ICE-322(PC/31)/jg 1

NUPLEX 80+ ADVANCED CONTROL COMPLEX DESIGN BASES

NPX80-IC-DP-790-01

Revision 00

Nuclear Power Systems
COMBUSTION ENGINEERING, INC.
Windsor, Connecticut

Issue Date 1/15/90

TABLE OF CONTENTS

TABLE OF CONTENTS (continued)

1.0 PURPOSE

The purpose of this document is to provide the bases for the Nuplex 80+ Advanced Control Complex (ACC) design. The intent of this document is to identify the driving forces (i.e. the "why") behind the philosophies and implementation methods adopted for Nuplex 80+.

2.0 SCOPE AND INTRODUCTION

The scope of this document includes overall Nuplex 80+ high level design bases and specific design bases for the man-machine interface, I&C systems and integrated systems features. Generally the document deals with the bases for design but also includes some implementation information where it aids in understanding the bases.

The bases provided in this document pertain specifically to the generic Nuplex 80+ ACC design. The generic Nuplex 80+ design is a reference design for an ACC which may be applied to specific plant designs for evolutionary LWRs (such as System 80+), other LWR designs (such as SIR) or other reactor technologies. The Nuplex 80+ generic design has evolved from the Nuplex 80 ACC reference design that was developed for the TVA Yellow Creek units in the late 1970's. Specific improvements have been made as a result of various industry driving forces. These driving forces are illustrated in Figure 2-1. Significant direction has been derived from customer requirements and the Utility Requirements Document generated in the EPRI ALWR program. Additional direction has come from new licensing requirements, industry standards and C-E's experience base. Many of these requirements can only be fulfilled because of the potential derived from advanced technologies.

The Nuplex 80+ generic reference design can be applied to any nuclear power plant. The generic I&C system designs and generic man-machine interface methodologies are applicable to both LWR and other reactor technologies. Though some changes in the actual control complex design will result from the unique application, the generic Nuplex 80+ framework will be suitable. In addition, the flexibility of the design derived from using software based systems and off the shelf hardware allows easy accommodation of customer requirements. The generic to project specific evolution is illustrated in Figure 2-2.

The flexibility of the generic Nuplex 80+ design provides the potential for application to many different plant designs. The design bases in this document pertain to the generic, reference ACC design though some of the implementation illustrations are based on the System 80+ plant design. Additional design bases for specific plant applications and to meet customer requirements should be added to this document to form a complete plant specific design bases for a specific I & C design.

ADVANCED CONTROL
REQUIREMENTS DEVELOPMENT

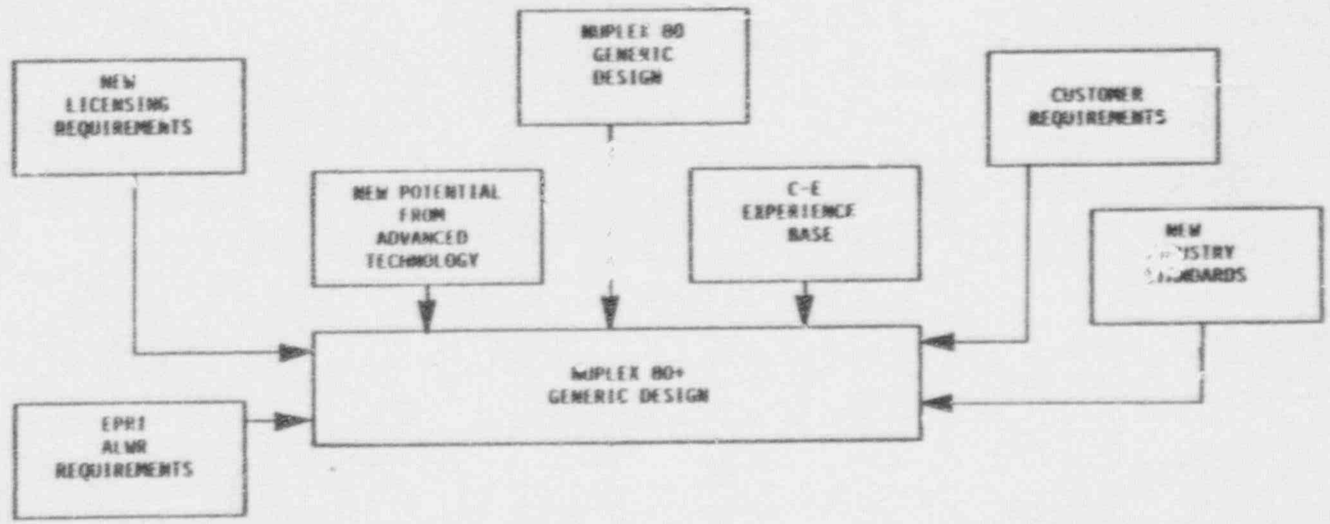

FIGURE 2-1

NUPLEX80+

APPLICATION OF GENERIC NUPLEX 80+ DESIGN

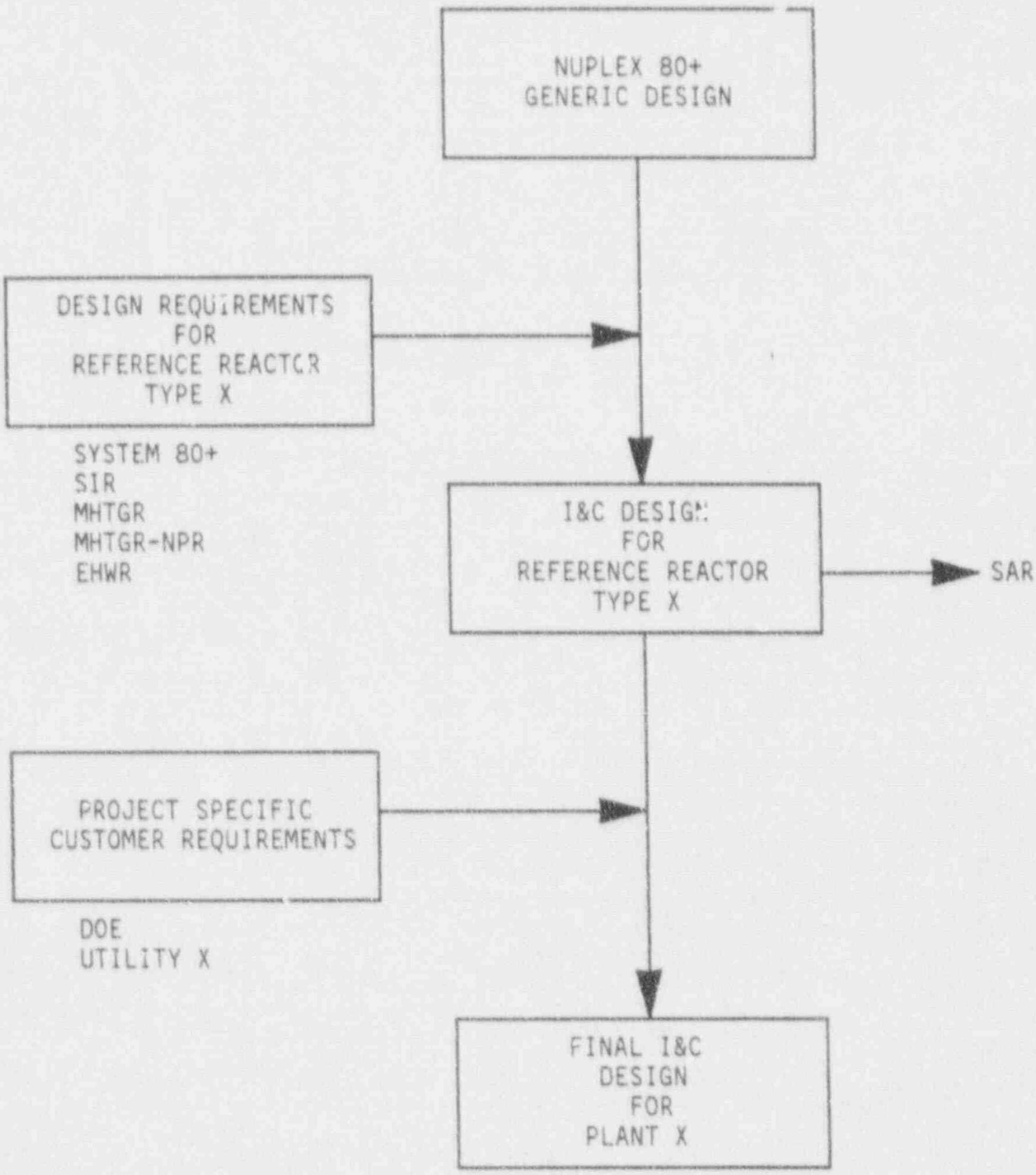

FIGURE 2-2

3.0 REFERENCES

1. CESSAR-DC Chapter 7 "Instrumentation and Controls", Rev. E, December 30, 1988.

2. CESSAR-DC Chapter 18 "Human Factors Engineering" Rev. E, December 30, 1988.

3. D. S. Jamison, "Design Criteria and Procedure for Layout of Control Room Indications and Controls for Nuplex 80+", NPX80-IC-DP791-01, February 14, 1989.

4. E. R. Frederick, "Design, Training, Operation - The Critical Links; An Operator's Perspective". Presented at the IAEA International Symposium on Severe Accidents in Nuclear Power Plants, March 1988.

5. D. S. Jamison, "System Description for Control Complex Information System for Nuplex 80+", NPX80-IC-SD791-01, February 23, 1989.

6. R. S. Rescorl, "Design Report for the RCS Panel for System 80+", NPX80-IC-RR-791-01, June 30, 1989.

7. D. S. Jamison, "Nuplex 80+ Integrated Process Status Overview", IC-88-088, April 18, 1988.

8. D. S. Jamison, "System Description for Critical Function and Success Path Monitoring in Nuplex 80+" NPX80-IC-SD790-02, June 22, 1989.

9. OECD Halden Reactor Project "Experimental Validation of the Critical Functions Monitoring System", HWR-312, March 1984.

10. OECD Halden Reactor Project, "The Experimental Evaluation of the Success Path Monitoring System Results and Conclusions", HWR-224, May, 1988.

11. D. L. Harmon, "Nuplex 80+ Safety Related Display Information Design Basis and Methodology", IC-88-073, March 17, 1988.

12. D. L. Harmon, "Nuplex 88+ Remote Shutdown Panel Design Basis and Methodology", IC-88-145, August 10, 1988.

13. R. B. Fuld, "Nuplex 80+ Verification Analysis Report", NPX80-IC-TE790-01, June 1989.

14. Nureg 0800, Standard Review Plan, July 1981.

15. Reg. Guide 1.75, "Physical Independence of Electrical Systems", Rev. 2.

16. C. F. Ridolfo, "System Description for the Data Processing System for Nuplex 80+", NPX80-IC-SD710-00, July 12, 1989.

17. R. M. Manazir, "System Description for the Discrete Indication and Alarm System for Nuplex 80+", NPX80-IC-SD880-00, April ?, 1989.

18. U.S. Department of Energy Advanced I&C Program, Subtask 1.13 Milestone Submittal: Data Acquisition System Communications, October 10, 1989.

19. "System Description for Megawatt Demand Setter (MDS) for Nuplex 80+", NPX80-IC-SD650, Rev. 00, May 6, 1989.

20. R. J. Moreau, "System Description for Power Control System for Nuplex 80+", NPX80-IC-SD630, Rev. 00, November 3, 1989.

21. W. M. Cushman, "System Description for the Plant Protection System for Nuplex 80+", NPX80-IC-SD560, Rev. 00, November 16, 1989.

22. U.S. Department of Energy Advanced I&C Program, Subtask 108 Milestone Submittal. "Intersystem Communication Methods", September 1, 1988.

4.0 NUPLEX 80+ HIGH LEVEL DESIGN BASES

The Nuplex 80+ ACC has three high level design bases. They are: 1) to resolve post-TMI concerns particularly regarding the man-machine interface at nuclear plants, 2) to continue to improve plant safety and 3) to improve the cost effectiveness of nuclear power generation.

Post-TMI concerns include reducing operator information overload, improving the human factors of annunciator systems, monitoring of safety related information and ESF status, designing for sabotage and fire protection and incorporating the safety parameter display function.

Improved plant safety is addressed by reducing the potential for human error through man-machine interface improvements, improving safety system reliability through fault tolerance, segmentation, diversity and automatic testing and reducing the challenges to safety systems through control system improvements.

The cost effectiveness of a nuclear plant is enhanced by cost reductions related to design, construction, operations and maintenance. Cost reductions in design are facilitated by using a common reference design for both NSSS and BOP. The Nuplex 80+ design is fully documented including licensing documentation complete to FSAR level of detail. Other design cost savings come from utilization of off-the-shelf equipment, automated design tools and flexible software based systems. Construction cost benefits are based on schedule acceleration and lower construction costs resulting from extensive use of multiplexing and use of standardized, factory tested systems. Operations and maintenance cost reductions will be significant for Nuplex 80+. These are based on standardization of the NSSS and BOP man-machine interface and I&C system, and their improved reliability. Further cost benefits are derived from extending automatic control ranges, providing load following capability, control sensor validation, pretrip control actions, variable protection limits and monitoring of critical power production functions much the same as critical safety functions are monitored.

4.1 MAN-MACHINE INTERFACE HIGH LEVEL DESIGN BASES

This section presents high level design bases for the Nuplex 80+ man-machine interface. The Nuplex 80+ man-machine interface shall:

A. Be based on the human engineering principles established for Nuplex 80 and include specific improvements in:

- Alarm handling
- Plant and system overview comprehension
- Operation with equipment failures

B. Accommodate the EPRI URD Advanced Light Water Reactor (ALWR) operating staff and meet the ALWR operations requirements.

C. Integrate NSSS and balance of plant systems into a unified control complex design.

D. Reduce the potential for human error that could affect plant safety or availability.

E. Reduce the operator's information processing requirements while meeting all of his information needs.

F. Improve the reliability of the man-machine interface through redundancy, segmentation, and diversity.

G. Meet all current regulatory requirements relating to the man-machine interface.

H. Base instrumentation and control requirements and panel functional groping on the results of a top down functional task analysis.

4.2 I&C SYSTEMS HIGH LEVEL DESIGN BASES

The high level design bases for Nuplex 80+ I&C systems are presented in this section. Nuplex 80+ I&C system designs shall:

A. Maximize the standardization of components to minimize personnel training and spare parts inventory, while maintaining a minimum level of diversity to protect against common mode failures.

B. Provide fault tolerance for all functions that impact plant safety or availability.

C. Use multiplexing, where cost effective, for data communication in all systems (safety and non-safety).

D. To the maximum extent possible, configure all systems using off-the-shelf products that are proven through at least three years of similar service.

E. Meet all applicable industry and regulatory requirements.

F. Utilize software based digital technologies except for signal conditioning and power conversion applications.

G. Provide continuous automatic hardware testing of all computer based systems and automatic functional testing for surveillance tests required on a monthly basis or more frequently.

H. Provide semi-automatic or computer assisted testing for functional tests required less frequently.

I. Provide easy modification with a minimum of hardware changes and provide adequate expansion capability.

5.0 MAN-MACHINE INTERFACE DESIGN BASIS

5.1 CONTROL ROOM STAFFING AND CONFIGURATION

The following design bases relate to the Nuplex 80+ control room staffing and configuration.

A. The Nuplex 80+ control room shall provide adequate workspace for the following operating staff during both normal and emergency operations:

- 1 Shift Supervisor (SS)
- 1 Control Room Supervisor (CRS)
- 2 Assistant Reactor Operators (ARO)
- 1 Shift Technical Advisor (STA)
- 2 Nuclear Equipment Operators (NEO)

B. The Nuplex 80+ controlling workspace shall allow operation by a single operator between hot standby and full power and shall accommodate a control room supervisor and two assistant reactor operators continuously if desired.

C. The Nuplex 80+ ACC configuration shall minimize required access to the controlling workspace for non-operating staff during both normal and emergency operation to minimize disturbance to plant operators.

D. The Nuplex 80+ configuration shall provide a workstation for a control room supervisor within the controlling workspace to allow direct coordination of operator activities.

E. The control room configuration shall allow visibility of a "big board" overview display from all locations within the controlling workspace, from control room offices and from the Technical Support Center (TSC), to enhance communication among all operating personnel.

F. To optimize the design of these facilities for all operating conditions the shift supervisor and the control room supervisor are provided enclosed offices within the control room with full view of the controlling workspace.

G. The control room configuration integrates facilities such as the offices for operations personnel and the Technical Support Center (TSC) into the control room design. The MCR shall be visible from the TSC to allow emergency personnel to monitor activities in the MCR and better communicate with personnel in the MCR.

H. In addition to its emergency response function, the TSC is utilized to accommodate visitors, allowing full visibility of control room activities without interference with operations personnel and without compromising control room security. Similarly the TSC can accommodate the plants technical staff providing CRT access to real time plant performance data.

Details on the implementation of the configuration and staffing design bases are provided in Reference 2, Section 18.5.

appropriate form. Because of the hierarchical nature of the information requirements a hierarchical organization of the displays is appropriate.

The Nuplex 80+ design addresses this basis through its information presentation methodology. The IPSO design provides plant level overview information as described in Reference 7 and Section 5.5.1 of this document. Key system level parameters are provided to the operator continuously on DIAS indicators. These are described in References 5 and 6. The CRT display system for the DPS is also based on a hierarchical structure with the top level display being IPSO, the first level dedicated to systems level monitoring, the second level for control and the third level for information for detailed diagnostics. This is completely described in Reference 5.

- o The Nuplex 80+ shall employ display techniques that allow rapid comprehension of the plant status by operators.

  The goal of providing information to the operator is to support his operational task performance. The methods employed to present the information are most effective when they quickly and efficiently allow the required task data to be obtained. This becomes increasingly important as the stress level of the operating staff increases during off-normal conditions.

  The primary means of facilitating rapid comprehension of plant status in the Nuplex 80+ man-machine interface is through spatially dedicated displays of key parameters. Key parameters include those most indicative of critical function or success path status to allow rapid assessment of safety status. Other key parameters relate to parameters requiring frequent surveillance for investment protection and parameters frequently monitored to support power production. By providing these parameters on spatially dedicated displays the operator is

5.2 INFORMATION PROCESSING AND DISPLAY

The following are design bases for the Nuplex 80+ information processing and display methodology.

- The Nuplex 80+ design shall reduce the quantity of data that must be mentally processed by the operators to minimize stimulus overload.

  Stimulus overload has been identified as a concern with conventional nuclear plant control rooms. The quantity of data generated from the plant is enormous and little data processing is performed in conventional plants before presenting it to the operator. This led to presentation of more information than a person can reasonably comprehend, particularly during plant upset conditions when many parameters may be changing. The 1979 TMI-2 accident provides a good example of key information being lost in the sea of information provided (Reference 4). Primary methods of addressing this in Nuplex 80+ are by cross-channel signal validation and reduction of data through related parameter correlation prior to display. These concepts are further discussed in References 5 and 6.

- The Nuplex 80+ design shall concisely relate displayed information of plant status to operator information requirements for general monitoring, control and detailed diagnostics.

  At various times during plant operation an operator requires different levels of information to support his operational tasks. His activities range from general monitoring of the entire process, specific systems or functions, to taking control of systems or subsystems to detailed diagnostics of specific components or processes. To best support these tasks the information presented to him should be processed into an relieved of the added task burden of accessing the information required for frequent monitoring activities or monitoring during times of high stress levels.

The Nuplex 80+ man-machine interface is designed to allow rapid comprehension of the information provided on DIAS and CRT displays. This is facilitated by appropriate use of digital displays, analog bar charts, deviation bar charts, trends and graphic presentation techniques. Colorgraphic CRT pages are designed using current human factors principles and criteria. Uniform symbology and dynamic conventions are employed throughout the man-machine interface design. The Nuplex 80+ display techniques are further discussed in Reference 5.

o The Nuplex 80+ design shall allow easy access of information at all levels.

In an advanced control room extensive use is made of computers for information processing and display. Less spatially dedicated information is presented than in comparable conventional control rooms, as computers provide serial presentations of data. The most important provision for easy access of information in Nuplex 80+ is the use of spatially dedicated displays for frequently accessed information, as discussed above. However, to facilitate efficient interaction with operators, the man machine interface must provide easy access to all levels of information. An efficient method of providing information access is through direct touch access to supporting data and menu selections. This access method takes advantage of a person's inclination to point.

The Nuplex 80+ man-machine interface features are designed to provide easy access to information. DPS display pages are accessed through dynamic touch target menus and touch access to detailed information through a point poke feature. Alarms are acknowledged and alarm messages are provided with a single touch of alarm tiles or DPS alarm targets. In response to acknowledgement through either media, a menu of CRT pages is displayed that gives direct access to pages that present supporting information. Discrete indicators provide supporting data through target touch access and menu selections. Touch targets on the indicator also result in a CRT page menu display for direct access to supporting CRT pages. Touch sensitive screens are used for process loop controls at the system level and to the subloop and component level through touch menu selection. The touch access features all provide easy access to Nuplex 80+ information. They are more fully described in Reference 5.

o The same displays that are used during normal operation shall be used by the operators during accident conditions to ensure their familiarity with the interface.

This basis is a design criteria provided for Post Accident Monitoring Instrumentation (PAMI) in Table 1 of Regulatory guide 1.97. Particularly when the operator is under stress during an accident, it is important that he is familiar with the displays that he is using to minimize the potential for operator error. This precludes the use of backup displays which are used only during accident conditions. The implementation of this basis is complicated by the requirements for expanded ranges of PAMI displays in Table 2, of Regulatory Guide 1.97. These ranges are often not compatible with the accuracy requirements of displays used during normal operation.

The Nuplex 80+ man-machine interface provides a unique approach to meeting this design basis. The discrete indicator algorithms continuously compare the validated parameter values to the PAMI instrument channels. If the comparison is acceptable the validated value is useable for post accident operation. This is indicated to the operator on the display. If the values disagree, an alarm is generated and the operator can then select a specific PAMI channel for display. Both PAMI and normal parameters are provided on seismically qualified DIAS displays. This method allows the normal parameter displays and ranges to be used during accidents without compromising the qualification criteria on the indications. This design is further described in Reference 6 and additional design bases are provided in Section 5.6.

Nuplex 80+ also integrates normal and post accident displays related to the safety parameter display system (SPDS). Critical safety function and success path monitoring algorithms and displays are integrated into the DPS. This allows the operator to use the same interface to access SPDS information as he uses during normal operation. In conventional plants the SPDS is typically a back fit, stand alone system that is designed for use only during accidents, and therefore not used effectively due to unfamiliarity.

Carrying SPDS integration one step further, Nuplex 80+ uses the SPDS method of critical safety function monitoring for normal plant operation, as well. As critical functions are defined and monitored for safety functions, critical functions are also defined and monitored for normal power production. All critical functions (both safety and power) have primary success paths which are monitored for performance or readiness. Alarms and displays are specifically designed to support CFM/SPM monitoring and diagnostics. This common approach to power production and safety ensures the operator's familiarity with the man-machine interfaces to optimize his performance during accident conditions.

- o The information processing and display devices shall provide sufficient redundancy and diversity to preclude impact of plant safety or availability by equipment failures.

  The ability of the operator to monitor the plant process should not be compromised by equipment failures such that plant availability is immediately affected or safety is impacted. This includes protection against common mode failures.

  The Nuplex 80+ design accommodates display and processing failure without significant operator impact in three ways:

  1) Redundancy within the DPS and redundancy and segmentation within DIAS giving each individual system high reliability.

  2) Automatic data and alarm checking between DPS and DIAS and global alarm acknowledgement to make the DPS/DIAS independence invisible to the operators.

  3) Sufficient plant indications and alarms provided through DIAS to allow continued operation for 24 hours without the DPS. Similarly, failure of DIAS results in no cost information since it is all available via DPS.

  These concepts are more fully discussed in Reference 5 and Reference 1.

5.3 ALARM PROCESSING AND DISPLAY

The following are design bases for the Nuplex 80+ alarm processing and display methodology.

- The Nuplex 80+ alarm methodology shall reduce the number of alarms generated to minimize stimulus overload.

  Alarm overload has been identified as a human factors concern with conventional nuclear plant control rooms. Particularly during post-trip transients, the overwhelming number of alarms generated often mask those alarms that are of real significance and increase the information processing requirements of the operational staff. Conventional alarm systems have no processing capability to provide clear, succinct information which reduces operator processing requirements. The Nuplex 80+ alarm design reduces the number of alarms generated by basing alarms on signals validated by cross-channel comparison and by providing alarm logic and setpoints contingent on applicable plant mode and equipment status. This results in an optimum set of alarms which provide all required alerting information while minimizing stimulus overload.

- Nuplex 80+ alarms shall be displayed with distinct visual cueing in accordance with the priority of required operator response.

  When dealing with multiple alarms it is important for the operational staff to know the relative importance of incoming alarms. This helps focus the operator's attention appropriately and helps in determining which plant conditions, represented by the alarms, require action first. The Nuplex 80+ ACC features a dynamic alarm prioritization methodology based on the time requirements for operator response. The following alarm priority categories were established:

Priority 1 - Immediate Action
Priority 2 - Prompt Action
Priority 3 - Caution
Operator Aid - Status Information

The salience of each alarm priority display method correlates directly to the importance of that priority i.e. the display of Priority 1 alarms is most salient. The priority of individual alarms are displayed through the same unique visual coding on both spatially dedicated alarm tiles and CRT display pages (including IPSO).

The Nuplex 80+ alarms are assigned to priority categories based on the time required for operator response. The types of alarm conditions in each priority are as follows:

Priority 1

1. Conditions that may cause a trip in less than 10 minutes.

2. Conditions that may cause major equipment damage.

3. Personnel/Radiation hazard.

4. Critical Safety Function violation.

5. Immediate Technical Specification Action Required.

6. First-Out Reactor/Turbine Trip.

Priority 2

1. Conditions that may cause a trip in greater than 10 minutes.

2. Technical specification action items that are not Priority 1.

3. Possible equipment damage.

Priority 3

1. Sensor deviations.

2. Equipment status deviations.

3. Equipment/process deviations not critical to operation.

More detail related to Nuplex 80+ Alarm prioritization can be found in References 5 and 6.

- Alarm displays shall aid the operator in quickly correlating the impact of the alarm on plant safety or performance.

  Alarms are required in a nuclear plant control room because the large number of relevant systems, subsystems and components are represented by too many parameters for control room personnel to individually monitor. Conventional annunciators typically provide alarms which indicate that a setpoint has been exceeded on a specific parameter. These alarms require the operators to assimilate the safety or performance impact of the alarming condition. This may be feasible when one or few parameters are in alarm but becomes a burden or an impossibility during multiple alarm conditions. These are the conditions when an alarm methodology should aid in assessing the impact of process and system deviations to allow operators to facilitate initiation of corrective action.

The Nuplex 80+ alarm methodology uses display techniques that correlate specific alarm conditions to impact on plant safety or performance. This is accomplished by three alarm features. Grouped alarm displays highlight the nature of the problem rather than the symptom indicated by a specific parameter alarm. For example all reactor coolant pump alarms are grouped into four alarm groups for each RCP, quickly indicating the location of the problem. In addition Nuplex 80+ panels have fixed, spatially dedicated alarm displays to take advantage of pattern recognition to avoid individual assessment of alarms. Multiple alarms in a specific plant system or function quickly indicate the location of the problem(s) through the spatially dedicated alarm tiles. In addition spatial dedication of tiles is effective in indicating where no alarms exist hence informing operators where no problem diagnosis is required. Finally the IPSO display and critical function CRT pages show the critical functions (both safety and power production) and success paths impacted by alarms.

The Nuplex 80+ alarm features are further discussed in References 5, 6 and 7.

o Nuplex 80+ alarms shall ensure that all alarms are recognized by operators without excessive task burden.

In performing its alerting function the annunciator system must guarantee that the alerting signal is perceived by the operator while not distracting operators from responding to the alarm by requiring an excessive amount of effort for acknowledgement. Conventional hardwired annunciator systems typically have a global silence and global or panel based acknowledgement capability. This allowed easy acknowledgement but did little towards assuring each condition was perceived.

Nuplex 80+ addresses this concern by requiring individual acknowledgement of incoming alarms or acknowledgement in small functionally related groups. The task burden associated with acknowledgement is minimized by allowing alarms to be acknowledged through either the spatially dedicated panel alarm tile (Section 5.5.2) or any CRT (Section 5.5.4). Panel alarm tiles allow rapid assessment and acknowledgement of multiple related alarms. Acknowledgement through the CRTs allows an alarm or alarms to be brought to the operators location in the control room without requiring him to move. Momentary audible alerts are used for alarm state changes, with periodic reminder tones to eliminate the need for a silence button. If acknowledgement of many alarms becomes a problem the operator can use the global "stop flash" to deal with only the Priority 1 conditions and then return to the lower priority alarms as time permits. "Stop Flash" causes all alarm flashes on the CRT and tiles (except unacknowledged Priority 1 Alarms) to go to the acknowledged or reset state (as appropriate). This does not acknowledge or clear the alarm but simply allows a deferred acknowledgement. The "Resume" feature causes all unacknowledged alarms to flash again in their appropriate unacknowledged state, allowing proper single point alarm acknowledgement. This feature eliminates the present operator tendency to hold the acknowledge button to avoid annoying flashes during conditions of high alarm density.

The acknowledgement features of the alarm system are described more fully in Reference 5.

- Nuplex 80+ alarms shall provide quick, direct access to supporting information to enhance operator response to alarm conditions.

An equally important annunciator function to informing operators of an alarm condition is to guide the operator's initial response to the deviation. An operator should be guided to information which will support his diagnostic activities and enhance his ability to take prompt corrective action.

The Nuplex 80+ alarm methodology accomplishes this in three primary ways. First the panel alarm tiles are functionally grouped with discrete indicators related to the same system and functions to facilitate proper alarm/display integration. Upon acknowledgement of an alarm, either by panel tile or CRT, a concise display of the specific alarm condition including an alarm message, the current parameter value and the setpoint is provided on the CRT and at the bottom of the alarm tile matrix. This immediately gives the operator guidance for his diagnosis and corrective action. Finally, upon acknowledgement, selection options for CRT pages related to the specific alarm are provided to allow quick access to further diagnostic information to support initiation of corrective action. The Nuplex 80+ alarm methodology guidance features are also discussed in Reference 5.

o The Nuplex 80+ alarm methodology shall provide redundancy and diversity in alarm processing and display.

As intelligent alarm processing and CRT alarm display and acknowledgement become fundamental to control room designs it is important for operators, who are used to hardwired annunciators, to have confidence in the advanced designs. This relates both to the accuracy of the alarm processing and the reliability of the display equipment. Neither a processing nor equipment failure should lead to a situation such that plant safety or performance is impacted.

This is addressed in Nuplex 80+ by having Priority 1 and 2 alarms processed and displayed independently by DIAS and DPS. The two systems cross check their alarm outputs and issue an alarm when deviations exist. This provides both redundancy and diversity in the alarm methodology. The continuous cross-checking is invisible to operators and the interfaces of the systems are integrated to appear as one system.

Further details on the alarm system redundancy and diversity are provided in Reference 5.

o The Nuplex 80+ alarm system shall provide sufficient expansion capability for changes expected during the life of the plant.

As systems, components, operational procedures and licensing analyses change during the life of the plant it is likely that additional alarms will be required. Alarm expansion has been difficult in conventional plants because of required hardware changes and a limited potential for expansion. Future plants must provide the capability for easy expansion and changes. The Nuplex 80+ alarm system allows easy expansion because both the DIAS and DPS are software based systems, including the displays. Thus alarm expansion will not require hardware changes.

o The alarm system shall provide the capability for "operator established" alarms.

Operators do not have the capability to change pre-programmed alarm logic or setpoints (this is considered a system maintenance function accessable outside the control room). However it is likely that operators will want to establish temporary alarms and setpoints to support specific evolutions or monitoring tasks based on the current plant status. The capability for operator defined alarms allows better detection of conditions before they deteriorate to impacting plant safety or performance and will foster operator acceptance of the alarm system. The Nuplex 80+ design allows establishing Priority 2 operator defined alarms through the CRT interface.

This feature is discussed in Reference 5.

5.4 CONTROLS

- The Nuplex 80+ automation philosophy shall be to maintain the operator in the control loop as much as possible.

  In general the tendency shall be to manual, not automatic controls. This keeps the operator in the control loop and therefore better prepared to handle off-normal conditions.

- Automatic controls shall be utilized where manual control would not be suitable due to workload (considering staffing levels), required response time, frequency of use or complexity of manual actions.

  Some control functions are considered beyond human capability due to task overload, complexity or diagnostic-decision-action response times. Other control functions may be within human capability but due to the frequency and routine or continuous nature of the control action they would become monotonous and therefore subject to frequent human error.

- Where manual controls are employed operator aids shall be provided to assist in the decision making process. The operator aids shall alarm when expected control limits are violated and, where appropriate, shall take automatic corrective actions to avoid plant shutdown.

  Keeping the operator in the control loop is a primary consideration in assuring operator preparedness and vigilance. However it is recognized that manual actions are subject to human errors. Therefore, computer aids such as COLSS and MDS are utilized to help the operator in keeping the plant within acceptable operating limits.

- Controls that require operator intervention shall be spatially dedicated to simplify access and speed of response.

Control access is a key consideration in a control scheme that relies significantly on operator intervention. In Nuplex 80+ all controls that require manual operator actions have spatially dedicated controls. Controls accessed through selectable displays are used for automatic control loops that normally require little or infrequent operator interaction.

In general component controls (ON/OFF) utilize dedicated pushbuttons. An exception to this are the component controls that are an integral part of a continuous process control loop (e.g., pilot solenoid controls on electro-pneumatic valves, circuit breakers or proportional heaters). These controls are selectable via the process controllers (see Section 5.5.5) since the operator normally controls the analog part of the device and is not normally required to interact with the pilot device.

- o Automatic control actions that are necessary for plant safety, equipment investment protection or to prevent personnel hazard shall not be subject to operator selection of the automatic mode. This philosophy is also applied to automatic control functions that are critical to power production and have no defined manual control tasks.

  To avoid human errors important automatic control actions are in effect at all times. Various levels of operator override are available to allow discretionary operator intervention after the control action has occurred.

- o Automatic controls that must have auto/manual mode selection shall have permissive interlocks to select the manual mode (e.g., process is outside auto control range) or shall be alarmed when the manual mode is selected.

5.5 DISPLAY AND CONTROL EQUIPMENT

5.5.1 Integrated Pr(ss Status Overview (IPSO)

Nuplex 80+ incorporates a large panel overview display called the Integrated Process Status Overview (IPSO) into the advanced control room design. The following are the design bases related to IPSO:

o The Nuplex 80+ IPSO shall present a relatively small quantity of readily comprehendible information to allow operators to obtain an overview or "feel" of the plant condition.

  A plant level overview display must address two operational concerns for nuclear power plant control rooms. First, due to the complexity and quantity of power plant processes the operator is overburdened with sensor, status and alarm information. To be readily comprehended this data must be reduced to a relatively small quantity of easily recognized and understood information. This is especially important during off-normal stressful conditions. The second operational basis for the plant level overview display results from the fact that an advanced control room design relies much more on serial presentations of data (e.g., CRTs) than conventional control rooms. As less information is presented in parallel in the control room, the ability of plant operators to obtain an overview or "feel" of the plant condition is diminished. To obtain a plant overview may require paging through numerous CRT display pages even at a high level in the display hierarchy. An overview display meets this operational need.

o The IPSO shall be displayed on a large format dedicated display in the Nuplex 80+ control room.

  Display of the plant level overview on a large format dedicated display addresses two additional but equally important operational concerns. First, operator tasks often require detailed diagnostics in very limited process areas. However, maintaining continuous awareness of plant-wide performance is necessary. This problem is presently addressed by multiple operators and the continuous presence of a control room supervisor whose job it is to maintain this plant level awareness. Reduced staffing objectives for the ALWR control room require one operator to handle detailed tasks, while also maintaining plant level awareness. The dedicated large panel can be viewed from anywhere in the control room and its simplicity and fixed forma makes it easily understood at a glance. Therefore, it provides an operator a continuous indication of plant performance regardless of the detailed nature of the task that may be requiring the majority of his attention. Second, the proper coordination and direction of the control room operating staff is important during all modes of plant operation. The large format overview provides a common mental model of the plant to facilitate a common plant visualization among all plant operational groups. This promotes a more effective communication process among plant personnel.

To address these operational design bases for providing required overview information in an advanced control room, Nuplex 80+ includes a large panel display called the Integrated Process Status Overview (IPSO). The IPSO continuously displays spatially dedicated information that provides the status of the plant's critical safety and power production functions. This information is presented using a small number of easy to comprehend symbolic representations that are the result of highly processed data. This relieves the operator of the burden of correlating large quantities of individual parameter data, systems/component status and alarms to ascertain the plant functional conditions. This continuously accessible and quickly comprehendible information directly aids the operating staff in determining current operating status, organizing operational concerns and establishing priorities for action.

The IPSO large panel display is visible throughout the control room and readable from up to 40 feet. The display is also presented as the highest level of the CRT display page hierarchy and is thus available on any control room CRT, in the TSC, EOF and at the remote shutdown panel. The IPSO is integrated with the rest of the control room man-machine interface to quickly and efficiently guide to operators to supporting information for operational concerns indicated on IPSO.

The functional bases for IPSO information are to indicate to the operator:

- Highest priority alarms indicative of the status of critical safety and power production functions, in order to focus the operator's attention on concerns impacting the ability to keep the plant safe and make megawatts, respectively.

- A small set of parameters most indicative of critical function status to improve an operator's and supervisor's early awareness of changing plant conditions. This data is presented either numerically or symbolically, based on the most useful format for the operator.

- System operational status, non-operational availability and highest priority alarms for critical function success paths (i.e., the primary systems utilized to maintain critical functions)) to improve operator's response to transient conditions.

This information is presented through an overview schematic of the plant's main heat transport and fluid flow systems. The IPSO display uses the same display conventions as adopted for the rest of the Nuplex 80+ information systems.

A prototype of the IPSO large panel display was evaluated through dynamic simulator experiments at the OECD Halden Reactor Project in Halden, Norway. The results of these evaluations indicate that the IPSO aided operators in detecting abnormalities and making appropriate diagnoses. The IPSO provided the subjects with a good, clean image of the plant and process with good use being made of both alphanumeric and symbolic data. The conclusion is that the IPSO experiments clearly advocate the implementation of a large screen plant overview in the control room. Halden reports (HWR-158 and HWR-184) document the IPSO evaluation.

The IPSO large panel display is approximately 4 ft. x 6 ft. The IPSO panel display and processing hardware are qualified for seismic integrity (to prevent personnel hazard) but are not functionally qualified for seismic events. Functional seismic qualification is not required because other spatially dedicated displays in the Nuplex 80+ control room present sufficient information to support adequate (although not optimum) operator's response during or after a seismic event. The overview panel's critical function and success path status information is part of the plant's SPDS function. SPDS designs are not required by the NRC to be seismically qualified.

5.5.2 Alarm Tiles

The following are design basis for the Nuplex 80+ alarm tiles:

Provide spatially dedicated alarm displays for conditions requiring quick operator response.

Spatially dedicated Alarm tiles are provided for Priority 1 Alarm (immediate operator action required) and Priority 2 Alarm (prompt operator action required) conditions. The alarm tiles present this information using conventional spatially dedicated display techniques which present all alarms in parallel. This takes advantage of the good attributes of conventional alarm tile systems. Other design bases provided here and in Section 5.3 are intended to resolve problems with conventional alarm tile systems.

o The Nuplex 80+ alarm tiles shall reduce the number of alarm tiles to minimize information overload.

During conditions that can actuate alarm tiles, an operator can be overburdened with the quantity of alarm tiles he must comprehend, especially during a plant upset. The Nuplex 80+ Alarm Tiles reduce this burden (and quantity of alarm tiles) using several techniques:

1- combining similar alarms under a single alarm tile (i.e. all Reactor Coolant Pump 1A cooling system alarms under a single tile). The alarm tile informs the operator of a high level problem related to a piece of equipment or process and a dynamic alarm message provides the detail related to the several problem.

2- Alarms are the result of prior signal validation, therefore separate channelized alarm tiles can be replaced by a single tile.

3- Separate tiles for different priority conditions such as low and low-low are replaced by a single tile with a dynamic priority display.

4- Alarm tiles are provided for Priority 1 and 2 conditions only. Priority 3 alarm and operator aids require much slower operator response therefore they are displayed via CRTs only. This reduces the number of tiles providing greater salience to Priority 1 and 2 conditions.

Alarm tile implementation is discussed in detail in References 2, 5 and 6.

o Display alarm tiles shall use techniques that help the operator quickly correlate the impact of the alarm on plant safety or performance.

During conditions that can actuate multiple alarm tiles, the operator may have difficulty identifying an alarm's impact on plant safety or performance because tile messages do not identify the nature of the problem. Additionally, the alarm tiles often must be read and processed one at a time because they do not support pattern recognition, a technique that helps speed up operator processing of related alarms.

The Nuplex 80+ alarm tiles are arranged in spatially dedicated groups which highlight the nature of the problem rather than symptoms. These alarms are arranged by system and/or functional groups, thus achieving spatial dedication and allowing pattern recognition.

Alarm tile implementation is discussed in detail in References 2, 3, 5 and 6.

- o Alarm tile acknowledgement shall provide quick direct access to supporting information.

Grouping multiple alarms under a single alarm tile may not provide the operator with the specific condition causing the alarm and thus lead to a delay in correlating the information and subsequent response. To resolve this concern, the alarm tiles on Nuplex 80+ are provided with dynamic message windows that identify the specific condition causing the alarm. References 2, 3, 5 and 6 provide additional information on alarm message windows.

F. Alarm tiles shall be seismically qualified for functionality during and after an OBE and SSE.

Alarm tiles will be a valuable source of information during plant emergencies. Seismic qualification of alarm tiles is required to facilitate operation during emergencies that is as close as possible to normal conditions.

5.5.3 Discrete Indicators

The following are design basis for Nuplex 80+ discrete indicators:

- Discrete indicators shall provide spatially dedicated displays that mimic conventional analog type indication and recorders, for parameters that are most indicative of the process status and/or system and function performance.

  Spatially dedicated displays are needed to insure that the operator has continuous (at a glance) access to key parameters because selectable information access, as on CRT displays, takes time and is not available without operator action.

  The Nuplex 80+ discrete indicators provide continuous display of all key plant parameters in the format (i.e. trend, digital, analog) needed for a particular process. References 2, 3, 5 and 6 provide additional information on spatially dedicated displays.

- Discrete indicators shall provide selectable displays for plant data required for operation without the plant computer.

  A conventional control room contains hundreds of indicators, many of which are infrequently used. These indicators take up a large amount of panel space and are difficult to read without extensive operator movement. The large panels needed for these indicators are complex and difficult to learn and use due to the size. Advanced control rooms make increasing use of CRTs driven by the plant computer to reduce panel size and thereby improve operability. The operating staff must be provided with an independent system capable of supplying plant information needed in the event that the CRT information system becomes unavailable. The Nuplex 80+ discrete indicators provide all parameters needed for operation for up to 24 hours without the plant computer. This includes technical specification surveillance items and accident monitoring instrumentation to maintain plant safety. It also includes instrumentation monitored to ensure plant availability and protect the utility's investment in major equipment. These indications are provided through selectable displays on a small number of discrete indicators (usually one or two per panel section). The number of Nuplex 80+ discrete indicators is significantly smaller than the number of indicators in a conventional control room. All important information that is not need for continuous display is available via a touch sensitive menu on the Nuplex 80+ discrete indicators. These displays are organized into the same functional groups as alarms, CRT pages and controls. These operator selectable menus reduce panel size and speed operator access to this important, but infrequently used information.

References 2, 3, 5 and 6 provide additional information on continued operation without the plant computer through use of the independent discrete indicators.

- o Discrete indicators shall provide a reduction in the number of indicators through auto ranging and signal validation techniques.

  A conventional control complex contains many indicators displaying similar or identical process parameters (i.e. as many as 20 indicators for pressurizer pressure). The operator is burdened with the task of determining which instruments are reading incorrectly (i.e. signal validation) and determining the appropriate indication for the present process conditions (i.e. wide range, narrow range, post accident instruments, etc.).

The Nuplex 80+ discrete indicators continuously validate information, check PAMI sensors and shift ranges automatically to provide the operator with a single easy to locate, spatially dedicated display of any process where multiple sensors are used. References 2, 3, 5 and 6 provide additional detail on the discrete indicators automatic ranging and validation features.

- o Discrete Indicators shall provide continuous display of Regulatory Guide 1.97 Category I parameters.

  To meet post accident monitoring requirements, Reg. Guide 1.97 Category 1 parameters are continuously displayed on a dedicated set of discrete indicators located on the safety monitoring panel. In addition, these same parameters are available on separate discrete indicators which are integrated into the appropriate functional groups throughout the control room. This is further discussed in Section 5.6.

- o Discrete Indicators shall be seismically qualified for functionality during and after the OBE and SSE.

  Spatially dedicated key plant parameters will be extremely useful during situations of high stress such as emergencies. To facilitate operation during emergencies that is as close as possible to normal conditions, seismic qualification of discrete indicators is required.

5.5.4 CRT Displays

The following are design basis for Nuplex 80+ CRT Displays:

- CRTs will provide access to essentially all plant information within the control room or remote locations.

  Due to the large quantity of information needed by the operating staff, a means to bring all of this information to individual workstations is needed. The Nuplex 80+ CRTs contain all power plant information in a structured hierarchical format. They provide graphical layouts of power plant processes in the most appropriate format. References 2, 3, 5 and 6 provide more detail on information access through CRTs.

- The CRTs display system shall duplicate and verify all discrete alarm and display system processing and identify any significant differences.

  In an advanced control room, all information is prioritized, with the most important alarms and indication processed by the Discrete Indication and Alarm System (DIAS). In the event that some part of the DIAS fails, the operator must have a duplication of this vital information. The CRTs provide a functionally independent, redundant method of displaying all vital indications and alarms. Additionally the DPS, via the CRT, alarms any significant differences between the redundant displays and alarms. References 2, 3, 5 and 6 provide additional detail on the information verification function of the DPS.

- CRT pages shall display information in an organized, easy to obtain and easy to learn format.

As CRTs are increasingly used in advanced control rooms, their serial means of information access must be set up in an organized, easy to obtain and easy to learn format. The Nuplex 80+ CRTs contain information in a structured hierarchical format. This format has IPSO at the top of the hierarchy with three levels of display pages below it. Level 1 pages are used for general monitoring, Level 2 pages provide useful information for controlling plant systems and components and Level 3 pages provide detailed diagnostic information on components and processes. Touch sensitive controls provide easy access. References 2, 3, 5 and 6 provide additional detail on DPS CRT display organization.

o CRTs shall provide the control room operator with the ability to acknowledge and obtain information on all control room alarms.

  A means to acknowledge and access all control room alarms from any control room work station is needed in an advanced control room to help minimize required operator movements between panels. From any CRT in the Nuplex 80+ control room the operator can acknowledge and obtain alarm information via touch sensitive alarm targets and a touch sensitive menu system for all control room alarms. References 2 and 5 provide additional information on the alarm acknowledgement through CRTs.

o CRTs shall provide quick direct access to supporting information to alarm conditions.

  To enhance operator alarm response, the CRTs provide quick direct access to supporting information. When Nuplex 80+ alarms are acknowledged on the CRTs, the menu at the bottom of the CRT changes to enable selection of a CRT page that provides additional detail on the alarming condition. Reference 5 provides additional detail on CRT alarms and menuing.

5.5.5 Process Controllers

The following are design bases for Nuplex 80+ process controllers:

A. Process controls shall be separated from displays.

To minimize the potential for human error, deliberate action shall be required to actuate process controls. Separation of controls from displays helps accomplish this. The Nuplex 80+ process controls are located on the bench board (lower) section and the displays are located on the vertical (upper) section of the control panels. Reference 2 and 3 provide more detail and examples of Nuplex 80+ process control layouts.

B. Process controls shall be grouped by function.

To insure that that process controllers support operational functions they should be located in functional groups with component controls and related indications. Nuplex 80+ controls and indication are grouped by function to support operational functions. Reference 3 discusses control panel layout.

C. Process controllers shall provide continuous display of all parameters being controlled.

To insure that the operator has all information necessary for optional process control, continuous display of all controlled parameters must be provided. The Nuplex 80+ process controllers have continuous display of the following: mode of control, status of subgroup control, setpoint, deviation from setpoint, process value and channel identification. Reference 6 provides more detail on parameters displayed on process controllers.

D. Process controllers shall allow easy access to separate controls for each control loop.

Easy control loop interaction is needed to insure that the operator can respond quickly to plant process problems with minimum probability of error. The Nuplex 80+ process controllers are designed utilizing generic display and control features. The controls for all master and subgroup process control loops are accessed via touch sensitive controls with a single touch. Control signal inputs, operator-set control limits and component selections need less rapid access and are available via no more than a two step touch control scheme. References 5 and 6 provide detail on process control access.

E. Redundant process controllers shall be provided for all controlled parameters and components in the Nuplex 80+ MCR.

Failure of a process controller display device must not prevent the operator from being able to take control of a process or component. To address this concern the ACSC safety monitoring panel provides access to all CCS controls and indications through channelized CCS operators modules. These provide redundant access to safety related components in Channels A, B, C and D as well as non-safety channels X and Y to address failure of the primary control device.

5.5.6 Component Controls

The following are the design bases for Nuplex 80+ component controls:

- o Component Controls shall be separated from displays.

  To minimize the potential for operator errors, deliberate action should be required to activate component controls. To help accomplish this Nuplex 80+ controls are separated from displays. The component controls are located on the benchboard (lower) section and the displays are located on the vertical (upper) section of the Nuplex 80+ control panels. References 2,3,5 and 6 provide more detail and examples of Nuplex 80+ component control layouts.

- o Component Controls shall be grouped by function.

  To ensure that the component controls support operational functions they are located in functional groups with the process controls and related displays. Nuplex 80+ controls and indication are grouped by function to support operator functions. Reference 3 discusses control panel layout.

- o Distinctive component and function control switch coding shall be used.

  Distinctive component and function control switch coding allows differentiation between different components (i.e. centrifugal pump vs. stop valve) and functions (i.e. on, off) to prevent operator errors. All Nuplex 80+ component control switches are designed using a generic coding scheme. Red status indicators for active or open and a green status indicator for inactive or closed. Blue/amber status indicator lights/switches are used to indicate and select automatic control. In addition to color coding, position coding is used (i.e. the red switch is always located above the green switch to reinforce control distinction). References 3 and 5 provide additional detail on component control switch coding.

o Component control switches shall be identified with clear and consistent switch labels.

Clear, consistent switch labels are needed in order to provide the operator with required information and minimize the probability of errors. The Nuplex 80+ component control switch labels display the following information: functional identifier (name of control, unambiguous identifier (unique number), control options available (on, off, auto) and current component state (on, off, auto). Visual coding is also used, including: alpha-numeric/graphic and relative position color coding. References 3 and 5 provide detail on Nuplex 80+ switch labels.

o Control switches shall provide abnormal status indication consistent and integrated with CRT displays.

To detect component failures the operator needs to be informed when equipment that should be operating is not operating or when equipment is not in its desired state (i.e., on, off, auto, open, closed, etc.). The Nuplex 80+ component controls contain logic that generates an alarm and flashes the component control backlight switch (if flash mode is enabled by the operator) when an abnormal condition occurs. (i.e. for example, for the abnormal condition "valve full open" the red status light flashes and the green status light is off. Reference 5 provides additional detail on abnormal status indication provided by component controls.

o Automatic control switches shall unambigously identify the automatic control action that will occur.

In conventional control room selecting the auto selection for a component may result in any number of different automatic control actions. As a result the operator must remember the automatic control response of several hundred different controls. Nuplex 80+ control switches clearly distinguish control actions such as:

- Single component cycling
- Multiple component sequencing
- Standby auto start
- Automatic sequence rotation

As a result, the operators are more aware of the expected control system response.

o Operator override of automatic control signals is consistently applied and executed.

Nuplex 80+ controls shall provide varying classes of operator overrides for different types of control signals. Control signal overrides result in varying degrees of system impact which should be apparent to the operator. To facilitate this in Nuplex 80+ more important control signals (e.g. EFAS) are more difficult to override. This approach is applied consistently to avoid operator confusion and to provide better operator awareness of the potential consequences of override actions.

5.6 SAFETY RELATED DISPLAY INSTRUMENTATION (Reg. Guide 1.97)

The following design bases relate to the Nuplex 80+ Safety Related Display Instrumentation.

o Nuplex 80+ shall meet all qualification criteria (Categories 1-3) for a System 80+ set of Type A variables and the PWR types B, C, D and E variables listed in Regulatory Guide 1.97, Table 3.

Requirements for light water reactor instrumentation during and following accidents were established in Regulatory Guide 1.97. The guide describes an acceptable method to comply with NRC's regulations for instrumentation to monitor plant variables and systems during or after accident conditions.

The Nuplex 80+ design displays Regulatory Guide 1.97 Post Accident Monitoring Instrumentation (PAMI) parameters by three methods:

A dedicated DIAS segment (DIAS-P) provides continuous display of all Category 1 PAMI parameters. This segment is provided by an independent, DIAS segment with display on the safety monitoring panel. DIAS-P inputs come from only channel A and B PAMI sensors.

DIAS-N segments (independent from segment P) provide category 1 and 2 PAMI parameter displays integrated into the normal workstation displays. The displays indicate validated "process representation" values which are the result of automatic comparison of all safety and non-safety sensor inputs including cross checking with the channel A and B PAMI sensors. PAMI channels are selectable for continuous display on these indicators. The displays include both present value and trend indication.

DIAS processing and displays are seismically qualified for both channels. DIAS processing and data communication is redundant for both channels.

The DPS displays validated "Process Representation" values (the same as DIAS-N) through CRT displays and also provides permanent historical recording of PAMI parameters. The DPS is independent and diverse from both DIAS channels.

A complete description of how Nuplex 80+ complies with each Reg. Guide 1.97 criteria is provided in Reference 11.

5.7 ESF STATUS MONITORING (REG. GUIDE 1.47)

The following are design bases for ESF Status Monitoring in Nuplex 80+:

- o The Nuplex 80+ ESF Status Monitoring function shall help notify the operator about undesirable changes in ESF equipment/system status. This information shall be designed to guide the operator when a disturbance affects a number of systems by allowing the operator to quickly assess what system and equipment are available or properly performing. The ESF status monitoring information shall also help the operator determine what equipment need(s) to be activated, fixed, or properly aligned to activate a system or train of a system.

  ESF status monitoring is required by Reg. Guide 1.47. The Nuplex 80+ design provides indication for each ESF system or dependency (e.g., vital power supply or essential cooling water) to identify its is unavailablity or poor performance. The information associated with the overall status of ESF Systems and each train of a system is continuously displayed in a single location labeled "ESF monitoring". The single location for ESF status assessment provides operators with a means for quickly understanding to what extent ESF systems have been rendered inoperable (i.e. one or more trains) and to what extent ESF systems are improperly performing (i.e. one or more trains).

  The operator is able to determine what specific equipment associated with an ESF system is the cause of the system unavailablity or poor performance by viewing the lower level CRT display pages associated with those systems. Inoperable equipment on the lower level display pages is displayed with alarm status coding. The alarm message associated with the inoperable equipment indicates the cause of the inoperability (e.g. loss of power, improper valve position). Process parameters indicating poor performance (e.g. low flow) are also highlighted with alarm status coding.

The approach to ESF status monitoring is discussed in Reference 2, Section 18.7.16.

5.8 INTEGRATION OF OPERATOR AIDS

The following are design bases for the integration of operator aids into the Nuplex 80+ Man-Machine interface:

- Nuplex 80+ operational aids shall help and the operator in maintaining plant control by performing information processing, information organization, and information presentation to support the operator decision making process.

  Many of the tasks that present day power plant operators perform require a large amount of data comparison and data manipulation. These are the types of tasks that computers are well suited for. A man-machine function allocation has been performed for Nuplex 80+ to ensure machines are used for those functions for which they are best suited. The Nuplex 80+ operator aids address many of these functions.

- Nuplex 80+ operational aids shall be integrated into the "Control Room Information System" in an organization that is based on a performance model of the operator's data gathering process. From the operator's viewpoint the "Operator Aids" shall be primarily transparent, although upon any failure in computer processing the operator shall be presented with information that informs him of the processing failure and supports any subsequent or resulting diagnostic activities.

  In conventional control rooms many operator aids have been back fits and are thus designated as stand alone systems (e.g., SPDS, ICC monitoring). In an ACC operator aids should be integrated into the design to provide the optimum man-machine interface. Operational aids incorporated into the Nuplex 80+ control room are briefly described below.

Signal Reduction and Validation - The Nuplex 80+ control and information systems use signal validation for plant processes containing multiple sensors measuring the same or closely related process parameters. This feature reduces the operator's mental data processing task by comparing multiple sensor readiness to determine the correct process measurement value ("process representation"). Validated values are used for the operator's data gathering tasks, process control, and algorithm/alarm inputs. Validation algorithms employ signal averaging, screen bad data and notify the operator about undesired sensor deviations, deviations from PAMI sensors, and an inability to arrive at a valid value. If an algorithm can't validate data the algorithm fault selects the sensor closest to the last valid signal. An alarm notifies the operator of the processing problem, and the algorithm allows the operator to select a sensor to replace the algorithm's output. When the algorithm can revalidate subsequent data, the valid signal replaces the operator selected sensor.

Signal validation is utilized in an integrated manner in all Nuplex 80+ control and display systems. In the DPS, signal validation is used for "process representation" values shown on IPSO, Level 1, Level 2 and Level 3 displays. In addition Level 3 displays show raw sensor input values. Validated data is used for bar charts, trends and alarm generation. In DIAS signal validation is used for "process representation" values, bar charts and trends on discrete indicators and for alarm generation. In the PCS and process-CCS, signal validation is used to establish a "process representation" value for automatic control loops. The DPS continuously compares its own "process representation" values to those from DIAS and the control system and alarms unacceptable deviations.

Integrated Process Status Overview (IPSO) - IPSO is a large overview display centrally located above the Master Control

Console. IPSO also exists as a display page at the top/apex of the display page hierarchy. IPSO provides the operator with the information that he requires to quickly assess overall plant status. The IPSO assists the operator by reducing large quantities of plant data to a minimum set of easily recognized graphic symbols and key numerical values. It is fully integrated into the Nuplex 80+ information system through common HFE conventions, its critical function design basis and its utilization at the apex of the integrated DPS/DIAS information hierarchy. IPSO design bases are described in Section 5.5.1.

Alarm Handling - The alarm handling system used in the Nuplex 80+ MMI allows the operator to obtain alarm information that is best for determining the most limiting plant concerns. The alarm system uses alarm reduction, prioritization, and categorization techniques to allow the operator to be more efficient in his alarm handling tasks. The Nuplex 80+ annunciator system incorporates the following characteristics.

- alarms catagorized by panel section to provide quick spatial correlation to the systems effected

- alarms based on plant operating mode to eliminate nuisance alarms

- alarms based on equipment operating status (e.g. low discharge pressure is only applicable when a pump is running) to eliminate nuisance alarms

- related alarms grouped within a single tile (e.g. "RCP1 PUMP/MOTOR TROUBLE", "LOW PRESSURE" with dynamic display of priority distinction for degrading/improving conditions to reduce the number of alarm tiles

- alarms prioritized into the following operational categories to properly direct operator response

    a. Priority 1 - Immediate Action Items
    b. Priority 2 - Prompt Action Items
    c. Priority 3 - Operator Cautions
    d. Operator Aids (not representative of alarm conditions) e.g. bypass enabled for testing

- all alarms require individual operator acknowledgement to ensure operator recognition. However, alarm flash suppression can be used by the operator to temporarily suppress excessive alarm system noise thereby allowing deffered acknowledgement.

- alarms are fully integrated throughout all Nuplex 80+ display media with common processing and HFE conventions.

- alarm information is displayed and may be acknowledged at alarm tiles, process display pages, or alarm listings. Diagnostic activities associated with alarms can take place at control panels or CRT displays. Redundant and diverse alarm processing by DPS and DIAS is invisible to the operator.

Design bases for alarm processing are provided in Section 5.3.

Critical Function Monitoring - Power and safety functions are monitored in the Nuplex 80+ control room to inform the operator about overall plant process performance concerns. The concept of monitoring plant power production and safety functions provides a categorization of the power and safety related concerns into a manageable set of inform[illegible] that is representative of the various plant processes. An alarm of a critical power function is indicative of a degraded condition that represents a threat to maintaining power production. An alarm of a critical safety function is representative of a degradation in the ability to control a plant process related to safety. The integration of critical function monitoring for power and safety allows an operator to use diagnostic techniques during accidents that he also uses during normal operation. Critical function information is integrated into the MMI primarily through the IPSO and DPS CRT display hierarchy.

o Success Path Monitoring - To maintain or restore critical functions, key systems referred to as success paths must be employed. To help ensure that a success path performs as expected when called upon, success path availability is monitored in Nuplex 80+. Success path availability monitoring notifies the operator if system problems, or system dependency problems (e.g. voltage, cooling water, air pressure) will limit the effectiveness of a success path if it is activated. To aid the operator in addressing success path performance problems, algorithms used to provide information to the operator on undesirable performance of active success paths. Success path performance monitoring information allows the operator to quickly assess the performance of important success paths so that he may quickly concentrate efforts on restoring any inadequately performing systems to proper operations or choose an appropriate backup system. Success Path Monitoring for normal and safety systems provides an integrated monitoring approach for all modes of plant operation. Success path information on IPSO, CRT displays and the "ESF Monitoring" panel provides an integrated information display system in the control room. Design bases Section 5.7 provides additional information about success path monitoring of ESF systems.

- Core Limit Monitoring - Core Limit Monitoring is incorporated into Nuplex 80+ to assist operations by performing calculations to support optimization of fuel burnup during steady-state plant operation and to maintain adequate margins to operating limits during load changes. This feature assists the operator in controlling the plant at its most efficient performance levels. Core plant monitoring is integrated into Nuplex 80+ through DPS CRT displays, critical function monitoring for power production (i.e. reactivity control) and plant control through the megawatt demand setter.

- Periodic Surveillance Testing in Nuplex 80+ - Periodic surveillance testing aids the operator in performing manual plant surveillance testing requirements. This feature is utilized for those tests that cannot be conducted automatically. These computer aids increase plant reliability and safety by reducing the number of operator induced errors during manual periodic surveillance tests and ensuring that equipment is returned to pretest conditions. Automatic testing of the Plant Protection System is defined in Section 6.3.

5.9 REMOTE SHUTDOWN PANEL

The following are the design bases related to the Nuplex 80+ remote shutdown panel.

- o In the unlikely event that the control room should become inaccessible, sufficient instrumentation and controls shall be provided at the remote shutdown panel (RSP) to:

  (a) Achieve prompt hot shutdown of the reactor, subsequently referred to as hot standby per standard Technical Specifications (reactor subcritical at operating pressure and temperature).

  (b) Maintain the unit in a safe condition during hot standby.

  (c) Achieve and maintain cold shutdown of the reactor from the RSP.

  Damage to equipment in the control room shall not preclude operation of any required equipment at the RSP and a single failure in an active safety train shall not preclude a safety function from being accomplished.

  Remote shutdown facilities are required by federal regulations at all nuclear power plants. Specifically, General Design Criterion (GDC) 19 Of 10CFR50, Appendix A, stipulates that instrumentation and controls outside the control room be provided to permit prompt hot shutdown of the reactor and to maintain the unit in a safe condition. In the remainder of this document this condition, subcritical at operating pressure and temperature, will be referred to as hot standby for consistency with plant technical specification mode definitions. The subsequent capability for cold shutdown, using suitable procedures, is also required. Appendix R to 10CFR50 requires that alternative shutdown capability be provided if redundant safe shutdown circuits are vulnerable to a single fire.

The Nuplex 80+ Advanced Control Complex design includes a remote shutdown panel which meets the above criteria as an integral part of its design. The Nuplex 80+ remote shutdown panel includes two independent trains of safe shutdown controls, each isolated from the main control panels. Sufficient information is provided for each safe shutdown system to maintain hot standby. The man-machine interface for this instrumentation is consistent with the main control room. The Nuplex 80+ RSP also provides indication and control for the normal control systems used for maintaining hot standby. The RSP instrumentation provides centralized controls and indications necessary for achieving cold shutdown. If failures occur, sufficient communications and indications exist to achieve and maintain cold shutdown using suitable procedures and local control stations. The indication and control at the Nuplex 80+ RSP are physically separated and electrically isolated from the Nuplex 80+ main control room.

The RSP and control room are electrically isolated by qualified isolation devices to assure that no fault caused by damage in the control room is propagated to the RSP and visa versa. The RSP and control room are located in physically separate locations to preclude an event simultaneously causing evacuation of the control room and inoperability of the RSP.

Reference 12 documents the Nuplex 80+ RSP implementation with respect to specific requirements for the RSP.

- The RSP shall be designed for safe shutdown as the result of a control room fire or other event causing the control room to become uninhabitable.

  To meet fire protection regulations (CMEB 9.5-1), damage from an exposure fire within the control room must be considered. For this case, consideration of a single failure unrelated to the fire is not required. For other (non-catastrophic) events requiring control room evacuation a single failure must also be assumed (References 14 and 15). There are no industry criteria that require the RSP to be designed for mitigating accident conditions.

  The Nuplex 80+ RSP provides shutdown capability after damage and evacuation resulting from a control room exposure fire. For required shutdown systems, two trains of equipment that are each isolated from and operated independently (without interaction)of the main control room equipment are provided. Therefore the Nuplex 80+ design can provide all shutdown functions after a control room exposure fire with a concurrent single failure, although meeting the single failure criteria is not an industry requirement.

  For control room evacuation without fire the limiting single failure is a loss of power to one Class 1E power supply. This results in a loss of power to one train of safe shutdown components and controls. The Nuplex 80+ RSP is designed for this situation by providing two trains of controls for each safe shutdown system. This precludes loss of indication or control due to a single failure in either train, including loss of power.

Although the Nuplex 80+ RSP is not specifically designed for accident conditions, all Post-Accident Monitoring Instrumentation (PAMI) parameters are provided on the DPS CRT. In addition, PAMI parameters which are also required for safe shutdown, are provided by the DIAS-N displays on the RSP.

- A means shall be provided to accommodate transfer of control from control room to RSP in the event the control room becomes uninhabitable.

  Control is transferred from the Nuplex 80+ control room to the RSP by separate channel switches in the channel equipment rooms. This arrangement allows transfer to the RSP from outside the control room, yet minimizes the effect of inadvertent transfer through train separation.

  Another feature of the Nuplex 80+ control room is the ability to disconnect power to individual panels at circuit breakers from within the control room. This allows an operator to disconnect controls selectively before leaving the control room as the result of an internal panel fire or exposure fire. This prevents equipment from being cycled spuriously before the transfer switches in the equipment rooms can be reached. This also precludes potential damage to both trains of a safety system due to an exposure fire with the Nuplex 80+ panel design.

  The transfer action is bumpless with no impact on controlled equipment status. This is accomplished by using momentary control switches and maintaining control setpoints in the process systems and not in the man-machine interface devices.

- Security measures shall be provided to prevent or deter unauthorized access to the RSP.

The RSP is located in a separate room with access controlled by the site security system. A Priority 3 alarm is generated in the control room when the RSP room door is opened. Access to the equipment rooms containing RSP transfer switches is also controlled by site security. A Priority 2 alarm is generated in the control room when the equipment room doors are opened. A Priority 1 alarm is generated in the control room if a channel transfer switch is actuated.

- The design of the RSP shall allow testing during power operation.

Testing of the RSP is accomplished by transferring control from the main control room to the RSP by panel section and individual channel on that panel. This aids the operator in maintaining cognizance of which components are being tested, as only those on one panel section can be activated at a time. It also prevents multiple channels from being simultaneously tested which could result in compromising both trains of a safety system.

Other details on the implementation of the RSP in Nuplex 80+ including a panel layout is provided in Reference 2, Section 18.8.

5.10 MMI VERIFICATION AND VALIDATION

The following design bases relate to the verification and validation of the Nuplex 80+ man-machine inte.:ace.

- The Nuplex 80+ man-machine interface design shall be verified from a human factors perspective to ensure that all necessary indications and controls are available in the control room with proper characteristics to support required operator tasks.

  The objective of the human factors verification process is to assure that operator tasks can be performed in the control room with minimum potential for human error. The focus : `n instruments and equipment, not on operator skills and knowledge. The premise is that the control room should provide all information and control capabilities called for by the operator task action requirements generated by the functional task analysis.

  The verification process consists of two steps. The first step is to verify the presence (or absence) of instruments and equipment that provide the information and control capabilities necessary to implement each task. This step will be referred to as the verification of availability. The second step is to determine whether the man-machine interfaces provided by the displays, controls, and other control room features are effectively designed to support task accomplishment. This step is referred to as the verification of human engineering suitability.

  The Nuplex 80+ man-machine interface verification process ensures both indication and control availability and suitability.

Availability of necessary indications and controls is verified by using information and controls requirements generated during the tasks analysis and experience-based instrumentation list generated during the panel design process. These are compared with the Nuplex 80+ instrument and control list to ensure all needed indications and controls are available to the operator. Characteristics, such as range and units, are also confirmed during this process. Additionally, this verification indicates the existence of any extraneous or unnecessary displays or controls that should be eliminated from the panels.

The suitability of the verification focuses on the standard man-machine interfaces used in Nuplex 80+. Each display and control device is evaluated against task analysis usage data to ensure that it is suitably designed for its intended usage. Individual prototypes of the multi-purpose displays and controls are utilized to evaluate manipulation and access mechanics of specific information or controls. Representative prototypes for the Discrete Indication and Alarm System (DIAS), the Data Processing System (DPS), process controllers and component controls are evaluated.

The Nuplex 80+ verification process and results are documented in Reference 13.

o The Nuplex 80+ man-machine interface design shall be validated to ensure proper integration of control room components to support operational functions.

  The objective of the human factors validation process is to determine whether the functions allocated to the control room operating crew can in fact be accomplished effectively within (1) the structure of defined operating and emergency procedures and (2) the design of the control room. In addition, the process of validation provides an opportunity to identify human engineering discrepancies that may not have become evident in the design processes or systematic review. The process of validation is associated with function execution and evaluates the integrated control room configuration.

Validation of the Nuplex 80+ control room design (per NUREG-0700) ensures that all operator interactions and dependencies on the design are supported for all operator functions. The validation process is performed in a two-phase approach. Phase 1 of Nuplex 80+ validation focuses on the following:

A. Evaluation of the integration of all display and control components, i.e., CRTs, alarm system, and discrete indicators.

B. Demonstration of one-man operation at the MCC for normal operation from hot standby to full power, including the first 10 minutes of a reactor trip.

Phase 2 of the validation uses a full scale partially dynamic mockup with plant specific emphasis to demonstrate successful integration of control room instrumentation and controls with operating procedures to support all required operator functions.

Details of the verification of the Nuplex 80 design is provided in Reference 13 and the full scope of Nuplex 80+ verification and validation activities is discussed in Reference 2, Section 18.9.

5.11 OPERATION WITH MAN-MACHINE INTERFACE FAILURES

- o The Nuplex 80+ design shall provide redundancy and diversity in information processing and display such that equipment failures do not impact availability and safety, and operators have confidence in the intelligent processing and display techniques.

  Information is processed and presented in Nuplex 80+ via two independent and diverse display systems; 1) The Data Processing System (DPS) and the Discrete Indication and Alarm System (DIAS). Data from both the DPS and DIAS play an important man-machine interface role in the Nuplex 80+ design. DIAS provides sufficient indications and alarms such that plant operations can continue without the DPS. If DIAS fails, there shall be no loss of important information in the control room. Continued plant operation will be subject to technical specification limits regarding loss of qualified information displays. To minimize these restrictions DIAS is designed with two independent channels for Regulatory Guide 1.97 Category 1 instrumentation (i.e. for Post Accident Monitoring).

  The DPS shall be designed for high availability and reliability. The DPS design accommodates the failure of any single computer hardware element without loss of functionality. Use of multiple communication channels, component redundancy, and automatic failover to backup systems are employed, to achieve this goal. The DPS provides all plant information in a human factored hierarchical format on CRT pages. The DPS also provides inputs for the IPSO large display format. The design bases of the DPS are further described in Section 6.1.

- o The Nuplex 80+ design shall provide sufficient indications and alarms to allow continued plant operations for 24 hours without the DPS.

Without the DPS the operator can use the DIAS for his information gathering requirements. The DIAS contains all safety related data and power production data that supports continued power production for a minimum of 24 hours. The operator is notified about Priority 1 and 2 alarm conditions via the alarm tile matrices on each panel and uses the discrete indicators on each panel to gather supporting information or conduct diagnostic activities. Each DIAS discrete indicator is related to a process, major component, or major parameter. The discrete indicators provide the same validated data and access to individual sensor values, as is available on the DPS CRT pages.

The 24 hour time period was selected based on the DPS Mean Time To Repair (MTTR) and the impact on Technical Specification surveillance caused by loss of the DPS. The DPS MTTR is approximately 1 hour based on board replacement maintenance methods. However by conservatively assuming that time may be needed to get a technician to the site, an 8 hour basis for continued operation was originally selected. Upon investigating the required additional monitoring by operators without the DPS, there was little difference between loss of the DPS for 8 hours and 24 hours. Hence extending the basis to 24 hours required little additional information to be provided by DIAS. After 24 hours, additional indication to support monitoring for Tech. Spec. surveillance was necessary. Thus to provide the most conservative time for operation with only the DIAS without overly burdening the display design 24 hours was selected as the basis.

5.12 INTEGRATION WITH PROCEDURES

- The Nuplex 80+ information system design shall provide task analysis based panel layouts and display formats. The panel and display designs shall consider the different types of operational tasks that must be accomplished.

  A task analysis is used as part of the control system design process to identify information and control requirements (and their respective characteristics needed to support operations). The task analysis output helps determine display page purpose, dynamic indication of status and values, and relationship to other display page information. The task analysis output also identifies the requirements for the operator to access new display pages, or supporting information. The use of task analysis data for display and control design implicitly links the man-machine interface with procedures since the procedures are also based on task analysis data.

- Procedures associated with the Nuplex 80+ control room shall contain references to DPS and DIAS information displays to allow the operator to be more efficient in his data gathering tasks.

  The Nuplex 80+ information processing algorithms shall be designed to support procedures where procedures require a large amount of data comparison for decision making. This is especially true for emergency procedures where the outputs of data comparisons determine operational strategies for recovery. For example, each emergency procedure requires the operator to monitor a safety function status check which contain setpoints for acceptable conditions of each critical safety function. Setpoints that are violated require operator actions. The Nuplex 80+ CFM algorithms continually monitor the acceptance criteria associated with the selected emergency procedure to ensure more rapid operator notification of deviant critical function conditions. This allows the operator to have more of a supervisory role and spend less time with routine data comparison, thus supporting rapid recovery to stable plant conditions.

6.0 I&C SYSTEMS DESIGN BASES

6.1 DATA PROCESSING SYSTEM (DPS)

The DPS shall provide high availability to support continued plant operations. The design shall be such that:

- o The DPS will accommodate the failure at any single computer hardware element without loss of essential functionality.
- o The complete loss of any single display generator will affect at most 3 CRTs.
- o The distribution of CRT's to display generators will be such that any single failed display generator will not blank out a contiguous section of panels.
- o The availability requirements for Emergency Response Facility data systems, per NUREG 0696, are achieved. This requires that the Safety Parameter Display System at the Main Control Room, Technical Support Center, and Emergency Operations Facility achieve an operational unavailability of $\leq$ 1% during all plant operating conditions above cold shut down.
- o "Bumpless" transfer occurs during failover operation.

The DPS shall provide suitable time response to support plant operations. The design shall be such that:

- o Touch target selections are acknowledged on CRT screens within 0.25 seconds.
- o System response to touch targets requests shall occur within 2.0 seconds of sensing a touch target request.

- o CRT's will have their dynamic data updated periodically every 2.0 seconds.

- o Plant I/O data will be periodically acquired every 2.0 seconds.

- o Periodic execution of application programs running as fast as once per second are supported.

The DPS shall support on-line maintenance. The design of the DPS shall be such that:

- o Facilities to allow on-line program development, via background support tasks, are provided.

- o The user shall be able to perform operability testing of CRT's, printers and touch screens while on-line.

- o On-line self-checks of system health shall be periodically performed in the host processor to allow early identification of system faults.

- o The host processors will perform a self test upon power up.

- o Sufficient redundancy is provided to allow hardware maintenance without taking the entire system off-line.

The DPS shall be both flexible and expandable to adapt to changing needs of the utility throughout the life of the plant. The design of the DPS shall be such that:

- o Additional application programs can be added by modular expansion without need to redesign or modify existing software.

- o The main memory can be expanded in size up to a total 32 megabytes via the addition of standard memory module boards.

- Increased bulk disk memory can be readily increased via the addition of standard disk drive units and controllers.

- Additional communication links can be readily accommodated via standard RS-232 datalink cards.

- Additional CRT mimic displays can be readily added by the user.

The DPS shall provide extensive, reliable data communications to support the required system information exchange. The design of the DPS shall be such that:

- Serial data communications to all required Nuplex 80+ Systems is supported.

- Bidirectional communications is supported.

- Isolation is provided when communications extend across a 1E system channel boundary.

- Error checking protocols are implemented to assure the integrity of the transmitted data.

- Periodic data transmission frequencies of once per 2.0 seconds are accommodated.

- The communication system is sized to accommodate a total of 10K - 15K I/O points.

Information concerning the implementation of the DPS to address these bases is provided in Reference 16.

6.2 DISCRETE INDICATOR AND ANNUNCIATION SYSTEM (DIAS)

The DIAS shall provide high availability to support continuous plant operations. The design shall be such that:

- The DIAS will accommodate the failure of any single computer hardware element without loss of essential functionality.
- Segmentation is employed to distribute DIAS functions over a number of small dedicated processors.
- "Bumpless" transfer occurs during failover operations.
- The overall unavailability of DIAS is $\leq$ 1% during all plant operating conditions.
- The meantime-to-repair is $\leq$ 1 hour.

The DIAS shall provide suitable time response to support plant operations. The design shall be such that:

- Touch targets are acknowledged within 0.25 seconds.
- Data is transmitted between DIAS segments within 0.50 seconds.
- Display updates will occur within 0.50 seconds of sensing a touch target request.
- Alarm tiles will be updated with 0.50 seconds of being set by the DIAS processors.
- Alarm messages are displayed within 0.5 seconds of selection of an alarm tile.

- o Plant I/O data will be periodically acquired at least once every 2.0 seconds

The DIAS shall support on-line maintenance. The design of DIAS shall be such that:

- o Sufficient redundancy is provided to allow hardware maintenance without taking the entire system off-line.

- o On line repairs will consist of board replacement on the CPU that has failed.

- o On-line self-checks of system health shall be periodically performed to allow early identification of system faults.

- o Each segment will periodically transmit status information which will be used for detection of segment faults.

The DIAS shall be both flexible and expandable to adapt to changing needs of the utility throughout the life of the plant. The design will be such that:

- o Additional DIAS segments can be readily added without need to redesign or modify the existing hardware.

- o At least 25% spare memory capacity will exist in the delivered system.
- o Additional RS-232 data communication links can be readily accommodated.

The DIAS shall provide extensive, reliable data communications to support the required system information exchange. The design shall be such that:

- o Serial data communications to all required Nuplex 80+ systems is supported.
- o Bidirectional communications is supported.
- o DIAS intra-system communications is accomplished via a redundant network.
- o Isolation is provided when communications extend across a 1E system channel boundary.
- o Error checking protocols are implemented to assure the integrity of the transmitted data.
- o The communication system is sized to accommodate a total of 5000 I/O points.
- o Total I/O data transmission does not exceed 250 milliseconds.

DIAS shall contain two physically and electrically independent divisions, designated DIAS-N and DIAS-P. DIAS-N shall process, display and alarm all signals appropriate for spatially dedicated displays in the control room. DIAS-P shall process and display only a subset of that same information that is required for continuous display per RG 1.97.

To ensure independence of the two divisions from common mode environmental effects DIAS-N processing equipment shall be located in the non-class 1E equipment room. DIAS-P processing equipment shall be located within the Main Control Room.

Information relating to the implementation of the DIAS to address these bases is provided in Reference 17.

6.3 PLANT PROTECTION SYSTEM

The following are design bases for the Nuplex 80+ plant protection system.

- The Nuplex 80+ plant protection system design shall assure adequate protection of the fuel, fuel cladding, and RCS boundary during anticipated operational occurrences. In addition the system shall assist the ESF in mitigating the consequence of accidents.

- The Nuplex 80+ plant protection system design shall meet the general design criteria of 10CFR50, NRC regulatory guides and IEEE standards.

- The Nuplex 80+ plant protection system design shall be digital design based, to take advantage of the high accuracy and drift free operation.

- The Nuplex 80+ plant protection system shall initiate the appropriate protection or safety action without operator action. Provisions shall also be made for the operator to manually initiate system action.

- The PPS shall segment trip functions into separate processors such that events that can be protected by two or more trip functions, have these trip functions processed by at least two separate processors.

- The PPS shall include continuous automatic hardware testing; and continuous automatic functional testing for all trip functions with the exception of sensor inputs and A/D conversion.

c. For functions not automatically tested built-in manual test features shall be provided and the function shall be continuously monitored (via cross channel comparison) to aid in failure detection.

Information relating to the implementation of these bases in the PPS design can be found in Reference 21 and Reference 1, Sections 7.2 and 7.3.

6.4 COMPONENT CONTROL SYSTEM

The following are design bases for the Nuplex 80+ component control system.

- The Nuplex 80+ component control system shall provide discrete and analog control of all NSSS and BOP process components (i.e., pumps, valves, heaters, etc.).

  Approximately 1000 discrete state and analog process devices comprise the actuated components of a PWR nuclear power plant. Historically these components were controlled from a number of independent and unrelated electromechanical relay based systems. System design responsibility was distributed among multiple suppliers resulting in many differing implementations. The operating and maintenance burden and potential for error was magnified as a result of these circumstances.

  The Nuplex 80+ component control system approach consolidates design responsibility resulting in more uniform and consistent implementation of plant component controls.

- The Nuplex 80+ component control system design shall include provisions to perform plant data acquisition functions.

  Component control and plant data acquisition has traditionally been performed by independent systems. Although many of the same interfacing signals are required for both functions, technological limitations dictated that signals be directed to both systems at the expense of complexity and cost. Modern instrumentation and control equipment has removed technological obstacles and now permits the consolidation of component control and data acquisition functions resulting in improved reliability and reduced cost.

The Nuplex 80+ component control system design includes provisions for plant data acquisition.

Reference 18 describes applicable technical considerations.

- Nuplex 80+ component control system component assignments shall preserve the level of fault tolerance provided in the plant mechanical system designs.

  Plant mechanical systems are designed with some degree of fault tolerance to component single failures. Plant components are assigned among CCS processors and equipment such that a single failure within the CCS does not compromise plant mechanical system fault tolerance.

  Nuplex 80+ component control system channels include, as a minimum, independent processors for plant primary and secondary components. Additional independence is also provided to permit selective assignment of redundant primary or secondary components to maintain the degree of fault tolerance afforded by the plant system designs.

- The Nuplex 80+ component control system design shall accommodate the use of commercially available software based digital control equipment.

  Equipment utilized to implement traditional plant component controls includes analog circuitry and discrete electro-mechanical relays. As a result, systems are complex, space inefficient, subject to the effects of long term aging and temperature-induced inaccuracy, mechanical wear and high commissioning, operating and maintenance costs. Implementations often require the use of single-source and custom equipment. Modification to system configurations to accommodate changing regulatory requirements is often cumbersome and configuration control is difficult to manage.

The Nuplex 80+ component control system design is based on the use of commercially available programmable logic controller (PLC) equipment. This equipment is industrial-hardened, field proven, digital software-based control equipment whose design overcomes the difficulties noted above for traditional component control implementation.

- The Nuplex 80+ component control system shall support the extensive use of remote multiplexing of I/O interface signals.

  A major contributor to lengthy construction cycle and high cost of a nuclear power plant is the plant wiring. Conventional control system designs feature centralized equipment cabinets to which several thousands of interfacing signals must be directed. Hardwiring these signals to centralized locations is time consuming, labor-intensive and restrictive with respect to future modifications. Remote multiplexing dramatically reduces overall plant wiring by distributing hardwired signal interfaces throughout the plant.

  The Nuplex 80+ component control system is designed for maximum utilization of remote multiplexing.

- The Nuplex 80+ component control system shall use advanced man-machine-interface (MMI) devices to consolidate and simplify operator controls.

  NUREG 0700 and Reg Guide 1.47 require consistent application of human factors engineering (HFE) throughout the design of a nuclear power plant. This consistency can only be achieved through application of component control system MMI devices whose integrated design and operation are consistent with MMI devices of other plant system (e.g., DPS, DIAS). Consolidation is necessary to support a one-person operating philosophy and is achieved using advanced MMI devices which perform multiple functions to reduce control panel space.

The Nuplex 80+ component control system design uses advanced MMI devices such as process controllers and component control switches with flashing discrepancy indication to achieve functional consolidation and consistency. Reference 2, Section 18.7.1.6 describes MMI devices related to the component control system.

- The component control system shall be designed to permit input and output module replacement without disturbance to field wiring connections and without the need to disconnect logic side power.

  Component control system repairs should have minimal impact on plant availability through low mean-time to repair characteristics. I/O module replacement should not require disconnection of field termination to preclude wiring reconnection errors and should not require disabling of logic or logic side power which might effect other unrelated functions.

  The Nuplex 80+ component control system design uses plug-in I/O modules that are replaceable without disturbance of field wiring under active logic conditions.

- Component control system information required by the DPS shall be transmitted using datalink interfaces.

  Earlier component control system designs provided interfacing signals to the plant data processing system (DPS) via discrete hardwired signals to the plant data acquisition system (PDAS). Since the information now resides in the component control system in a digitized format, use of PDAS as a DPS front end is no longer necessary. Direct datalink interface to the DPS will simplify the interface design and significantly reduce interface wiring.

The Nuplex 80+ component control system design provides datalink interfaces to the DPS. This feature is further described in Reference 1, Section 7.7.1.7.

- o Nuplex 80+ component control system memory shall be non-volatile and program memory contents shall be continuously monitored to verify program integrity.

  Any distributed software-based system will experience loss of power at some point in its commissioned life. System restart must be automatic and program reload must not be necessary upon restoration of power since manually accomplishing these would be extremely cumbersome and time consuming for a distributed system. Additionally, program memory integrity must be continuously monitored to prevent undetected alteration resulting from any system fault.

  The Nuplex 80+ component control system uses non-volatile programmable read only memory (PROM) for the executive program and battery-backed dynamic random access memory (RAM) for application programs. Memory contents is continuously monitored by a dynamic read/write method in the component control system and by the checksum method in the plant data processing system (DPS). Failures are annunciated by the DPS.

- o Nuplex 80+ component control system software execution shall be deterministic.

  The software execution cycle for nuclear power plant instrumentation and control systems must be predictable, repeatable and non-interrupt driven (i.e., deterministic) to preclude overloading under postulated and unanticipated transient conditions. System performance and response under all conditions can only be ensured with deterministic software execution.

The Nuplex 80+ component control system performs deterministic software execution.

- o Component control man-machine interface (MMI) devices required for hot shutdown shall be located on the plant remote shutdown panel (RSP). Control devices shall be geographically separate and electrically independent from equivalent controls in the main control room.

  Reg. Guide 1.120 and CMEB 9.5-1 impose fire protection criteria for alternate plant controls which recommends that alternative or dedicated shutdown capability should be provided where the protection of systems whose functions are required for safe shutdown is not provided by established fire suppression methods.

  The Nuplex 80+ component control system design duplicates those MMI devices necessary to achieve hot shutdown for placement in the RSP. Fiber optic isolation is used to isolate both RSP and main control room controls to ensure hot shutdown capability. Reference 1, Section 7.3.1.1 provides a description of the fiber optic RSP interface.

- o Nuplex 80+ component control system equipment shall include provisions for automatic self-health testing and annunciation of failures.

  Early detection of single failures is essential to maintaining system level operability with distributed control systems. A simple method of failure identification also reduces mean-time-to-repair characteristics. These features significantly improve plant availability.

  The Nuplex 80+ component control system includes continuous on-line self-health testing and annunciation of failures for all equipment.

- The Nuplex 80+ engineered safety feature-component control system (ESF-CCS) shall accept isolated discrete initiating signals from each channel of the plant protection system and perform selective 2/4 logic for each ESF function.

  Selective 2/4 logic for ESF functions has historically been implemented using channelized electromechanical relay based equipment in a system independent from plant component controls. This approach resulted in a complex, hardwired interface to direct individual actuation signals to the component control logic. In addition to the component control logic, the Nuplex 80+component control system design provides selective 2/4 logic processing for ESF functions resulting in simplified interface wiring, elimination of interposing electromechanical relays, and simplified operation and testing.

- The Nuplex 80+ ESF-CCS shall provide geographical separation of redundant channels. Isolation shall be used to maintain channel independence.

  Reg. Guide 1.120 and CMEB 9.5-1 impose criteria for fire protection in nuclear power plants. One method which meets the fire protection criteria is to locate redundant channelized equipment in geographically separate fire zones such that an exposure fire can only impact the operation of a single channel. Traditional technology precluded the use of geographic separation due to the practical limitations associated with electrical isolation of numerous signals between protective equipment channels. Current technological advancements have now eliminated these restrictions. The Nuplex 80+ ESF-CCS is designed to accommodate geographical separation of channels using fiber optic isolated datalinks to satisfy Reg. Guide 1.75 criteria for channel independence as defined in Reference 1, Section 7.3.2.3.2.F.

- The Nuplex 80+ ESF-CCS design shall include provisions for sequencing of protective loads on the plant emergency diesel generators. Sequencing shall be adaptive as a function of plant conditions and energize equipment as quickly as possible to minimize the overall plant disturbance.

  Priority sequential loading of essential and non-essential diesel generator loads provides a method to eliminate unnecessary equipment cycling and minimize diesel generator size without sacrifice of plant operability.

  The Nuplex 80+ ESF-CCS includes algorithms which can be selectively applied to optimize the emergency diesel generator loading sequence based on current plant conditions. A description of the diesel loading sequencer is given in Reference 1, Section 7.3.1.1.2.3.

- The Process-CCS design shall include provisions for automatic and manual control of NSSS primary and secondary pressure and coolant level.

  Control of NSSS primary and secondary pressure and level has historically been provided by independent control systems which were separate from plant component controls. This design approach often resulted in diverse equipment of varying design which was difficult to functionally coordinate and maintain.

  The Nuplex 80+ Process-CCS includes turbine bypass, steam generator level and primary pressure and level control functions in an integrated design using common control equipment to overcome the difficulties noted above. These functions are selectively assigned to individual, redundant processors to enhance tolerance to single failures. Reference 1, Sections 7.7.1.1.2, 7.7.1.1.4 and 7.7.1.1.5 provide a description of these features.

- o The Nuplex 80+ Process-CCS shall provide a means diverse from the reactor trip system to automatically trip the reactor and initiate emergency feedwater follow under conditions indicative of anticipated transient without SCRAM (ATWS) events.

  10CFR50.62 imposes the diverse reactor trip and emergency feedwater initiation requirement for ATWS for all pressurized water reactors. The Nuplex 80+ Process-CCS design includes an alternate protection system (APS) function to satisfy ATWS concerns. A description of the APS function is given in Reference 1, Section 7.7.1.1.11.

- o The ESF-CCS shall contain 4 physically and electrically independent divisions, designated A,B,C,D. Each division shall be associated with the appropriate mechanical division equipment.

- o The Process-CCS shall contain two divisions, designated N1 and N2. This divisional arrangement is only to accommodate the large quantity of non-class 1E plant equipment. Both divisions shall control X and Y equipment as required. Each division shall include sufficient redundancy to prevent a single credible failure resulting in a common failure of X and Y components.

6.5 POWER CONTROL SYSTEM

The following design bases are provided for the Nuplex 80+ power control system.

- The Nuplex 80+ power control system design shall include provisions to automatically control plant electrical megawatt output through the turbine control system to ensure that plant variables are maintained within their operating limits.

  Nuclear power plants have historically been operated in the base load mode. As the percentage of nuclear power plants on the grid is expected to increase, the need arises for load follow operation. Automatic control of plant electrical megawatt output will improve plant availability under load follow conditions by limiting load demand to levels which can be accommodated by the NSSS.

  The Nuplex 80+ power control system includes the megawatt demand setter (MDS) function to improve plant load follow capability. This function is further described in Reference 19.

- The power control system shall include the capability to automatically control reactor coolant average temperature and reactor power for all warranted maneuvers and steady-state plant operating conditions.

  The most responsive means of reactor power regulation is to manipulate T_{AVG} as opposed to boron regulation. Automatic regulation of T_{AVG} through control rod manipulation most closely maintains NSSS parameters within their operating limits and optimizes NSSS response to load changes required during normal plant operation.

The Nuplex 80+ power control system includes the reactor regulation (RR) function to automatically control T_{AVG}. This function is described in Reference 1, Section 7.7.1.1.1 and Reference 20.

o The Nuplex 80+ power control system design shall provide the capability to rapidly reduce reactor power under NSSS fault conditions including 100% load rejection.

NSSS fault conditions such as 100% load rejection, loss of one operating feedwater pump, abnormal reactor core power or dropped rod failures normally result in a reactor trip. Rapid reduction of reactor power under fault conditions improves plant availability since return to power upon resolution of the fault can be accomplished in a much shorter time period if a reactor trip is averted.

The Nuplex 80+ power control system includes the reactor power cutback (RPC) function to preclude reactor trip under NSSS fault conditions. This feature is defined in Reference 1, section 7.7.1.1.6 and Reference 20.

o The power control system design shall include the logic and power control circuitry to facilitate automatic and manual manipulation of control element assemblies (CEA's) to regulate NSSS power.

The Nuplex 80+ power control system design provides CEA motion control (CMC) and CEDM power control (CEDMPC) capability. These design features are described in detail in Reference 20.

o The Nuplex 80+ power control system shall provide reliability to support operation such that no single failure within the system equipment shall perturbate stable system operation.

The Nuplex 80+ power control system incorporates redundancy in key design areas such as processors and network and datalink communications to ensure reliable system operation upon single failure in any of these components. In areas where redundancy is not provided such as man-machine-interface devices or RSPT I/O interface chassis, the system is designed to fail gracefully (i.e., hold last value or fail to midscale) to allow continued system operation until repair can be made. All failures are alarmed and extensive diagnostic features are incorporated to simplify the maintenance task for repair.

o The power control system shall provide a system throughput of not greater than 0.5 seconds for critical system functions. System throughput is defined as the time interval which encompases input parameter change of state sensing, control logic processing and output signal manipulation.

The power control system is designed to provide rapid system throughput (i.e., less than 0.5 seconds) through the use of a scheduling feature that allows critical system functions to be serviced more frequently than noncritical functions. Sufficient margin exists to accommodate any critical functions as necessary.

o The Nuplex 80+ power control system shall provide data communications compatability for interface with other Nuplex 80+ system equipment.

The Nuplex 80+ power control system design provides ASCII/RS232 ports to facilitate datalink interfaces to other Nuplex 80+ systems such as DPS, DIAS and PPS and main control panel devices such as operators modules. Industry standard ASCII data format is used to ensure communications compatability under circumstances where other interfacing systems are implemented with equipment that is diverse from [illegible]r control system equipment. This design approach also ensures capability for application of fiberoptic cable where electrical fault isolation is required between systems and devices.

o The power control system shall allow 30% expansion capability to accommodate future operational enhancements.

The Nuplex 80+ power control system is a distributed programmable logic controller (PLC) based system that includes 30% expansion capability. Enhancement features such as a feed-forward reactor power control strategy and an expansion of the reactor power cutback function to address additional plant transient events can be easily accommodated within the power control system architecture.

7.0 INTEGRATED SYSTEMS FEATURES DESIGN BASES

7.1 EQUIPMENT QUALIFICATION

The following are design bases for the Nuplex 80+ equipment qualification

- Where possible, Nuplex 80+ system shall utilize proven industrial products and qualify them to assure suitability for nuclear applications.

  Extensive utilization of custom equipment in the past has resulted in high equipment and qualification costs. It has also resulted in spare parts availability and obsolescence problems. The more extensive use of commercially available products and technology in Nuplex 80+ reduces initial procurement costs and later spare parts unavailability and costs.

- Nuplex 80+ equipment qualification shall be performed utilizing representative design equipment, that contains all possible hardware modules and configurations.

  This permits in-service hardware configurations to be easily analyzed utilizing the representative design equipment results. When combined with generic hardware package and software based systems (e.g. PLCs), it provides for early delivery and installation of equipment cabinets, without all of the final functional details being available. It also provides for easy future changes without extensive qualification efforts being required.

- o Nuplex 80+ I&C system equipment shall be selected to be compatible with its environment under all normal conditions, and under accident conditions as appropriate to meet functional requirements.

- o Nuplex 80+ I&C system equipment qualification shall meet the requirements of general design criteria of 10CFR50, NRC regulatory guides and IEEE standards.

7.2 STANDARDIZATION AND DIVERSITY

The following are design bases for Nuplex 80+ systems with regard to standardization and diversity.

- Nuplex 80+ shall maximize the utilization of common hardware and software modules throughout the control, protection and monitoring systems.

  This standardization will reduce plant design, construction and maintenance costs by:

  - Minimizing engineer and technician training
  - Minimizing spare parts inventory
  - Minimizing design engineering
  - Minimizing equipment procurement efforts
  - Maximizing the potential for quantity purchase discounts

- Nuplex 80+ shall maximize standardization while maintaining a minimum level of diversity in key areas to ensure that the nuclear industry precedence for "defense in depth" is not compromised.

  Present plants exhibit significant unplanned diversity due to multiple suppliers of I&C systems. Although unintentional, this defense in depth has been important to the safety record of the nuclear industry and the excellent availability of C-E plants.

  Diversity becomes even more important in the design and supply of equipment for nuclear power generating stations as system complexity increases and utility experience with rapidly developing new technologies is low. This is exemplified by the fact that diversity was a key factor in the licensability of C-E's digital protection system. Diversity is not a substitute for quality. Similarly, QA in design and operation is considered fundamental in achieving system reliability, but is not an adequate substitute for the defense in depth achieved through diversity.

Nuplex 80+ employs the following diversity in the system designs:

Function	Design Type 1	Design Type 2
Reactor Trip	Plant Protection System	Alternate Reactor Trip Within Process-CCS
Fluid System Controls	Emergency Success Paths (e.g Emergency Feed-water) via ESF-CCS	Normal Success Paths (e.g. Main Feedwater) via Process - CCS
Reactivity Controls	Emergency Boration via ESF-CCS	Normal CEA Control - via Power Control System
Alarm and Indication	Alarm Tiles and Discrete Indicators - via DIAS	CRT Displays - via DPS

It is also noted that per 10CFR50.62 diversity is required between the reactor trip system and actuation of the emergency feedwater system. Nuplex 80+ meets this requirement by actuating reactor trip from the PPS and actuation of the EFW system from both the PPS and Process-CCS (i.e. Alternate Feedwater Actuation Signal).

o Diversity shall be maintained in all areas where the technology utilized is not well proven in the nuclear industry.

The need for diversity pertains primarily to complex technology areas (e.g. computer, multiplexors, video displays, etc). It is not intended that diversity be extended to technologies for which utilities have significant experience (e.g. relays, switches, terminations, sensors etc.). Diversity in these simpler proven technology areas is maintained only as dictated by licensing requirements (i.e. ATWS rule).

o Nuplex 80+ shall utilize environmental diversity of systems and hardware where practicable. That is equipment of different channels, or other redundant equipment should be located in different plant geographic areas.

This minimizes the potential for common failures from externally induced events.

o Nuplex 80+ shall utilize functional diversity as dictated by licensing requirements or to achieve desired reliability goals.

Functional diversity is different than hardware/software diversity in that common hardware/software may be utilized but the functions performed are different. Examples of functional diversity includes such approaches as 1) controlling core reactivity by control rods and boron, 2) automatic and manual control, 3) Reactor trip through two different process measurements for the same accident event (e.g., loss of feedwater flow results in trip signals from low steam generator level and low pressurizer pressure).

7.3 REDUNDANCY AND SEGMENTATION

The following design bases address redundancy and segmentation requirements for Nuplex 80+ systems.

- Nuplex 80+ safety-related systems shall meet channel redundancy and independence requirements established in applicable regulatory standards.

  Regulatory standards including Reg. Guides, NUREG's and IEEE standards thoroughly define channel redundancy and independence design requirements for class 1E safety-related systems in nuclear power plants.

  Nuplex 80+ ESF control systems are designed for channel redundancy and independence as required by the plant fluid systems.

  The Plant Protection System includes four redundant channels, the ESF Component Control System includes four independent trains, the Discrete Indication and Alarm System contains two independent channels for post accident monitoring Category 1 displays.

- Nuplex 80+ safety and non-safety control systems shall utilize functional group control and segmentation techniques to achieve high reliability and independence of I&C functions comparable to the independence of plant mechanical functions.

  Effective utilization of the processing power and design flexibility of distributed microprocessor-based technology dictate that multiple plant components be controlled by a single controller. Single loop independence that was previously afforded by discrete instrumentation and control equipment cannot be achieved for distributed microprocessor-based technology.

However, Nuplex 80+ distributed systems achieve significantly higher reliability and more manageable failure modes by grouping mechanically dependent control functions together (e.g., pumps and valves in a process loop) into common control equipment and separating independent control functions (e.g. redundant pumps, flow paths, etc.) into different segments of the control system. This technique minimizes the number of components in the control system, thereby maximizing MTBF. At the same time it achieves more manageable failure modes since all components in a process loop are controlled by a common system that has a predictable failure mode.

Nuplex 80+ can be compared to a control system of the past where a process loop containing multiple components had each component controlled by a separate controller. The large number of controllers results in poor MTBF. The failure of each controller individually results in a unique process failure mode for every occurrence. The benefit, however, of single loop control is that mechanically unrelated functions are not commonly impacted by a single controller failure.

Nuplex 80+ utilizes functional grouping and segmentation to achieve the mechanical independence of single loop controllers without the disadvantages of poor MTBF and complicated failure mechanisms.

Refer to Reference 1, Section 7.3.1.1.c for examples of Nuplex 80+ segmentation techniques.

o The Nuplex 80+ design shall employ redundancy within safety and non-safety control systems for those elements of the system that are common to multiple control segments.

In distributed microprocessor-based systems, a single CPU which includes the central processing unit, memory, and communications servicing electronics may be common to multiple control functions (or segments). Since several control segments are controlled by the CPU, a single failure will disable the system which could have adverse impact on plant availability in many cases.

Nuplex 80+ instrumentation and control systems include CPU redundancy in all cases where multiple control segments could be impacted by a single CPU failure.

Similarly, network and datalink communication paths are relied on to transact large amounts of concentrated data between processors in any distributed microprocessor-based system design. In some cases, the data may support interlocks or functions that are critical to the operation of multiple control segments. As such, the communication path can not be susceptible to single failures in either the transmitting and receiving electronics or the media itself.

Nuplex 80+ utilizes redundant datalink and network communications to preclude adverse effects of single failures on multiple control segments.

o Independent control segments shall not rely on common CPU's or control communication paths (even with redundancy) if the independence of the control segments is required to meet single failure assumptions in the plant's safety analysis.

Common CPUs and/or communication paths compromise control segment independence. Although redundancy in these elements significantly improves their reliability, for safety analysis purposes it must be assumed that both redundant elements fail.

This is true because this redundancy does not comply with all electrical independence requirements for redundant channels (e.g. IEEE-384). Therefore, in cases where the plant's safety analysis relies on independent failure (e.g. feedwater control will not fail concurrently with pressure control), segments shall remain independent in all areas that can offset their control function.

- Within the DPS redundancy shall be provided for all elements of the system that could result in loss of display information.

  In the DPS there are multiple independent CRTs located in all required plant locations. In addition, redundant CPU's and peripherals are provided to accommodate failures that would result in information blackout.

- Within DIAS channel redundancy shall be applied selectively on a cost benefit basis.

  DIAS is redundant to the DPS; to accommodate post accident monitoring requirements DIAS channel N is redundant to DIAS channel P. Therefore, no redundancy within a DIAS channel is necessary. Redundancy is provided only for: 1) CPU's which are the most complex and therefore most likely elements to fail, and 2) for inter-segment communications, since a single failure could compromise the performance of multiple indication and alarms.

7.4 POWER SOURCES

The following are design bases for the Nuplex 80+ power sources.

- o Vital instrument power sources shall be designed such that a single failure, including catastrophic failure such as fire and flood, will effect only one channelized bus.

  Nuplex 80+ includes four vital instrument buses A,B,C,D. Each bus powers a separate channel/train of the PPS and ESF-CCS. In addition, busses A and B power DIAS-P; busses C and D power DIAS-N.

- o Non-vital power sources shall be designed such that a [illegible] credible electrical failure (excluding catastrophic events) will effect only one channelized bus (X or Y, not both).

  Nuplex 80+ includes two non-vital instrument busses for the non-class 1E control systems and two separate non-vital instrument buses for the DPS. Non-vital instrument busses are designated X and Y respectively.

- o All instrument busses shall be designed such that single credible electrical failures at the Remote Shutdown Panel or in the Main Control Room will effect the bus in that location only, not in the alternate location.

  In Nuplex 80+ total MCP/RSP isolation is maintained.

- o Class 1E motive power sources shall be designed such that a single failure, including catastrophic event, will effect only one electrical division.

  Nuplex 80+ includes two Class 1E power divisions each with a separate emergency diesel generator and one non-1E division. Division I includes busses A and C, Division II includes busses B and D, Division N includes busses X and Y.

- Within a division, busses shall be designed such that a single credible electrical failure (excluding catastrophic events) will effect only one of the two busses.

- Motive power sources shall not enter the area of the RSP or MCP.

- The ESF-CCS and Process-CCS shall be powered by both the instrument buss and motive power buss of the appropriate channel.

  This ensures that there is power to the CCS anytime there is power to its controlled equipment.

- Nuplex 80+ class 1E onsite power sources shall be designed to permit appropriate surveillance, periodic inspections, and testing of important areas and features to assess the continuity of the systems and conditions of their components.

- Nuplex 80+ shall have a non-class 1E alternate AC source to help mitigate the effects of loss of onsite power and station blackout scenarios. The alternate AC source shall be normally lined up to the non-safety division. However, it shall be capable of powering a class 1E division for situations when an emergency diesel generator is out of service. When lined up to a class 1E division the AAC source will power only one non-1E instrument bus (i.e. X or Y) and only one non-1E reactive power bus (i.e. X or Y).

- Nuplex 80+ vital battery chargers shall have adequate capacity to supply its assigned steady-state loads while simultaneously recharging its associated battery.

7.5 MAINTENANCE AND TESTING

The following are Nuplex 80+ design bases for I&C maintenance and testing:

- Nuplex 80+ I&C systems shall have continuous on-line hardware self testing to provide monitoring of overall system availability with rapid identification of hardware failures.

- All systems shall have integral test and maintenance panels or built-in jacks for quick connection of portable test and maintenance panels. These panels shall provide diagnostic displays that allow quick location of hardware failures.

- Nuplex 80+ PPS shall provide automated periodic functional testing (i.e. protection system trip paths shall be continuously tested automatically) to improve overall system reliability through identification of system failures.

- Nuplex 80+ DPS shall provide computer aided test features for ESF component testing that verifies functionality, locates failures upon detection, and records test results.

7.6 ESF TESTING

The following design bases are provided for Engineered Safety Features (ESF) testing for the Nuplex 80+ design.

- o All Nuplex 80+ ESF functions shall be fully testable from initiating sensor to final actuation device during all modes of plant operation. Testing shall not interfere with engineered safeguards protective action.

  ESF equipment is operated infrequently and, as such, must be tested to ensure operational readiness. The equipment used to implement each Nuplex 80+ ESF function including sensor, trip bistable, local coincidence logic, initiation logic, actuation logic and final actuation device (i.e., pump, valve) is designed to meet test requirements of IEEE Std 338-1977 and Reg. Guide 1.22 to facilitate testing.

  Testing details are given in Reference 1, Section 7.3.1.1.8.

- o The Nuplex 80+ design shall maximize the use of automated testing of ESF functions.

  Personnel errors which can have adverse impact on plant safety and availability are largely associated with maintenance and testing of plant systems.

  Nuplex 80+ incorporates continuous automatic testing of the protection system and ESF initiation circuitry to minimize potential for personnel-induced errors, provide early identification of failures and reduce mean-time-to-repair (MTTR). Plant safety and availability is improved as a result of these features. Reference 1, Section 7.3.1.1.8 provides further description of automatic ESF testing.

- o Operational aids shall be utilized to reduce potential for personnel errors during manual testing of Nuplex 80+ ESF functions

  All portions of ESF functions cannot be automatically tested. Where manual testing is necessary a concern exists that complex procedures are inadequate to prevent errors.

  The Nuplex 80+ design incorporates computer automated testing (COMAT) algorithms as part of the data processing system (DPS) which

  - store initial ESF component lineups
  - confirm correct component test lineups
  - confirm proper component actuation upon manual initiation of test including position response time and performance (e.g. pump flow).
  - confirm restoration of correct post-test component lineups

  A further description of COMAT is provided in Reference 1, Section 7.3.1.1.8.6.

- o Nuplex 80+ ESF components shall be grouped to accelerate testing by simultaneously actuating all components in a group. Groups shall be arranged to prevent complete, undesired actuation of an ESF system during testing.

  The Nuplex 80+ PPS and ESF-CCS are designed to preclude undesired ESF system actuation due to single component failures. Testing errors can similarly result in undesired actuation of ESF systems.

Nuplex 80+ takes advantage of the inherent plant system design features to accelerate testing, while preventing spurious or undesired system actuation. The components for each ESF are assigned in groups (i.e., pump group and valve group) and testing is performed one group at a time to prevent undesired actuation.

A further description of selective group testing is presented in Reference 1, Section 7.3.1.1.8.6.

7.7 CLASS 1E SOFTWARE QUALIFICATION

The following are design bases for Nuplex 80+ class 1E software qualification.

- The Nuplex 80+ class 1E software shall be designed and qualified in accordance with Reg. Guide 1.152 and ANSI/IEEE 7-4.3.2-1982 requirements.

  A significant advantage of software-based systems is the inherent design flexibility offered. This flexibility, however, can be a liability unless careful controls are imposed throughout the software life cycle to ensure the integrity of software-based system performance. Proper definition and verification of system performance under all conditions is critical in class 1E applications. Reg. Guide 1.152 and ANSI/IEEE 7-4.3.2-1982 provide a structured software design and qualification approach which results in high reliability software for class 1E applications.

- Class 1E software for the Nuplex 80+ design shall be categorized as application software or executive software. Application and executive software shall be subject to qualification in accordance with the requirements of Reg. Guide 1.152 and ANSI/IEEE 7-4.3.2-1982 requirements.

  Application software defines system function for the intended class 1E application and, as such, must undergo rigorous verification and validation during the design process to ensure high reliability. Executive software which includes the operating system, I/O handling, communications handling and self-testing software is typically supplied by the computer system manufacturer. In most cases, the executive software design process is not thoroughly documented and in some cases may even be proprietary. As such, an alternate means for qualification of executive software is required.

Qualification of Nuplex 80+ executive software is accomplished by demonstration of proper performance and reliability through a combination of the following:

- successful operating history in similar applications
- validation through extensive testing of application software for the intended class 1E application.

After validation strict configuration controls are employed to ensure that Nth of a kind software is the same as that qualified, and that the qualified software is properly maintained over the life of the plant.

o Nuplex 80+ class 1E software shall be modular in design. Software modules shall be designed to facilitate individual validation and subsequent integration and validation on a system basis.

Class 1E safety systems are typically complex in design and function. Such systems exhibit multiple operating modes with many combinations of static and dynamic input conditions. A historically effective design approach has been to segment the software into modular elements which can be more easily and thoroughly tested. Once validated for correctness, software modules are then integrated and validated through system level testing.

Nuplex 80+ class 1E software is developed, verified and validated using the modular method where system complexity so dictates.

- A detailed software development plan shall be produced for each Nuplex 80+ class 1E software-based system at the beginning of the software development process. Each software development plan shall include definition of the development process with identification of appropriate verification and validation points.

  High quality software results from a well-defined, structured design approach. A detailed software development plan which is consistent with and complementary to system hardware and software design specifications will promote structured software development and serve as a guideline to ensure completeness of the development, verification and validation process.

- A detailed software specification shall be provided for each Nuplex 80+ software-based class 1E system. This document shall serve to define software performance, response and accuracy requirements in detail.

  Well defined software requirements are necessary to ensure correct and reliable software performance. The software specification serves as the vehicle to convey software design requirements to the programmer(s). This document will also serve to define software modularization and validation acceptance criteria.

  In the Nuplex 80+ design, the software specification will complement the software development plan and hardware specification for each software-based class 1E system.

7.8 NON-CLASS 1E SOFTWARE V&V

Non-class 1E software V&V shall assure that the non-1E software satisfies its intended function and that implementation errors are detected and corrected, thus assuring a reliable software system end product. The following are individual design basis for non-class 1E software V&V for Nuplex 80+.

- o Non-class 1E software shall be based on a structured design approach.

  A generic structured design methodology creates a software development environment which is conducive to producing reliable software and which assures a uniform approach to software design and implementation.

  The primary methods of addressing this on Nuplex 80+ is the creation of software design guidelines which embody the structured design methodology to the utilized.

- o New software which is related to investment protection or which due to its complexity and/or importance to plant operations is deemed a critical application, shall be subject to independent review.

  Certain critical applications, which represent new software, (such as alarm reduction techniques, sensor validation, safety function status check application program) are to be reviewed due to their importance in plant operations. This will allow early detection of errors, thus allowing sufficient time to devise corrections and minimize schedule impact. However, "critical" software which has previously been subject to an intense QA effort need not be subject to such independent review since there is little (if any) value added.

The primary method of addressing this in Nuplex 80+ is via an independent reviewer (or review team) knowledgeable in the subject matter. The review may encompass any software design/implementation phase as appropriate including: Design specification, program constants, coded algorithms, etc.

- Non Class 1E software modules shall be subject to "unit test" prior to being integrated within the system.

  Unit testing of software modules will verify the individual modules work correctly in a "stand-alone" environment prior to system integration, thus simplifying the integration task and subsequent debugging.

  Unit testing is accomplished by software implementers prior to releasing the module for integration.

- Software which has been integrated together within the system shall be subject to independent Integrated System testing.

  Integrated System testing assures the software is interfaced correctly and meets its specification requirements.

  Integrated System testing is conducted by an independent tester (or test team) who is familiar with the integrated system performance requirements. It is accomplished via a formal test procedure in accordance with a structured test plan. This testing may be carried out through several levels of "system builds", as appropriate.

- Mature, industry accepted operating systems need only be verified indirectly via test activities performed during unit testing and system integrated test.

Mature operating systems have proven themselves through their longevity, widespread usage, and industry acceptance. Indirect testing of OS features during units and integration testing will verify those portions of the OS which are being used by the non IE software.

- Configuration controls shall be implemented throughout the product life cycle.

  Configuration controls will assure that application software, operating system and hardware are adequately controlled throughout the project life.

  This is achieved via implementation of hardware and software configuration control procedures at the inset of the project.

7.9 DATA COMMUNICATIONS

The following are the design bases for Nuplex 80+ data communications.

- o Multiplexing shall be used in the Nuplex 80+ design for both safety and non-safety applications where it is cost effective.

  The Nuplex 80+ design makes extensive use of remote multiplexing for data communications to minimize the number of field cables, cable trays and labor for cable pulling and termination. Multiplexing allows approximately a 70% reduction in cables, trays and associated labor which results in a net 15% to 20% savings in the cost of the plant's I&C systems.

  Each data communication application is evaluated to determine the most cost effective means for data communication. Multiplexing is used where the number of cables replaced is adequate to equal the cost of the multiplexing equipment.

- o Control, protection and PAMI systems shall receive field sensor data directly in analog form where possible.

  Systems that are critical to plant operation and safety require rapid data acquisition. In the Nuplex 80+ design, data latency concerns are addressed by providing signals directly to control, protection and PAMI systems. This is accomplished by two means. When signals are used in only one system the sensor signals are multiplexed directly to the system. This is the case with most signals feeding the PCS, Process-CCS and ESF-CCS. In other cases where the sensor signals are used in multiple systems, these signals are provided directly to the Auxiliary Process Cabinets where they are then distributed to all of the appropriate systems. This is typified by signals used commonly by the PPS and other control systems such as the Process-CCS and/or PCS.

- o Monitoring systems shall receive field data from other systems when possible.

  The time criticality of data for monitoring systems, such as DPS and DIAS, is not as great as for control and protection systems. Thus in Nuplex 80+ these systems are provided data via data links from the systems which require the signal directly (e.g., PPS or CCS). This approach minimizes the data acquisition costs since the interface of raw field I/O is minimized.

- o Multiplexors shall be designed for location in remote plant locations without the need for special controlled environmental conditions.

  All remote multiplexors are designed for continuous operation at 122 ^{o}F and 95% non-condensing humidity. Multiplexor enclosures are drip proof and designed for wall or floor mounting.

  At present the NPX80+ multiplexors are not intended to be located inside containment primarily due to insufficient test data. However, there are applications, such as for incore instrumentation and CEA position measurements, where in-containment multiplexing would offer significant economic advantages. Therefore in-containment multiplexing is continuing to be evaluated and will be offered when it is considered proven technology.

- o To take full advantage of the Nuplex 80+ I&C architecture, the AE shall be encouraged to distribute motor control centers to locations in close proximity to the associated equipment.

Traditionally, Motor Control Centers (MCCs) have been centrally located near the control room or in the control complex in nuclear units. This location was selected to minimize the lengths of the large number of cables that interfaced from the MCCs to the control room and I&C systems. Unfortunately, this location results in long lengths of power cables required from components to the MCCs.

In Nuplex 80+, multiplexing will be used to minimize the cabling from the MCCs to the control room and I&C systems. It therefore becomes logical to distribute the MCCs, locating them as near to the components being controlled as possible. This has many benefits. First is the cost reduction and reduction in installation labor based on multiplexing control signals to the MCCs and using much shorter power cables from MCCs to components. Shorter power cables ;minimize the potential for EMI/RFI emissions from power cables and reduce line losses in the cables. Distributing MCCs locally has the advantage of reducing the size of cable spreading rooms and provides enhanced separation for channel independence. This improves both fire resistance and sabotage protection. The potential advantages of using distributed control in Nuplex 80+ will be fully realized when the MCCs are also distributed.

- The Nuplex 80+ data communications shall accurately, reliably and in a timely manner support intersystem and intrasystem information exchange within the advanced control complex.

The Nuplex 80+ advanced control complex will contain approximately 15,000 I/O process points which must be communicated in both an intrasystem and intersystem manner throughout the advanced control complex. The communication architecture must support channelized independence, accommodate single failures within the communication system, support the time response requirements of interfaced systems, insure the integrity of the transmitted data, and minimize the required quantity of communication links consistent with single failure concerns.

- o Fiber optic links shall be used where channalization independence is required.

- o Error checking methodologies shall be used for transmitted data to assure data integrity.

- o Point-to-point dedicated digital links shall be used for intersystem communications to minimize interface problems between systems manufactured by diverse vendors and reduce the likelihood of communication bottle necks. Data highways may be used for intrasystem communications.

- o Redundancy shall be provided within the design to accommodate communication failures as previously defined in Section 7.3.

Data communication methods are further discussed in Reference 22.

7.10 FLEXIBILITY AND EXPANSION

The Nuplex 80+ design includes advanced man-machine interface features and advanced control and protection features. Some examples are signal validation, mode dependent alarm processing, power dependent trip setpoints, expanded reactor power cutback, megawatt demand setting, success path monitoring, expanded critical functions, etc.

Additional features that are not presently part of the design can also be anticipated. Some examples of these are automated technical specification monitoring, expanded control functions for enhanced load following, and integration of procedure text into video displays.

Nuplex 80+ systems shall be designed such that presently defined features and/or new features may be implement[illegible] phased-in approach over time. This phase-in may occur prior or subsequent to initial plant commissioning. To accommodate this flexibility and expansion capability the following design bases are defined:

- All functions shall be software based.

  Software based systems allow functions to be changed or added with significantly less cost impact as compared to hardware based systems.

- All software shall be written in modules with each module linked to an I/O data base.

  Modularization and data base structuring allows ease of expansion.

- I/O and data communication shall be multiplexed to the maximum extent practical.

Multiplexing allows I/O to be added as necessary for future functions without the need to pull additional field cabling.

- o All systems shall include 20% spare I/O and memory built-in to the delivered system.

- o All systems shall provide the capability to expand the I/O and memory by an additional 20% through the addition of hardware as needed.

- o System response time requ[illegible]ts shall be set with the maximum expans[illegible] [illegible]fined above.

7.11 SENSOR REDUCTION AND EFFECTS ON CONTROL/PROTECTION INTERACTION

The following are design bases for Nuplex 80+ sensor reduction and the effect on control/protection interaction.

- o The Nuplex 80+ design shall minimize the number of plant sensors required to perform control functions while satisfying control and protection system interaction requirements of IEEE Std 279-1971.

  In the past control system parameters were monitored using one or two redundant control grade sensors. In most cases, the control grade sensors monitor the same plant parameters monitored by four channel protection system safety grade sensors. This extensive duplication of sensors has been a concern with conventional nuclear power plants. This control/safety duplication results in high construction and maintenance costs, and potentially contradictory and confusing information presentation to the plant operator. In addition, since control systems utilized only two sensors, failures require immediate operator interaction to avoid averse control actions. The Nuplex 80+ design addresses these concerns through the elimination of control grade sensors. Control system parameters are instead derived from isolated four channel safety sensor signals using signal validation techniques. Signal validation offers the following advantages:

  - Sensor redundancy for control parameters is increased from two to four channels, allowing automatic elimination of failed sensors.
  - Single failure of a sensor does not affect control system performance thus control system malfunction and resulting challenge to protection system is eliminated; this satisfies IEEE Std 279-1971 requirements to ensure that

single failures do not simultaneously degrade the protection system and force challenges to the protection system
- Operator information is simplified.
- Plant sensors are minimize reducing initial capital cost and plant operation and maintenance burden.

o Control sensors shall be eliminated only where there are duplicate protection system sensors with adequate range and accuracy to meet the control system requirements.

o Control sensors shall not be eliminated where diversity from the protection system is required as for the alternate protection system.

Where safety sensors are used in the control system the following design bases apply:

o Safety sensor signals shall be transmitted to the control system via fiber optic cables to maintain electrical isolation.

o The control systems shall receive sensor analog signals as directly as possible to minimize signal latency and potential adverse impact to control system response time performance.

o The signal validation software within the control system is not class 1E, but it is considered important to safety. Therefore it shall be designed and controlled as if it were class 1E.

o The DPS shall continuously compare the control system's "process representation" value (i.e. result of signal validation) to the DPS calculated "process representation" value. Differences that are outside a predefined tolerance shall be alarmed. This is a defense in depth feature to ensure correct control system performance.

The Nuplex 80+ control system sensor inputs are further discussed in Reference 1, section 7.7.1.1.13.

7.12 FIRE PROTECTION AND SABOTAGE

The following are the design basis for Nuplex 80+ compliance to Fire Protection and Sabotage design requirements.

7.12.1 Fire Protection

The Fire Protection features of the Nuplex 80+ Advanced Control Complex shall be designed to sustain an exposure fire while providing sufficient control of systems used to mitigate the consequences of a design basis event. The following are the individual design basis for Nuplex 80+ Fire Protection.

- o The fire tolerance of the Nuplex 80+ Advanced Control Complex shall protect against the loss of function of systems used to mitigate the consequences of a design basis event.

  This assures that sufficient fire protection is provided so that a fire which is not promptly extinguished will not prevent a safe shutdown of the plant. This is accomplished by separating safety channels into four independent plant fire zones (A,B,C,D) such that the effects of an exposure fire are limited to only one channel. The computer room and Division N equipment room shall be in an additional two separated fire zones. The separate fire zones shall be maintained in all areas of the plant except the main control room and remote shutdown control room.

- o Where multiple channels must come in close proximity (i.e. where fire zones cannot be maintained) such as within the Main Control Panel and Remote Shutdown Panel, the following design bases apply:

- The channels shall remain electrically independent
- Wire coding shall be used to distinguish each channel.
- The channels shall be separated by a minimum distance to prevent flash over between channels.
- Signals shall be less than 50 VDC. Power cables shall be no greater than 120 VAC/125 DC and shall be enclosed in conduit or separated from low voltages by at least 6 inches.

This design ensures that single credible failures (not catastrophic failures) will not result in erroneous control signals to multiple channels.

To accommodate catastrophic events the design shall incorporate other features defined below.

o Fire isolation shall be maintained between the main control panels, remote shutdown panel and the equipment rooms and plant areas which house the I&C equipment.

This assures that a fire in the main control room or at the remote shutdown panel will not propagate to the other location or to the I&C equipment locations. In addition this assures that one facility remains intact to initiate a shutdown and that the necessary I&C equipment for shutdown is not affected by a fire at either the main or remote shutdown facility.

This is accomplished via establishment of fire barriers between the main control room, remote shutdown room and the four independent equipment areas which house the safety related I&C equipment and the two equipment rooms that house the non-1E I&C equipment.

- o Where all channels must be in close proximity (i.e., at the Main Control Panels and Remote Shutdown Panel) isolation shall be provided to assure that electrical faults at these locations will not propagate failures in the remotely located system electronics.

  This is accomplished via use of fiber optic cables between the MCP, RSP and I&C equipment rooms.

- o Control disconnect and transfer devices shall be provided to disconnect MCP controls (which are normally active) and transfer control to the RSP (which is normally inactive).

- o The MCP disconnect devices shall be located in the Main Control Room to allow rapid actuation by the operator.

  Although fiber optic cables isolate faults that could potentially damage the I&C systems, these cables cannot distinguish between valid and erroneous control signals. Locating disconnect switches in the Main Control Room allows operation to stop propagation of false signals from the control room to the I&C equipment, promptly after a catastrophic event is detected (e.g. a fire). Any false signals that may have been transmitted prior to activating the disconnect can be corrected when the operator takes control at the RSP.

- o The location of the control transfer devices (transfer switches) between the main control room (MCR) and remote shutdown panel (RSP) shall be in an area which is separate from and immune to faults at either the MCR or RSP. Also, no single failure (including a fire) shall result in inadvertent transfer or the prevention of transfer of more than one channel of equipment.

The transfer devices must be protected against faults resulting from fires so that successful control transfer between the main control room/RSP can be accomplished.

This is accomplished by locating the transfer devices for each channel away from the RSP and MCP and within the corresponding separate fire zones which house the I&C equipment.

- To ensure bumpless disconnect and transfer all controls at the RSP and the MCP shall be passive. Momentary control switches shall be used with all control commands, setpoints, . stored in the remote system electronics, not in the control panel devices.

  This feature ensures that transfers do not result in spurious control actions. It also allows control panel devices to be disconnected for maintenance of the control systems.

- The remote shutdown panel shall be capable of achieving a cold shutdown condition.

  Advances in digital technology offer the capability to centralize cold shutdown indications and controls at the RSP without duplication of the extensive instrumentation in the MCR and without the need to access local controllers distributed througnout the plant.

  This is achieved by providing touch sensitive "soft controls" for all plant components necessary to achieve cold shutdown on the remote shutdown panel.

7.12.2 Sabotage Resistance

The sabotage resistance features of the Nuplex 80+ Advanced Control Complex shall provide protection against a knowledgeable insider from defeating or adversely affecting any safety related system or function. The following are the individual design basis for Nuplex 80+ sabotage resistance.

- o With the exception of sensors, controlled components and remote multiplexors, I&C equipment not located within the MCR or RSCR shall be located in separate channelized equipment rooms.

- o Sensors, components and remote multiplexors shall be separated by the maximum distance practical.

- o All I&C cabinets shall be equipped with locks and door entry alarms.

- o Unauthorized entry into any single equipment room or vital I&C instrument cabinet, by a knowledgeable insider, shall not result in defeating or adversely affecting any safety related system or function.

  Since multiple equipment rooms and cabinets must first be entered before a safety system or function can be defeated, there is ample time to detect and respond to the threat.

  This is achieved by separating the four safety related I&C equipment channels into four separate equipment rooms with each having a single controlled access entry point. In addition, vital I&C cabinets within each of these rooms shall be locked and shall contain an internal entry alarm.

- o Unauthorized entry into any single remote I&C cabinet or motor control center (MCC), by a knowledgeable insider, shall not result in defeating or adversely affecting any safety related system or function.

  Since multiple cabinets or MCCs must first be entered before a safety system or function can be defeated, there is ample time to detect and respond to the threat.

  This is accomplished by physically separating remote I&C cabinets and MCCs and alarming access.

- o Digital based safety related systems shall be protected against unauthorized alternations to software (this includes setpoints and code).

  By providing suitable protection for software, the integrity of the digital safety systems will be maintained.

  This is accomplished by utilization of memory protection facilities within the safety related digital systems to "lockout" software from alterations and by continuous on-line monitoring of memory checksum by the Data Processing System (DPS) to detect any alterations.

7.13 FIELD TERMINATION METHODS

- The Nuplex 80+ design shall use compression screw terminal blocks as the standard method for field termination.

  Compression screw terminal blocks offer many advantages over ring lug connections for field wiring termination. These include a significant reduction in installation labor time compared to ring lug connections. Compression screw terminal blocks also provide a higher density of field terminations which leads to improved maintainability by providing more working space within the enclosures in which they are located. More working space is made available while still allowing smaller enclosures. These result in considerable savings in floor space and, therefore, reduced civil construction costs. Compression screw terminations have been used in world-wide industrial and international utility applications for many years, but have not generally been used by the U.S. utility industry. They have clear cost and schedule advantages over ring lug connections. Ring lug connections can be provided for Nuplex 80+ as an option.

7.14 FAIL-SAFE DESIGN

This section defines the mode of operation on loss of power, data communications or equipment failure for major portions of the Nuplex 80+ design. These failure modes are applied in general however specific designs may require exceptions to these design bases. Exceptions are accommodated on a case by case basis.

- On loss of power or equipment failure the PPS shall fail with its output(s) generating trip signals to the RTSG and/or ESF-CCS.

  The PPS is designed to fail actuated in accordance with the General Design Criteria. Due to the independence of each of the four PPS channels and the 2-out-of-4 trip channel arrangement, single channel failures will not cause spurious trips nor prevent valid trips.

  It is noted that other NSSS vendors have licensed PPS designs where the containment spray function does not fail actuated. This will be evaluated for Nuplex 80+ in the future.

- A PPS channel failure or inter-channel trip path data link failure shall result in a single channel trip in the unfailed channels. An exception to this shall be in the CPC's where a CEAC failure shall not cause a trip condition.

  If a PPS channel cannot receive data from another PPS channel the receiving channel shall assume the sending channel has failed. To support the previous fail actuated design bases this shall result in a single channel trip condition. This philosophy is not followed in the case of the CEACs due to the 1-out-of-2 penalty factor logic in the CPC - Trip Limit Calculators. For a CEAC failure or data link failure an alarm is generated forcing Limiting Conditions of Operation (LCO) in accordance with the plant's technical specifications. These LCOs accommodate operation with the one remaining CEAC channel.

- The CCS shall fail with its control outputs unactuated.

  This will result in the following failure modes for various types of controlled equipment:

  - Motor operated valves - fail as-is
  - Solenoid operated valves/dampers - fail as defined on piping and instrumentation diagrams (e.g. FO,FC)
  - Contactor operated pumps, heaters, fans, etc. (usually 480V and lower) - fail de-energized
  - Electrical distribution breakers - fail as-is
  - Circuit breaker operated pumps, heaters, fans, etc. (usually greater than 480v) - fail as-is

  For the ESF-CCS this is a significant departure from the previous ESFAS-Auxiliary Relay Cabinet which is designed to fail-actuated. However, this is consistent with the TVA-CCS design and designs of other plants that utilize a common system for automatic ESF actuation and manual control of ESF components (e.g. YGN 3&4).

  In previous designs (e.g. ANPP) where the ESFAS and manual control functions are separate, the manual control function is designed to allow operator override of the ESFAS function. Therefore, if spurious ESF actuation occurs (due to its fail-actuated design) the operator can intervene to secure the ESF system. It is noted that the manual control part of previous systems has always been designed to fail-unactuated.

The automatic ESF function and manual control function have been combined in the Nuplex 80+ ESF-CCS to minimize the cost of the CCS and to minimize the cost of CCS to component interfaces (e.g. relays, cables, cable trays and terminations). This is consistent with the YGN 3&4 design. Although the ESF-ARC is retained for YGN, its signals interface to plant equipment via the Interposing Logic System. Within the ILS the ESFAS and manual control signals are combined to provide a single interface to the controlled equipment (as in Nuplex 80+, to reduce costs).

It is noted that within the ESF-CCS the ESFAS logic (which is equivalent to the logic performed in the ESFAS-ARC) is designed to fail-actuated. Thus, the automatic ESF function is designed as conservatively as possible, but the manual override capability of previous designs is retained.

o As much as practical, the PCS shall fail in a mode that holds CEAs stationary and retains turbine control signals as-is.

  It is recognized that there will be failure modes that result in rod drops and changes to turbine control signals, but this will be minimized.

o The DPS and DIAS shall fail without generating unrelated alarms; all displays shall clearly indicate that the data is not being refreshed.

o On failure of data links between Nuplex 80+ systems the receiving system shall alarm the communication failure and should utilize the last good data value in its calculations.

  This approach minimizes plant disturbances and allows operator intervention to avoid future transients.

7.15 HEATING, VENTILATION AND AIR CONDITIONING

The following are design bases for Nuplex 80+ HVAC.

- The Control Building Ventilation and Air Conditioning Systems shall be designed to maintain the environment in the control complex within acceptable limits for the operation of unit controls, for maintenance and testing of the controls as required, and for uninterrupted safe occupancy of the control building area during post-accident shutdown.

- The control room shall be designed to maintain approximately 73°F to 78°F and 20% to 60% maximum relative humidity. The computer room shall be designed to maintain a maximum temperature of 85°F. The I&C equipment room shall not exceed 104°F. All plant areas for remote multiplexor shall not exceed 122°F. These conditions shall be maintained continuously during all modes of operation for the protection of instrumentation and controls, and for the comfort of the operators.

- Continuous pressurization of the control room and the control room area shall be provided to prevent entry of dust, dirt, smoke, and radioactivity originating outside the pressurized zones in accordance with the intent of NUREG-0700 requirements. Pressurization shall be maintained slightly positive relative to the pressure outdoors and in surrounding buildings.

- Outdoor air for pressurization shall be taken from either of two locations such that a source of uncontaminated air is available regardless of wind direction. Each air intake shall be located as far away from the diesel generator exhaust as practical. All outside air shall be filtered.

- o Each outside air intake location shall be monitored for the presence of radioactivity, toxic gases, e.g., chlorine, and products of combustion. Isolation of the outside air intake shall occur automatically upon indication of high radiation level, high chlorine concentration or smoke concentration in the intake. Should both intakes close, the operator shall have the ability to override the intake monitors and by inspection of the control room readouts select the least contaminated intake. This will ensure pressurization of the control room at all times.

- o Each outside air intake is provided with a tornado isolation damper to prevent depressurization of the control room during a tornado.

- o All essential air conditioning and ventilation equipment shall be able to perform required safety functions assuming the worst single failure of an active component concurrent with a loss of offsite power.

- o All essential air conditioning and ventilating equipment, ductwork and supports shall be designed to withstand the safe shutdown earthquake. In addition, this equipment shall be protected from the effects of internally generated missiles, pipe breaks and water spray. Essential electrical components required for the heating, cooling, and pressurization of the control complex during accident conditions shallbe connected to emergency Class 1E standby power.

- o Instrumentation shall be provided for the air conditioning systems to control and indicate the temperature, and to indicate radioactivity levels. Early warning ionization-type smoke detectors shall be located in the supply, return and outside air ductwork serving the Control Room Area Ventilation System.

- o The control complex HVAC shall be designed such that a single credible event can result in uncontrolled environmental conditions in no more than one of the following areas: Equipment Room (ER)-A, ER-B, ER-C, ER-D. There shall be no single credible event that can effect the environment in ER-N, computer room, main control or remote shutdown room.

- o The control complex HVAC systems shall be designed such that a single catastrophic event can result in uncontrolled environmental conditions in no more than one of the following plant areas: ER-A and ER-C, ER-B and ER-D, ER-N, computer room, main control room, remote shutdown control room.

ATTACHMENT 2

NUPLEX 80+ COMPLIANCE WITH NUREG-0737 SUPPLEMENT 1 REQUIREMENTS

Requirement 1: Should provide a concise display of critical plant variables to control room operators.

The Nuplex 80+ Advanced Control Complex provides a concise display of critical function and success path performance indications to control room operators via the Data Processing System (DPS), i.e., the plant computer. All critical function alarms, variables and parameters, those related to safety or critical power production, are located on a single display screen. This overview display called the Integrated Process Status Overview (IPSO), is designed to support both normal and emergency operations. The set of information provided to the operators in this concise subset of all DPS data is particularly useful in assessing plant safety status.

Requirement 2: Should be located convenient to control room operators.

Critical function information is provided through a dedicated DPS critical function display page hierarchy and is available on all CRTs in the Nuplex 80+ control complex. There is a CRT on every panel section in the controlling workspace (e.g., RCS, CVCS, ESF, etc.). There are also two CRTs on the control room supervisor's console, one each in the shift supervisor, control room supervisor and operator offices, as well as in the technical support center. In addition, the IPSO big screen, in front of the control room, displays a concise overview of critical functions and success paths at a location which is convenient to anyone present in the control room.

Requirement 3: Will continuously display plant safety status information.

The IPSO big board display is a dedicated display which continuously shows all critical function alarms and key critical function and success path parameters to the control room operators. Operators do not have the option to display any other screens or information on the big board. The information displayed on IPSO, though fixed, is mode dependent such that it is applicable and useful for determining plant safety status during normal, transient and accident conditions.

Requirement 4: Should have a high degree of reliability.

The DPS system, which provides the Nuplex 80+ SPDS function, has a reliability of greater than 99.99%. This reliability was calculated based on a formal reliability analysis and hardware information supplied by potential vendors.

Requirement 5: Shall be suitably <u>isolated</u> from electrical or electronic interference with safety systems.

The DPS system is a redundant system which is fully isolated from all safety systems. The DPS relies on fiber-optics for communication with safety systems. The fiber-optics serve as isolators such that no propagation of electrical fault is possible. Further, the DPS receives only data from the safety systems; there is no control interface from the DPS to the safety systems.

Requirement 6: Shall be designed incorporating accepted <u>Human Factors</u> Engineering Principles

The DPS MMI design has been developed according to a comprehensive ABB-CE Human Factors Standards and Guidelines for System 80+. These standards were developed based on accepted industry and generic human factors principles and guidelines which are fully documented and cross-referenced. The human factors engineering process has used accepted ergonomics techniques to assure that displayed information can be readily perceived and comprehended by Critical Functions Monitoring (i.e., SPDS) users.

Requirement 7: <u>Minimum information</u> displayed shall be sufficient to determine plant safety status with respect to five safety functions:

i. Reactivity Control
ii. Reactor Core Cooling and heat removal from the primary system
iii. Reactor coolant system integrity
iv. Radioactivity control
v. Containment conditions

All five of these elements are included in the DPS Critical Functions Monitoring hierarchy which forms the basis of the Nuplex 80+ SPDS function. Critical functions include reactivity control, core heat removal, RCS heat removal, RCS inventory control, RCS pressure control, radiological emissions control, containment environment control, containment isolation and vital auxiliaries. These functions exceed the minimum needs for SPDS specified in NUREG-0737, Supplement 1. Specific parameters were determined based on human factors engineering and operations input.

Requirement 8: <u>Procedures</u> and operator <u>training</u> addressing actions with and without SPDS should be implemented.

The System 80+ Critical Functions Monitoring function (SPDS) is being developed in a complementary (parallel) fashion with the development of System 80+ Emergency Procedure Guidelines. Generic emergency procedure guidelines are used during the design process. In developing System 80+ guidelines which involve use of SPDS information, provisions for operating with and without Critical Functions Monitoring are being made.

ATTACHMENT 3

The following items from the Human Factors Standards, Guidelines and Bases for System 80+ will be incorporated into the HFE Tracking System:

"The use of engineering units shall conform to the standards of [TBD]." (p. A-38, Section 2.4.7, Engineering Units)

"Installed equipment items with unique designators shall incorporate some form of scan code system [TBD] into their labels that will provide access to O&M databases." (p. A-39, Scan Codes).

Scan Code - The item's scan code shall be [TBD]." (p. A-40, Section 2.5.5, Layout of Identification Labels).

"These items, in addition to identification, shall be labelled to indicate contents, rated pressure, and direction of flow. Piping shall be so labelled every [TBD] feet. (p. A-43, Section 2.5.12, Tanks, Filters, Heat Exchangers, & pipes)

"Supplemental keys, such as shown in broken outline in Figure 3.3.2, should use a standard arrangement which is [TBD]." (p. A-55, Section Alphanumeric Keyboards)

"There are a variety of different touch screen technologies with distinct advantages and disadvantages. The standard touch screen mechanism is [TBD]." (p. A-59, paragraph 1)

"Printers [TBD]" (p. A-62, Section 3.6, Printers)

"Vibration [TBD]" (p. A-91, Section 7.4, Vibration)

"Installed Platforms, Workstands, Stairs and Ladders [TBD]" (p. A-95, Section 7.5.8)

"Equipment items that are entered in the planned maintenance system shall be labelled to incorporate a selected scanning technology [TBD] to provide a direct interface to the planned maintenance system database through portable laptop-type computers." (p. A-116, paragraph 1)

"Cranes, Hoists, & Lifting (TBD" and "Scaffolds, Stands, & Miscellaneous Facilities [TBD]" (p. A-18, Sections 8.3.2 and 8.3.3, respectively)