QUALIFIED DISPLAY SYSTEM ARCHITECTURE

Glenn E. Lang, Keith Harvey, Craig Pfledderer

Patricia L. Barnes, Micah Drake, Dan Ho, Tommy Hunter

Lockheed Martin Corporation; Lockheed Martin Energy

P.O. Box 650003, Dallas, TX 75265-0003

ABSTRACT

There is a need in the nuclear industry for a Qualified Display System (QDS) architecture as described in this paper. The function of the QDS is to process and display Regulatory Guide 1.97 post accident monitoring parameters. The QDS is implemented on the Lockheed Martin Field-Programmable Gate Array (FPGA) based Nuclear Protection and Control (NuPAC) digital platform, coupled with a Qualified Display Controller (QDC) and a Safety Display Unit (SDU). The QDS is designed to meet the requirements of IEEE 603-1991 (endorsed by Regulatory Guide 1.153, Rev. 1), IEEE 497-2002 (endorsed by Regulatory Guide 1.97, Rev. 4), and IEEE 7-4.3.2-2003 (endorsed by Regulatory Guide 1.152, Rev. 3). The QDS is designed with flexibility such that it can be implemented in an advanced reactor design, Small Modular Reactor (SMR) with any cooling medium, or digital upgrade project for an operating nuclear plant.

The QDS has four independent and redundant divisions. Each division has five layers in the architecture: Process variable input signals; Process Protection Logic (PPL); Algorithm Logic (AL), Interface Panel (IP); and Safety Display Unit (SDU). The QDS meets the following design criteria: redundancy, independence, predictability and repeatability, and diversity capability. The QDS architecture also meets the simplicity design principle.

The QDS architecture design provides flexibility in the implementation in a plant. The QDS can be implemented in the design of a new advanced plant or as a digital upgrade in an operating plant.

Key Words: Qualified Display System, Architecture, Digital Instrumentation and Control

1 INTRODUCTION

This paper discusses the following aspects of a Qualified Display System:

a. Design criteria (Section 2)
b. Architecture description (Section 3)
c. Display hierarchy (Section 4)
d. Plant implementation flexibility (Section 5)
e. Future development tasks (Section 6)

Each of these areas are discussed in the following sections of the paper.

2 QDS DESIGN CRITERIA

The QDS architecture is designed to meet existing regulatory requirements and guidance and applicable industry standards. The following is a list of the key regulatory and industry requirements and guidance documents that are met by the QDS design:

a. IEEE Std. 603-1991, clause 5.8.1

"The display instrumentation provided for manual controlled actions for which no automatic control is provided and that are required for the safety systems to accomplish their safety functions shall be part of the safety systems and shall meet the requirements of IEEE Std. 497-1981. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator."

b. IEEE Std. 497-2002, clause 9

"Microprocessor based instrumentation development including software validation and verification shall be in accordance with the requirements of IEEE Std. 7-4.3.2-1993."

c. IEEE Std. 497-2002, clause 7

Types A, B and C instrument channels *"shall be seismically and environmentally qualified in accordance with IEEE Std. 344-1987 and IEEE Std. 323-1983."*

d. IEEE Std. 497-2002, clause 6.6

"The power supply for instrumentation that monitors Type A, Type B, and Type C variables shall be Class 1E."

"Where Class 1E power supplies are used, refer to IEEE Std. 308-1991 for the requirements that apply."

e. Design-Specific Review Standard for mPowerTM iPWR Design, Section 7.1, Fundamental Design Principles:

1. Design Basis

The design bases of the QDS shall be well defined before design and implementation in an advanced reactor, SMR or operating nuclear plant.

2. Independence

Each redundant QDS division is communication independent, physically and electrically independent, and functionally independent of each other.

The communication links used in the design of the QDS meet the guidance provided in the Digital Instrumentation and Controls Interim Staff Guidance Task Working Group #4 (DI&C-ISG-04), Section 1. The only inter-divisional communication is between the Process Protection Logic and the Algorithm Logic which enables the calculation of group values of redundant process variable signals. The only interface between safety QDS and non-safety systems is by means of the Class 1E/non-Class 1E unidirectional Gateway.

The QDS architecture meets the guidance provided in IEEE Std. 384-1992 (endorsed by Regulatory Guide 1.75) concerning separation of redundant safety divisions and safety/non-safety circuitry.

The QDS is designed to ensure that a postulated failure in another plant safety subsystem does not result in the degradation of the performance of the QDS.

3. Redundancy

The QDS is designed with four redundant divisions. Any postulated single failure does not preclude the display of redundant process variable values. The QDS architecture is designed to meet the intent of IEEE Std. 379-2000 (endorsed by Regulatory Guide 1.53) concerning postulated single failures.

4. Predictability and Repeatability

The signal display path and the system response time is the same during normal operation and following a design basis accident. The QDS design meets the functional time response requirements under the most limiting cycle time assumptions.

5. Diversity and Defense-in-Depth

The QDS architecture includes features that enables the routing of process variable signals to a diverse display system independent of the QDS software. NUREG-0800, Chapter 7, Branch Technical Position (BTP) 7-19 states the following:

"A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in Items 1 and 3 above."

The QDS architecture is designed to provide the capability to the system designer to provide a diverse process variable signal path independent of the QDS software.

f. DI&C-ISG-04, Section 1, item 3

"Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that performs the same safety function, but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors. Such a complex design, therefore, should be avoided within the safety system."

The QDS features a simple architecture with minimal inter-divisional communication. Only design features that are necessary to meet the QDS functional requirements are included in the design. Non-required design features are implemented on a non-safety display system.

3 DESCRIPTION OF QDS ARCHITECTURE

A simplified QDS architecture diagram is illustrated in Figure 1. The QDS architecture has four independent and redundant divisions.

There are five layers in each division of the QDS architecture:

a. Process variable input signals (including the Signal branching Cabinet (SBC))
b. Process Protection Logic (PPL)
c. Algorithm Logic (AL)
d. Interface Panel (IP)
e. Safety Display Unit (SDU)

A brief description of each layer of the architecture is provided below:

3.1 Process Variable Input Signals

There are four signal paths possible for inputting a process variable to the QDS:

a. Process variable sensor input signals hardwired directly from the field.
b. Process variable signals hardwired from the SBC to which the process variable sensor signal is hardwired from the field
c. Process variable hardwired from another Safety Sub-system (e.g., Nuclear Instrumentation System, Radiation Monitoring System)
d. ESF actuated component position status hardwired to the Component Control Logic and transmitted to QDS via a serial data communication link

Only post accident monitoring variable sensors that are powered from a Class 1E power source that meet the guidance of IEEE Std. 308-1991 are input to the QDS. Post accident monitoring variable sensors that are powered from a non-Class 1E power source are only input to a non-safety display system.

For those process variables that are required to be displayed in a diverse manner based upon a system Diversity and Defense-in-Depth Evaluation using the guidance provided in NUREG/CR-6303, independent signals are routed directly to a diverse display system or the process variable input signals are electrically isolated in the SBC and hardwired to the diverse display system as illustrated in Figure 1.

3.2 Process Protection Logic

The PPL performs the following functions:

a. Pre-filtering
b. Analog-to-Digital conversion
c. Engineering unit conversion
d. Signal compensation

The output of each division of the PPL is transmitted to each division of the AL (i.e., inter-divisional communication) by means of serial data communication links. Transmitting the signals from the PPL in each division to the AL in each division allows signal validation to be performed. This minimizes operator tasks following a design basis event.

3.3 Algorithm Logic

The AL performs the following functions:

a. Computes group values for process variables with redundant inputs, e.g., average, minimum, maximum
b. Computes calculated variables based upon the process variable input signals, e.g., Core Exit Thermocouple (CET) core average temperature, Subcooling Margin (SCM)

The output of the AL is input to the Interface Panel in its respective division by means of a serial data communication link.

3.4 Interface Panel

The IP serves as a marshalling point for all QDS process variable signals and calculated parameters in each division, a gateway point to a non-safety display system, and a connection point for the Test Panel.

The inputs to the IP include

a. AL (via serial data communication link)
b. ESF Component Control Logic (via serial data communication link)
c. Test Panel.

The outputs from the IP include

a. PPL (via serial data communication link used for test injection signals and modifying constants)
b. AL (via serial data communication link used for test injection signals and modifying constants)
c. QDC/SDU (via serial data communications link used for display of information)
d. Test Panel
e. Class 1E/non-Class 1E unidirectional Gateway

The Test Panel, connected to the Interface Panel via serial data communication links, is used to conduct periodic surveillance tests, and modify PPL and AL selected gains and time constants.

The Class 1E/non-Class 1E Gateway (unidirectional only) is used to transmit all QDS data to a non-safety display system.

3.5 Safety Display Unit

There is at least one SDU (and associated QDC) per division located in the main control room which display all post accident monitoring variables on each division. The number of displays per division is determined from a human factor evaluation of the main control room on a plant-by-plant basis.

An SDU displays the post accident monitoring process variable input signals associated with all four divisions, and the calculated post accident monitoring signals (from its respective division only). The operator has the capability to select different display pages on each division of the SDU.

4 SDU DISPLAY HIERARCHY

For a digital upgrade project on an operating plant, the display pages associated with an SDU are customized on a plant-by-plant basis. Some plants may desire to maintain the same display pages that are available on a digital display system being replaced, i.e., to minimize operator retraining. Other plants may be interested in replacing numerous existing displays (analog and/or digital) that currently exist on the main control board with a single SDU, i.e., due to equipment obsolescence. Still other plants may be interested in implementing a complete digital main control board concept.

For a new advanced reactor design, the following display hierarchy is recommended:

a. QDS display hierarchy
b. Display page with overview of all Type A, B, and C variables.
c. Display pages with detailed data for Type A, B and C variables
d. Display pages with Type A, B and C variables time history
e. Display pages with detailed data of each Type D and E process variable powered from a Class 1E power source
f. Display pages with position status of each ESF actuated component

The QDS display hierarchy is designed to ensure that any display page can be accessed with a maximum of two touch or click points depending on the QDS design.

Figure 2 provides an example of a QDS Display Hierarchy layout on the SDU. The QDS Display Hierarchy touch point on the top is included in the header of each display page. Touching or clicking on the QDS Display hierarchy touch point accesses the illustrated display page. The shaded boxes on the display provide active touch points. The non-shaded boxes on the display provides non-active background information only.

Figure 3 provides an example of a typical Type A, B and C variables Reactor Vessel Detailed Data display for a four loop plant.

5 QDS PLANT IMPLEMENTATION

The QDS architecture design features flexibility with respect to plant implementation. The following examples describe possible implementation variations.

a. For a new reactor design (e.g., advanced plant or SMR), the architecture illustrated on Figure 1 can be implemented.
b. For an operating plant that has an existing digital safety display that must be replaced due to equipment obsolescence, only the IP and SDU portion of the QDS architecture can be implemented.
c. For an operating plant that has a digital safety display with no inter-division communication, the inter-division communication links can be removed from the QDS architecture illustrated on Figure 1.

The NuPAC platform provides considerable flexibility to the system designer in implementing the PPL and AL in the processing of the post accident monitoring variables.

6 FUTURE QDS DEVELOPMENT TASKS

Future development efforts are planned to enhance the capability of the SDU to accept soft commands using either a touch point or click point (via a mouse or trackball) for operator control enhancement. The SDU will not only be used for the display of post-accident monitoring parameters, but will also provide the main control room operators the capability to take manual actions associated with the Reactor Trip System (RTS) and the Engineered Safeguards Actuation System (ESFAS) that are necessary for plant startup, plant shutdown and post accident recovery.

Soft control capability will be provided for the following functions:

a. Manually initiate Block and Reset commands associated with the RTS and ESFAS

b. Manually change the state of Engineered Safeguards Features (ESF) actuated components
c. Manually update Nuclear Instrumentation System (NIS) calibration constants

Figure 4 provides an example of a typical High Source Range Neutron Flux Reactor Trip Function Block and Reset soft manual controls and status display page. The following features are provided on the display page:

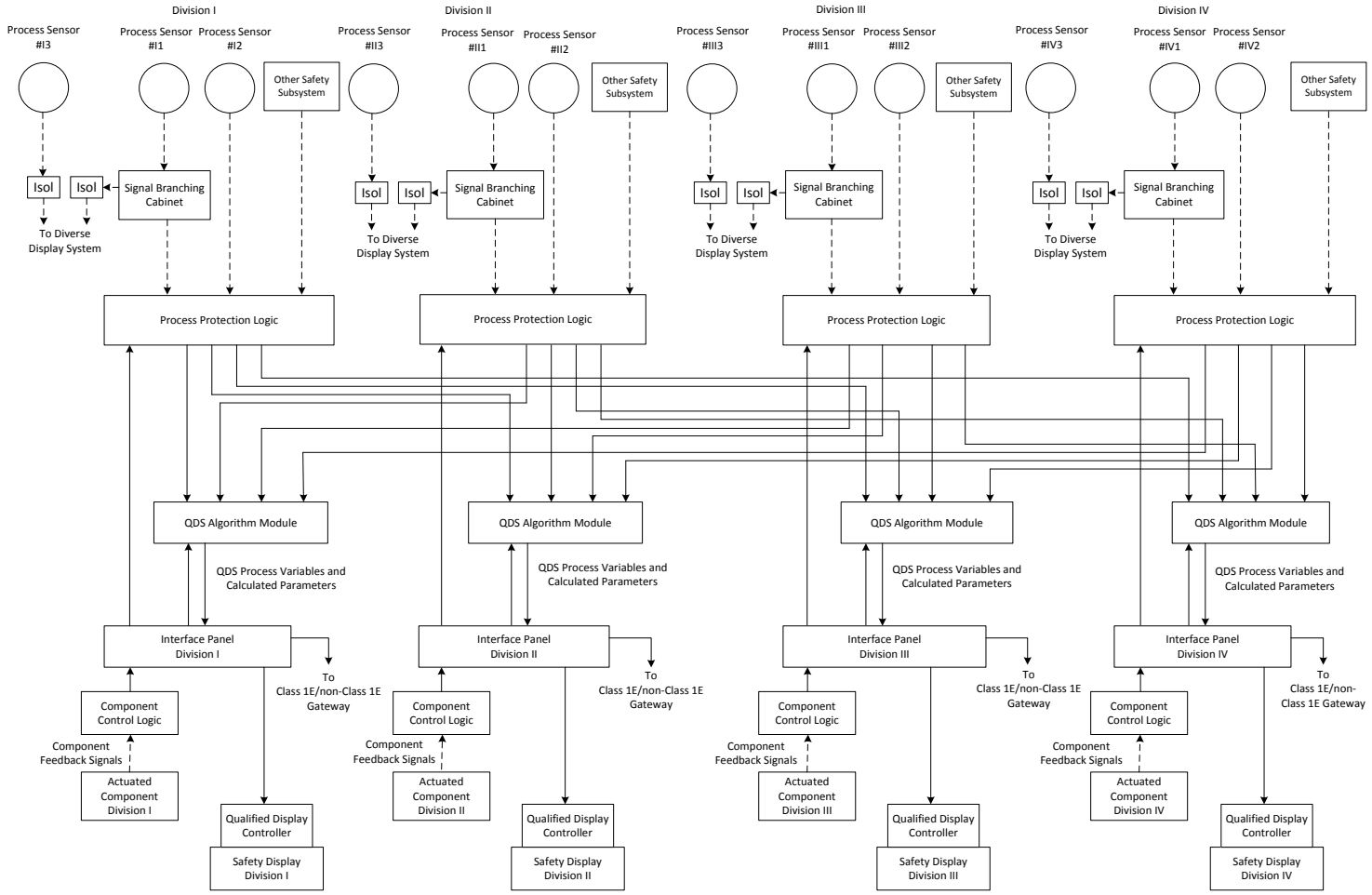
a. Indication as to whether the soft manual Block and Reset controls of the High Source Range Neutron Flux Reactor Trip function are Enabled (Enabled/Not Enabled)
b. Soft manual High Neutron Flux Reactor Trip Block and Reset controls
c. High Source Range Neutron Flux Reactor Trip channel status (Tripped/Not Tripped, Blocked/Not Blocked)
d. High Source Range Neutron Flux Reactor Trip Division status (Tripped/Not Tripped)
e. High Source Range Neutron Flux Reactor Trip status (Tripped/Not Tripped)

7 CONCLUSIONS

This paper provides the design criteria and description of a Qualified Display System architecture that can be used to display post accident monitoring variables on a qualified display system. The QDS architecture features four independent and redundant divisions. Each division has five layers in the architecture: Process variable input signals; PPL; AL; IP and SDU. The QDS architecture provides flexibility in its implementation in either a new advanced plant or as a digital upgrade in an operating plant.

8 REFERENCES

1. IEEE Std. 603-1991, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.
2. IEEE Std. 7-4.3.2-1993, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.
3. IEEE Std. 497-2002, IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations.
4. IEEE Std. 323-1983, IEEE standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations.
5. IEEE Std. 344-1987, IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations.
6. IEEE Std. 308-1991, IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations.
7. IEEE Std. 379-2000, IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems.
8. IEEE Std. 384-1992, IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits.
9. Regulatory Guide 1.152, Rev. 1, Criteria for Digital Computers in Safety Systems of Nuclear Power Plants.
10. Regulatory Guide 1.153, Rev. 1, Criteria for Safety Systems.
11. Regulatory Guide 1.97, Rev. 4, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants.
12. Regulatory Guide 1.53, Rev. 2, Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems.
13. Regulatory Guide 1.75, Rev. 3, Physical Independence of Electrical Systems.
14. NUREG/CR-6303, Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems, October 1994.
15. DI&C-ISG-04, Rev. 1, Working Group #4: Highly-Integrated Control Rooms – Communications Issues (HICRs)
16. Design-Specific Review Standards for mPower™ iPWR Design, Section 7.1, Instrumentation and Controls-Fundamental Design Principles, March 2009.
17. NUREG-0800, Chapter 7, BTP 7-19, Rev. 6, Guidance for the Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems.



Legend:

- - - - Hardwired Connection

____ Serial Data Communication Link

Figure 1: Simplified Qualified Display System Architecture Diagram

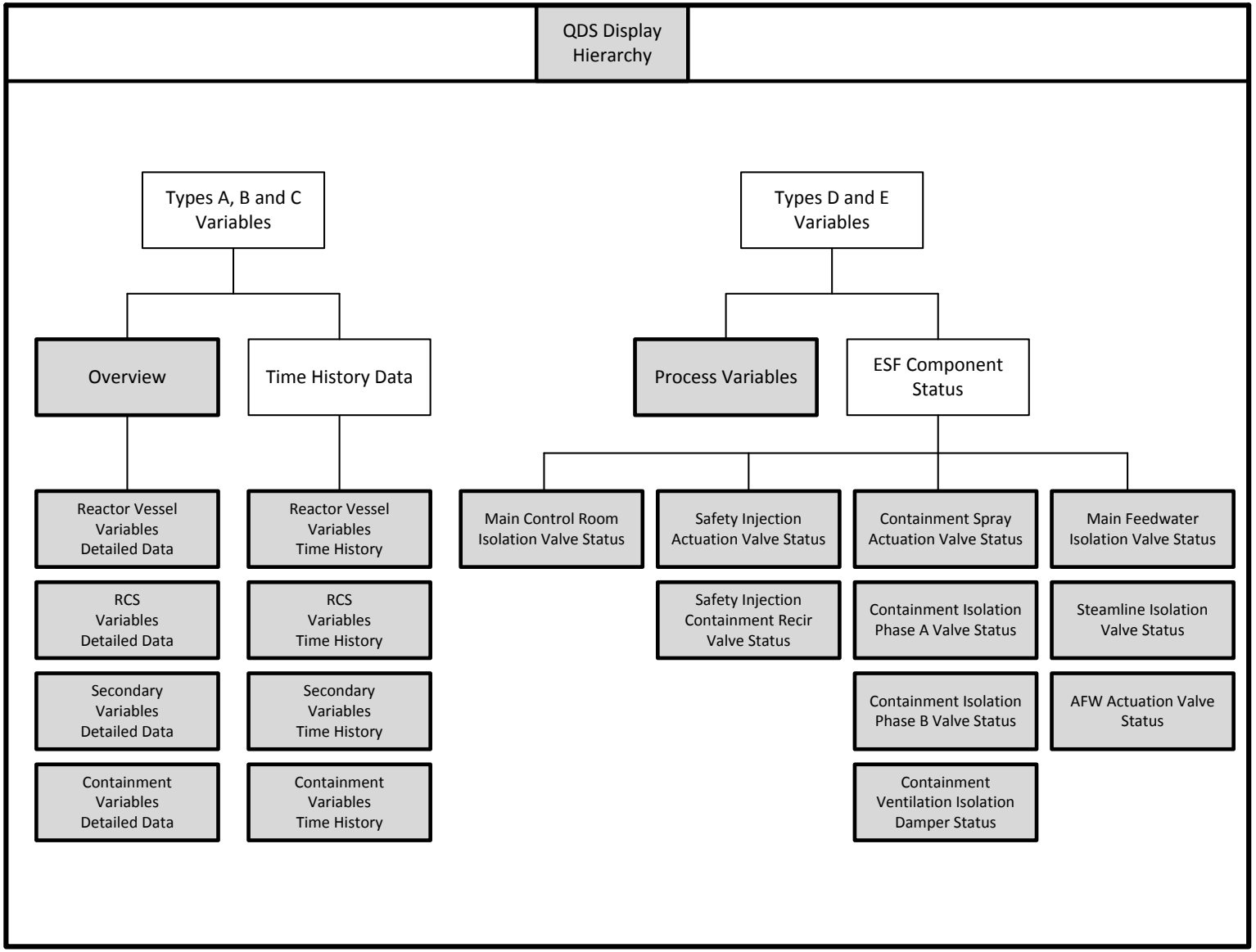


Figure 2: Example of QDS Display Hierarchy Layout

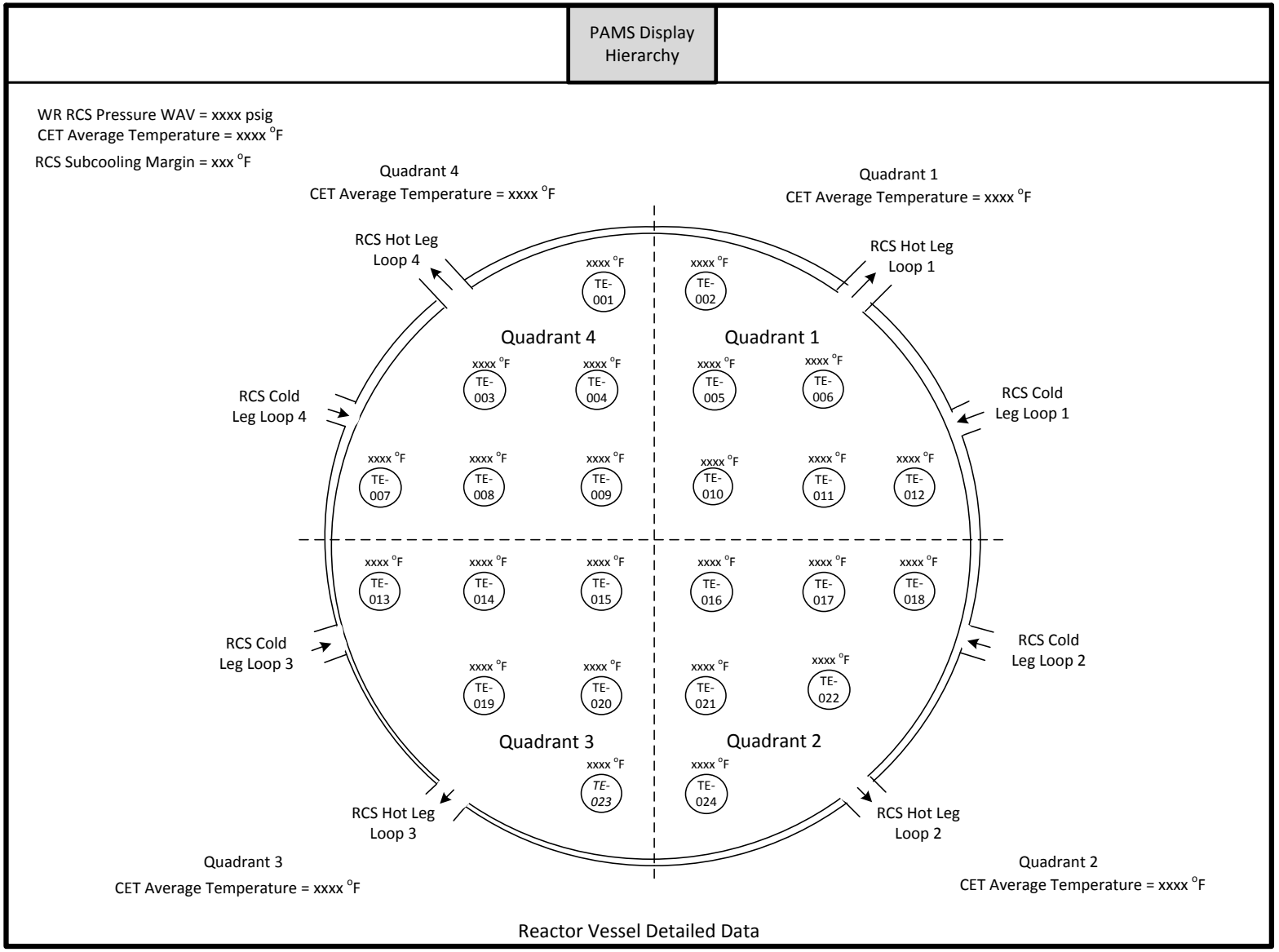


Figure 3: Example of Reactor Vessel Detailed Data Display

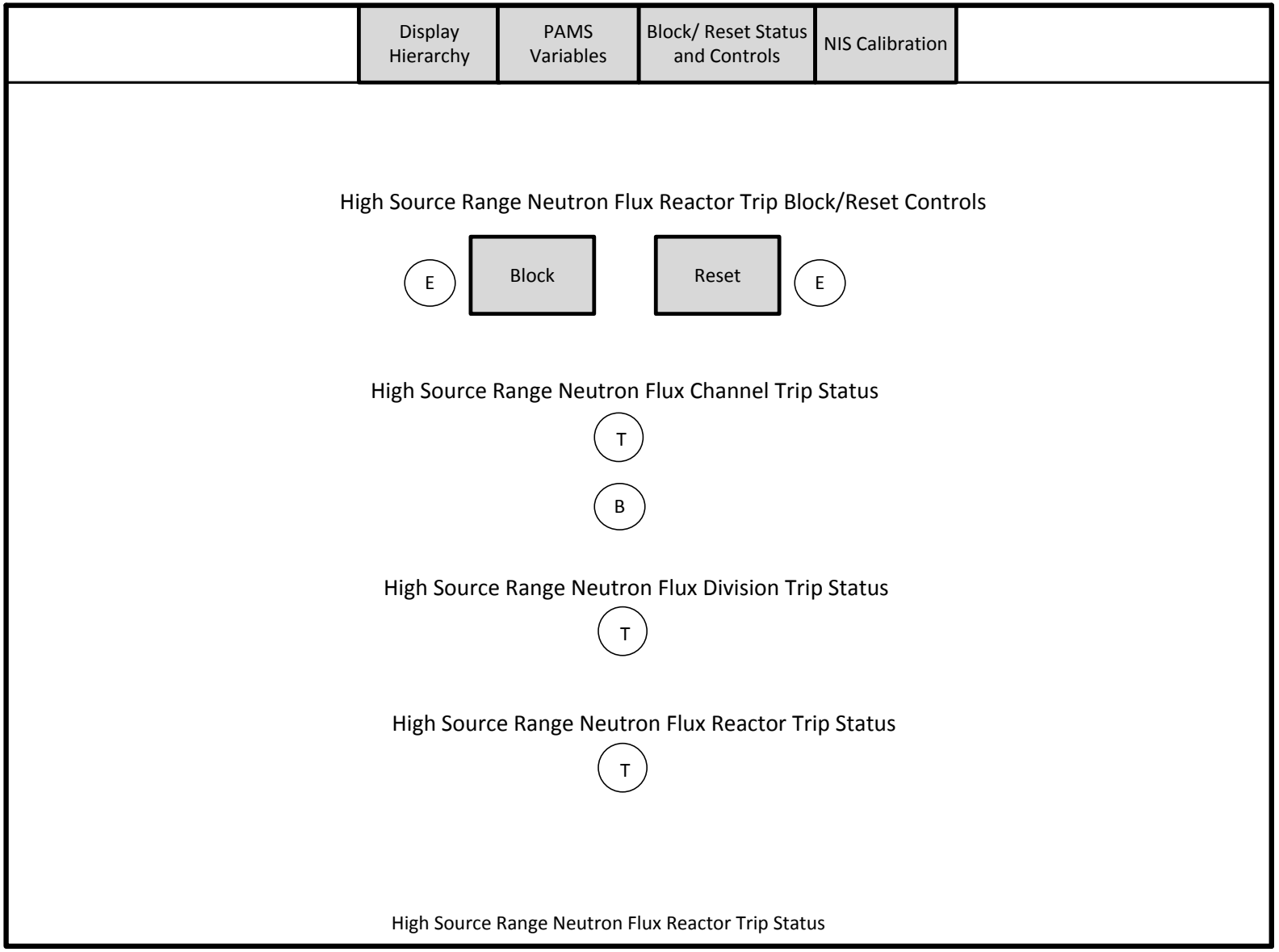


Figure 4: Example of High Source Range Neutron Flux Reactor Trip Status and Control Display