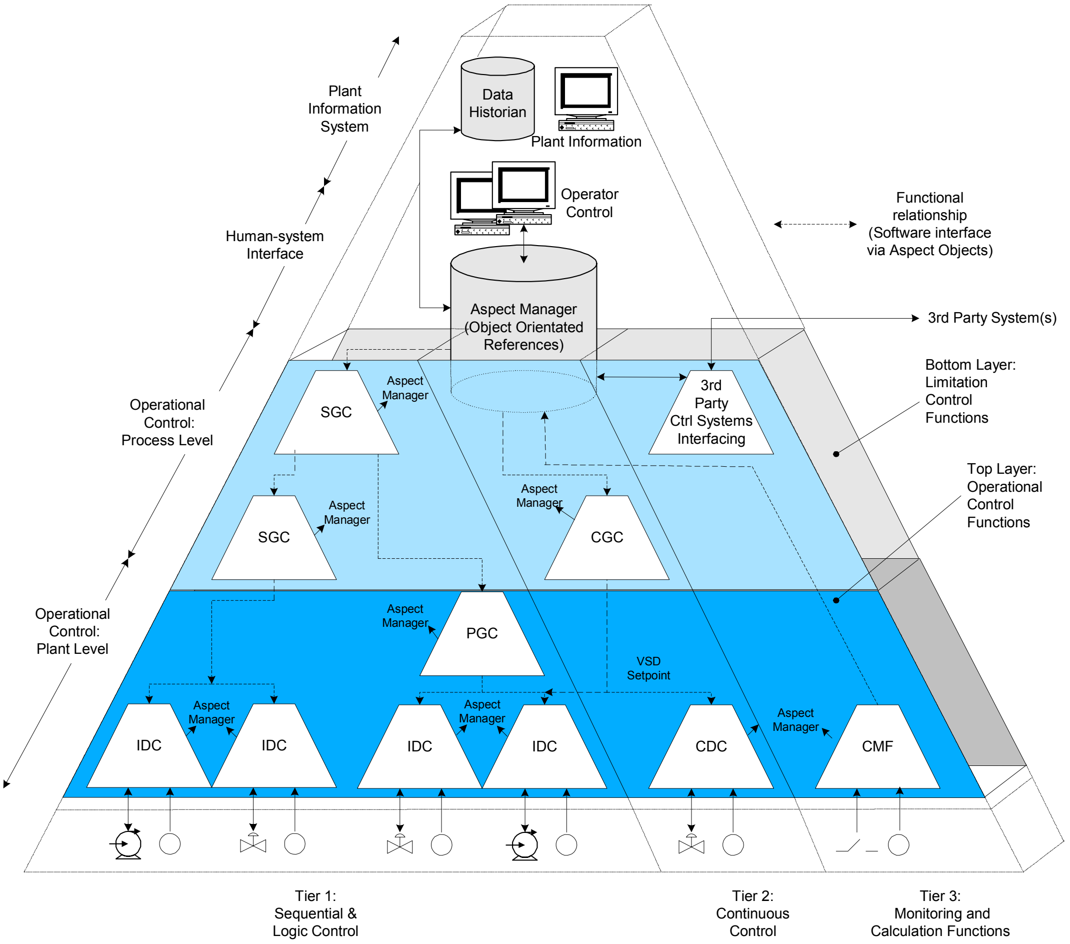
Plant Information System
Data Historian
Plant Information
Human-system Interface
Operator Control
Functional relationship (Software interface via Aspect Objects)
Aspect Manager (Object Orientated References)
3rd Party System(s)
Operational Control: Process Level
SGC
Aspect Manager
3rd Party Ctrl Systems Interfacing
Bottom Layer: Limitation Control Functions
SGC
Aspect Manager
Aspect Manager
CGC
Top Layer: Operational Control Functions
Operational Control: Plant Level
Aspect Manager
PGC
VSD Setpoint
Aspect Manager
Aspect Manager
Aspect Manager
IDC
IDC
IDC
IDC
CDC
CMF
Tier 1: Sequential & Logic Control
Tier 2: Continuous Control
Tier 3: Monitoring and Calculation Functions

Fig. 4: Software hierarchy for the OCS.

The software functions are allocated to:

- Sequential Group Controllers (SGCs);
- Plant Group Controllers (PGCs);
- Individual Device Controllers (IDCs);
- Continuous Group Controllers (CGCs);
- Continuous Device Controllers (CDCs) and
- Calculation and Monitoring Functions (CMFs).

The main features of the group controller structure are the following:

- The control system employs a central database (Aspect Manager) for all information handled during the engineering process.

  The Group Controllers are handled as Aspect-Objects in the engineering process, where these Aspect-Objects are used as containers for engineering and run time data. An Aspect-Object is a data model for an entity treated in design, engineering, operation and maintenance processes.
- The HSI uses the objects (data) from Aspect-Objects to represent operator views of the plant and writes data to Aspect-Objects to control the plant.
- Specific Aspects (Data) of Aspect-Objects are stored in a long-term Data Historian for use by the Plant Information System.
- Every active control function is allocated to a Group Controller (SGC, PGC, IDC, CGC, CDC or CMF). The task of each superordinate group controller is to coordinate the operation of the various subordinate groups allocated to it.
- The operational control is divided into two Horizontal Levels of control, three Vertical Tiers of control as well as two Layers of control.

4.3 Controller Structure

The horizontal levels of control consist of:

- *Process Level Control*: This is the superordinate control on the highest level of the Automation Hierarchy. This level executes functional requirement for the system under control.
- *Plant Level Control*: This level of control is the subordinate control on the lower level of the Automation Hierarchy. It is physically orientated, according to the plant hardware.

A Process Level Controller determines the correct time and conditions for changing the mode of a functional group of major plant drives/devices, depending on plant conditions and desired mode(s) of operation. It issues appropriate commands to a set of Plant Level Controllers (Plant Group Controllers or Individual Device Controllers) in order to control the related major plant drives/devices.

Within the above-mentioned horizontal levels, the following vertical differentiation (tiers in Fig. 4) is made:

- *Sequential and Logic Control*: Sequential and logic control functions are implemented in this tier.
- *Continuous Control*: Closed-loop and open-loop continuous control are implemented in this tier.
- *Calculation and Monitoring*: Calculation and monitoring of variables as well as estimation of unmeasured variables are implemented in this tier.

A third dimension is added to the control system structure for the implementation of limitation functions:

- *Operational control functions (top layer)*: This layer is the normal control of the plant, within the defined operational boundaries. Both horizontal levels and vertical tiers are implemented for this layer.
- *Limitation control functions (bottom layer)*: This layer of control is only active during abnormal conditions in the plant. The aim of the limitation functions is to provide a defence-in-depth functionality as shown in Fig. 5. The OCS will change certain operational parameters in order to prevent the EPS or RPS from being activated. For example, during certain conditions, running the plant at lower power, but preventing the RPS from tripping it, is preferable to running at full power with the risk of tripping the plant.

  Where limitation functions are required, these are implemented in the applicable horizontal levels and vertical tiers.

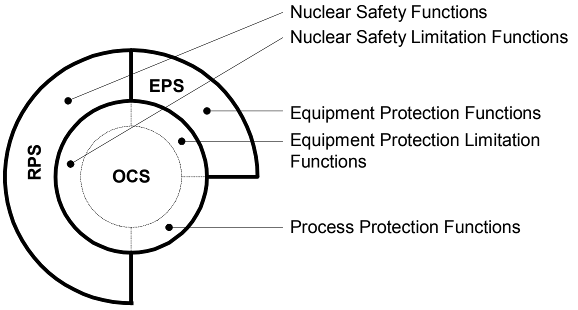
Nuclear Safety Functions
Nuclear Safety Limitation Functions
EPS
Equipment Protection Functions
Equipment Protection Limitation Functions
RPS
OCS
Process Protection Functions

Fig. 5: Protection and Limitation Functions. A specific plant parameter will be controlled under normal operating conditions, by the OCS, to stay in the centre of the 'OCS' circle in the figure. A disturbance could force the parameter towards either the reactor protection or the equipment protection limits. The Limitation functions within the OCS will strive to keep the parameter within its original boundary.

4.4 Sequential Group Controllers

A specific control function is coordinated by defining a set of operating modes, designed to achieve specific functional objectives. Each mode is defined by a unique combination of plant states and operating parameters. These control functions are implemented, using Sequential Group Controllers (SGCs).

Mode transitional sequences are initiated on any of the following conditions:

- Protection limits. The OCS limitation functions take action to prevent these protection actions;
- Automatically;
- By operator command;
- As a result of disturbances;
- As a result of a failure to respond to commands; and
- As a result of equipment failure that forces the plant out of the operating envelope defined by the prevailing state.

Note:

- One SGC may be used for the implementation of multiple functions;
- SGCs are only active when sequences are executed.
- Interlocks prevent operator requests that are invalid at the time of the request;
- The OCS performs continuous diagnostic tests on the instrumentation and actuating devices. It monitors process events and disturbances that could effect control functions.

A Mode and Mode Transition diagram for a Process Level SGC with x functions each having m modes is shown in Fig. 6.

The following modes are defined:

Mode 0:	Maintenance Mode for the SGC.
Mode 1:	Off Mode for the SGC.
Mode a.1:	Initialise Mode for Function (a) of the SGC.

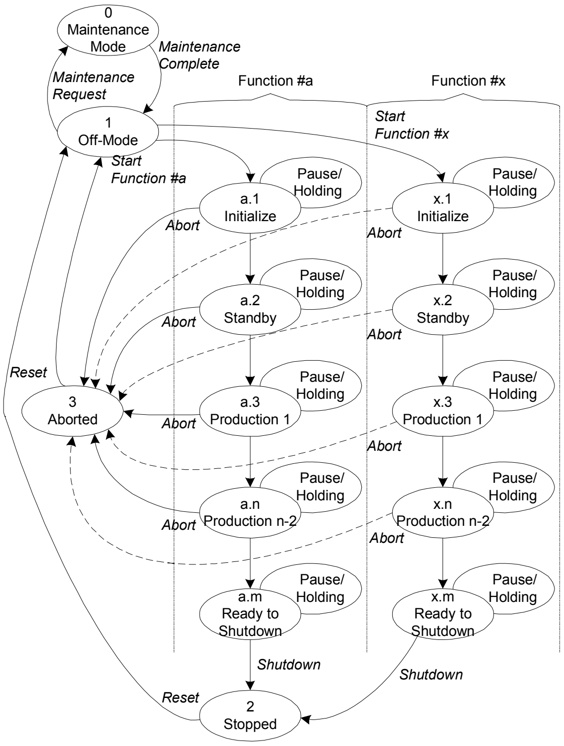

Fig. 6: Modes and Mode Transition Sequences for Process Level SGCs.

Mode a.2: Standby Mode for Function (a) of the SGC.

Mode a.3: Mode 3 (Production mode 1) for Function (a) of the SGC.

Mode x.n: Mode n (Production Mode n-2) for Function (x) of the SGC.

Mode x.m: Mode m (Ready to Shutdown Mode) for Function (x) of the SGC.

Mode 2: Aborted Mode for the SGC.

Mode 3: Stopped Mode for the SGC.

Note: 'Pause' and 'Holding' modes could be requested in each of the functional modes.

4.5 Continuous Group Controllers

Continuous Group Controllers (CGCs) are used within Tier 2 of the OCS software hierarchy for the implementation of the following continuous control functions:

- *Closed-loop feedback control* (PID, Lead-Lag, etc);
- *Open loop continuous control* (either the control system or the operator sets the analogue output signals to required values).

CGCs use the DCS standard function blocks for the implementation of continuous control functions.

4.6 Calculation and Monitoring Functions

Calculation and Monitoring Functions (CMFs) span both horizontal levels in the Automation Hierarchy and use standard DCS function blocks for the implementation of the following functions:

- *Monitoring and signal conditioning routines*: All plant signals are monitored and conditioned within CMFs. Primary alarms are calculated and the resultant status and measured values stored in the Aspect-Object vault.

  Where logical trip or threshold signals are needed for sequential control functions, the calculations on the analogue variables are done within CMFs.
- *Calculation routines*: Specialized calculations, necessary for any one of the following, are done within calculation routines:
  a) Control within other Group Controllers;
  b) Operator decision support;
  c) Plant performance evaluation; and
  d) Manipulated values for management information.
- *Estimation routines*: Physical plant or process conditions make the direct measurement of certain critical variables impossible. As a result, a combination of measurements is used to estimate specific variables or parameters. These estimation routines could vary from very simple to complex routines.

4.7 Other Issues

4.7.1 Human-systems Interface

The OCS control philosophy does not include the Human-systems Interface (HSI) philosophy, but the Plant and Process level software is structured in such a way as to allow optimal integration between these levels and the HSI software (see Fig. 4). The object-orientated nature of the control philosophy greatly enhances this integration process.

The operational and design philosophies for the HSI are defined from a Human Factors Engineering (HFE) point of view. This process is followed in parallel with the OCS software development, and is used to provide inputs for the HSI software design and implementation on the OCS.

4.7.2 Alarms

The Functional Specification documents for each of the plant subsystems specify the alarm requirements for those subsystems.

Although grouping of alarms is done along within the HSI development, the Process and Plant Level of the OCS executes calculations for Group Controllers in order to reduce nuisance alarms when Group Controllers are in operational states that do not necessitate the alarming of control room operators.

5. CONCLUSION

The following design objectives were achieved:

- The OCS control philosophy provides a design outline for all plant systems/subsystems using a common methodology;
- The OCS control philosophy establishes a control hierarchy with clearly defined levels of functionality; and
- The OCS control philosophy divides the plant into logical and functional structures, suitable for operator control from a centralized control room.

REFERENCES

ANSI/ISA-88.01-1995, American National Standard on Batch Control. Part 1, Chapter 5 – Modes and States, pp.55-60. The Instrumentation, Systems and Automation Society. North Carolina, USA.

IAEA Safety Series, NS-G-13 (2002). Instrumentation and Control Systems Important to Safety in Nuclear Power Plants. International Atomic Energy Agency, Vienna.

IAEA Safety Standards Series, NS-G-1.1 (2000). Software for Computer Based Systems Important to Safety in Nuclear Power Plants. International Atomic Energy Agency, Vienna.