ADVANCED DIGITAL INSTRUMENTATION AND CONTROL SYSTEM FOR NUCLEAR POWER PLANT PROTECTION

Dan SABINO, VVER Engineering, Westinghouse Electric Corporation, Pittsburgh, U.S.A.

Introduction

The Diverse Protection System (DPS) is a back-up to the Primary Reactor Protection System (PRPS) developed for use at the Temelín Nuclear Power Plant. The DPS is a digital system which provides a wealth of benefits from today's advanced technology. These benefits include a compact hardware design with high performance microprocessors and a structured software design using a high level language. An overview of the DPS functions, hardware and software are provided.

Functional Overview

The DPS is composed of four subsystems, each of which plays a part in providing automatic reactor protection, and the controls and indications required by the operator to bring the plant to a safe shutdown condition. These functional are provided for the occurrence of a DPS design basis event concurrent with a common mode failure of the PRPS. The DPS functions consist of:

1. Diverse Reactor Trip (DRT) System

The DRT system contains three independent divisions which automatically issue division reactor trip demands in the event that DPS setpoints are reached. All division reactor trip demands are voted two-out-of-three among the divisions. That is to say that if a trip condition exists within one division, a logic trip is generated and output to the other two divisions. Upon receipt of the same logic trip input from another division, a division reactor trip demand is generated and the associated division AC and DC reactor trip breakers are opened. The DPS reactor trip breakers are wired in a matrix such that division reactor trips must be generated by two DPS divisions before a reactor trip occurs and control rods are inserted.

The DPS reactor trip breakers are independent of the PRPS reactor trip breakers. The DPS and PRPS reactor trip breaker matrices are wired in series. Therefore, the DPS or PRPS can independently trip the reactor, and neither system prevent the other system from tripping the reactor.

2. Diverse Engineered Safeguard Features (DESF) System

The DESF system generates automatic component actuation signals in all three divisions. These signals are transmitted to the Non-Programmable Logic (NPL) to actuate, control or enable manual control of the ESF components (pumps and valves) needed to meet the DPS design objectives.

Unlike the DRT subsystem, the DESF subsystem shares ESF components with the PRPS. These components are shared via the NPL system. The NPL is a hardware only system and acts to allow either the PRPS or DPS to control the ESF components. Normally the NPL acts as an "or" gate to allow either the PRPS or DPS to control the ESF components. However, in the event of a conflict in commands (i.e. opposite commands) from the PRPS or DPS, as postulated in the event of a PRPS or DPS failure, the NPL acts to protect the ESF components and provide indication to the operator. For all DPS design basis events the operator has sufficient manual controls and time to manually initiate ESF, if required.

3. Main Control Room Diverse Monitoring System (MDMS)

The MDMS provides adequate monitoring for the operator to stabilize the plant using the diverse manual controls following the occurrence of a DPS design basis event concurrent with a common mode failure of the PRPS. The MDMS system is independent of the Post Accident Monitoring System in the Main Control Room.

4. Emergency Control Room Diverse Monitoring System (EDMS)

The EDMS provides adequate monitoring for the operator to assess the status of the plant Critical Safety Functions to attain safe shutdown following a postulated common mode failure in the PRPS. The EDMS is independent of the Post Accident Monitoring System in the Emergency Control Room.

Hardware Implementation

A single division of the Diverse Reactor Trip and Diverse Engineered Safeguard Feature subsystems are implemented within the same Diverse Protection System Cabinet. The Diverse Protection System (DRT and DESF) consist of three redundant safety divisions. Each of the divisions are physically and electrically separated to reduce the possibility of a common mode failure. Each DRT and DESF safety division contains the equipment necessary to perform the following:

1. Permit acquisition of inputs (plant sensors, component status signals, etc.) required for DRT and DESF calculations.

2. Perform computations based on these inputs.

3. Permit manual trip or bypass of individual DRT or DESF functions.

4. Provide data to external systems.

5. Provide continuous self diagnostics and support periodic surveillance testing.

Figure 1 provides an overview of a single DPS cabinet hardware architecture. Inputs to the DRT and DESF processing systems from plant sensors and plant components are protected by surge suppression circuitry at the Input and Output modules. These signals are routed to the interface circuitry that convert the signals to low level analog or digital signals as appropriate. These low level signals are connected to analog or

digital input circuitry that resides on modules connected to the VMEbus. The protection processors which perform the DRT and DESF calculations also reside on the same VMEbus. Outputs from the DRT and DESF processing systems consist of either isolated voltages, semiconductor switches or data sent over the DPS Highway. Table 1 provides an overview of the DPS hardware capabilities.

The DPS design uses a VMEbus architecture which allows for flexibility in adding input modules, output modules and processing modules. The VMEbus uses a master-slave architecture. A master module is one which can initiate data transfer bus cycles. The master modules transfer data to and from the slave modules. A slave module detects bus cycles generated by the master module and participates only if selected. Because more than one master module can reside on the VMEbus it is referred to as a multi-processing bus. In the DPS only the processors that perform protection functions (DRT and DESF) are master modules, the remaining modules are slave modules. This ensures the test processor can not affect system operation. Test circuitry and test processors interface to the protection processors via shared memory buffer over the VMEbus.

Communication between protection divisions and other subsystems is through a reflective memory interface to the VMEbus, referred to as the DPS Highway. By using three sets of redundant highways that daisy chain in opposing directions, the Diverse Protection System ensures reliable data communications among the subsytems. Set 1 (A1, B1) of the highways is dedicated to Division 1 and the EDMS, Set 2 of the highways (A2, B2) is dedicated to Division 2 and the MDMS, Set 3 of the highways (A3, B3) is dedicated to Division 3. The specified division is the only one which can write to the division ring set. The other divisions can access that ring set on a read-only basis. This ensures independence among divisions. Failure of any system on the ring will not prevent communications among remaining subsystems due to the counter rotation of the ring. An optical bypass switch located at each node on the ring provides additional fault tolerance. Upon loss of power to the node, the optical switch automatically closes, bypassing the node to maintain ring integrity.

Each DPS division also contains a single test processor. The test processor is primarily responsible for surveillance testing and calibration of the DRT and DESF functions. It also facilitates communications with, and provides an interface to a non-1E tester man-machine interface. The non-1E tester man-machine interface is implemented on a portable Sparcbook for ease of use. Prior to beginning testing, a key switch inside the DPS cabinet must be placed in the test position. In addition to the key switch, the test processor and tester man-machine interface provide password protection and safety interlocks. The safety interlocks ensure no other divisions are in bypass prior to the start of test, otherwise the start of the test is blocked. A test initiated from the tester man-machine interface typically involves injection of simulated inputs and monitoring of outputs to demonstrate that expected results are obtained. Test results are available on the tester man-machine interface and can be printed. The test processor also monitors the protection system for failures and diagnostic information during normal operation.

The MDMS and EDMS systems use the same hardware architecture as the DRT and DESF systems. Each system receives all of its data from the DRT and DESF systems

via the DPS highway. This information is processed and formatted for display. Each system contains a single remote assembly containing a liquid crystal display (LCD), audible alarm and keyboard. This assembly is mounted in the respective control room panels. The keyboard can be used to select the desired display, acknowledge the audible alarm, or acknowledge visual alarms on the display.

The DPS highway is also connected to a Data Highway Gateway (DHG). The DHG is transparent to the DPS and can only read data from the DPS highway. The purpose of the DHG is to pass data from the DPS highway to the Plant Data Highway for use in the Unit Information System.

Software Implementation

The DPS uses a subset of the Ada language for its software programming. Although the Ada language is superior to many other languages for use in safety critical applications, it still contains features that are not suitable for these applications. Therefore the DPS uses the Thompson Certifiable Small Ada Run Time (C-SMART) tool set compiler and run-time executive which meet the safety critical requirements of the commercial aviation industry. Additional restrictions were applied to avoid Ada features that could possibly lead to run-time, erroneous execution or order dependence errors. These restrictions were established in a detailed coding standard document.

The use of object-based concepts provides for a standard software design based on standard software components. The software design can be described on three levels:

1. Subsystem - Software resident on an embedded computer. A subsystem is an assembly of software components.

2. Component - One or more Ada packages that perform a specific function. The component is the basic unit of reusable software for the DPS.

3. Package - A package is a collection of type definitions, data declarations and subprograms.

The DPS is comprised of several different subsystems. As a result, the DPS places great emphasis on development of a common architecture for all subsystems using a core set of components. Examples of core components are those used for communications, input processing, and output processing. All components are passive, requiring activation from and external agent (the executive). Also all components are independent. This allows for components to be added or removed from the subsystem architecture with no impact on other components. To support this design, an inter-component communications mechanism known as the data manager was developed.

To support component independence, but maintain a coherent interface each DPS component follows a standard architecture. Each component is made up of the following Ada packages:

Interface - Each component has a single interface where subprograms and data structures necessary for using the component are specified. Types necessary for component use are put in a separate subsystem wide types package.

Configuration Data - In order to facilitate reuse, the components are designed to be as configurable as possible. The data and constants necessary for configuring the component are contained in this package.

Algorithms - The algorithm packages perform any support processing not performed by the subprograms in the interface package.

Types - Any data types that are only used locally within the component are declared in this package.

Low-Level Interface - Components that interface with hardware or operating systems use a package that provides an abstract interface layer.

Data Manger Interface - Each component interfaces to the data manager as the inter-component communications mechanism. The interface to the data manager is considered part of the component.

Packages were developed with types, data structures and services that support the overall design.

Conclusion

The DPS is a state of the art digital protection system. It provides a compact hardware design based on VMEbus technology. This technology allows for ease in adding or modifying the number and type of inputs modules, output modules, and processors. The DPS software is written in a high level language suitable for safety critical applications. The software is both modular and configurable allowing for potential future modifications and software reuse.

Table 1
DPS Hardware Capabilities

Module Name	Capabilities
Processor Module	Motorola 68040 processor operating at 25 Mhertz with 1 Mbyte Flash Memory, 256 Kbyte NVRAM and 4 Mbyte RAM
Digital Input Module (VDI)	32 Input channels configurable to use either 24 or 48 VDC wetting voltage. Provides surge withstand circuitry, relays to support test injection and signal isolation
Analog Input Module (VAI)	16 Input channels configurable in groups of four. Provides either 30 VDC sensor power, 1 milliamp or 2 milliamp current source and surge withstand circuitry
Analog Signal Conditioning Module	16 input channels configurable to provide a signal gain of 1, 10 or 100. Provides signal isolation and filtering
A/D Converter Module	64 channels of A/D conversion with 16 bit resolution. Input is configurable for either 0-10 or 0-5 VDC range
Digital Output Module (VDO)	32 channels of digital outputs configurable to provide either "dry contact" or 24 VDC outputs. Provides signal isolation and surge withstand circuitry
Reflective Memory Module	Forms DPS fiber optic data highway with a data transfer rate of 6.2 Mbytes/Second. Available in read/write or read only configuration

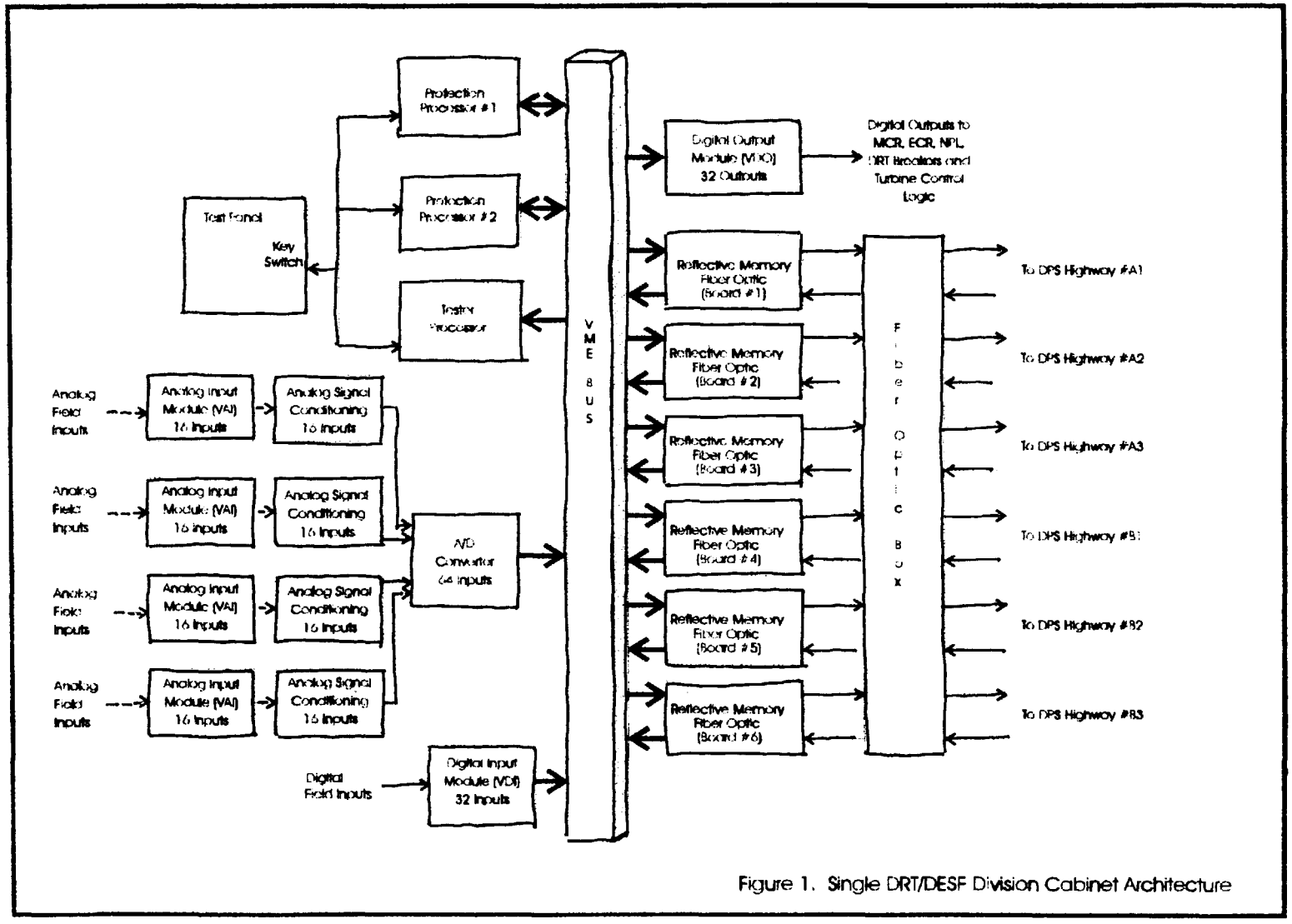

Figure 1. Single DRT/DESF Division Cabinet Architecture