TS(MISC2)/lr 1

CONTROL COMPLEX INFORMATION SYSTEM

BASES

FOR

NUPLEX 80+

NPX80-IC-DB791-01

ABB COMBUSTION ENGINEERING, INC.
Nuclear Power
Windsor, Connecticut 06095-0500

Issue Date 1/15/93

RECORD OF REVISIONS

NO.	DATE	PAGES INVOLVED	PREPARED BY	APPROVALS
00		All		

TABLE OF CONTENTS

TABLE OF CONTENTS (continued)

1.0 INTRODUCTION

1.1 PURPOSE

This document provides the bases for the material presented in the Control Complex Information System Description (CCISD) for Nuplex 80+. The purpose of the CCISD Basis is to provide references and explanations applicable to the CCISD.

1.2 APPROACH

CCISD Basis information may take one of two forms:

1) Reference - Where bases are provided in design documents or docketed material, direct reference to the source is provided.

2) Rationale - In some cases, a basis may not exist in reference material. In these cases, a rationale is provided to explain the reasons and justification for the decision. In some cases, the rationale may take particular note of a specific section of a reference.

Some CCISD document subheadings are simply introductory or other general explanatory material. Where a subheading does not itself present design standards or guidance immediately below, the statement "No CCISD entries" will appear below in its corresponding CCISD Basis entry. References provided in a higher level heading apply to CCISD entries at lower levels unless more specific basis material is provided.

The CCISD Basis begins with Chapter 3 of the CCISD, since Chapter 1 was introductory material and Chapter 2 was scope material.

2.0 SCOPE

Consistent with the CCISD, the bases presented in this document are applicable for all main control room information features in the NUPLEX 80+ advanced control room and the Nuplex 80+ remote shutdown panel. These features are expected to be applied to the entire plant with exceptions identified and evaluated. Exceptions to these bases may exist on a case by case basis for pre-packaged control room displays that are provided as an integral part of another suppliers product (e.g., Main Turbine Generator panel insert). For these displays a mapping is performed to ensure that there are no unacceptable conflicts with the Nuplex 80$^+$ design. The bases provided herein should support evaluation of the trade-offs required for application of the standard MMI design features and characteristics to pre-packaged displays and controls, and/or displays and controls outside of the Main Control Room and Remote Shutdown areas. The majority of design bases for Nuplex 80$^+$ information presentation is documented in Reference 1.

3.0 NUPLEX 80+ CONTROL ROOM INFORMATION OVERVIEW

Rationale: It is taken to be self-evident that "rapid and accurate, monitoring and control" is needed for safe, reliable and efficient operation of nuclear facilities, as is ease of information availability and provision of an operator-supportive format.

3.1 MAN-MACHINE INTERFACE

Rationale: The Nuplex 80+ Man-Machine Interfaces (MMI's) are designed in an integrated hierarchial ensemble, with no interface considered as unused "back up", and with appropriate diversity in hardware and software as defense-in-depth against common-mode failures. As noted in Ref. 1 (Section 5.2), a hierarchial organization was chosen as being appropriate because an operator requires different levels (e.g., general plant monitoring, specific systems or functions, detailed diagnostics) of information for support of tasks at various times during plant operation. Spatial dedication of selected MMI's was retained as a positive feature of the "current generation" of control rooms in providing frequently used, and important, functionally related information.

3.2 INFORMATION PROCESSING

COMPONENT/SYSTEM UNAVAILABILITY AND POOR PERFORMANCE

Rationale: As stated in the CCISD, the basis for algorithms to monitor equipment/system unavailability and performance is that this information helps notify the operator about undesirable changes in equipment/system status. The use of such algorithms is based on the Nuplex 80+ design basis goal of reducing the operators information processing burden. The use of safety-related parameters in validation algorithms with non-safety parameters is to enable alarms and indications to be based upon a single "Process Representation Value", with the operator being notified of deviations among the set of safety and non-safety channels. This enables a reduction (relative to prior control room methods of simultaneously presenting indications of all channels) in the operator's information processing burden, since simple algorithms are continually doing cross-channel comparisons. This also enables the indicators (DIAS) to be used by the operator at all times (no unused back-ups), since the validity of the single "Process Representation Value" with respect to Post-Accident Monitoring Instrumentation is always known to the operator.

COMPUTERIZED ALARM PROCESSING

Critical Functions and Success Paths Monitoring

References: Reference 1 - 5.2, 5.8

Composed Point Processing

Rationale: The basis for composed point processing in the Data Processing System is to establish an organized "building-block" approach, wherein component status and process information is used to compose the next higher level (e.g., flow path) of information, which in turn can be used to compose the next higher level of information (e.g., train), and so on. At each level the various composed points are appropriately linked to the alarm, status symbol or graphic indication, etc. that identifies to the operator the required information. This method is used to ensure consistency, provide a relational basis to the operator to rapidly find the sources of problems, and to support the operator's choices during diagnosis to seek out succeeding lower levels of causes preceding effects.

Composed Component Status

Rationale: Composed component activity and status is performed by the Data Processing System (DPS). The DPS uses the component control system actuation logic outputs to present component activity status and composed system and status. Display real estate is also conserved.

Composed Alarm Status

Rationale: Composed alarm status for a system and its trains follow the method described for Composed Point Processing, above, i.e., a building-block approach to providing component alarm information. Critical Function status check acceptance criteria alarms are separate from the composed system and train alarm algorithms because the critical function alarms are based upon parameters indicative of the adequacy of the maintenance/restoration of critical safety functions (e.g., RCS heat removal), rather than the one or more systems that can be used to do the maintenance/restoration (success path monitoring).

COMPOSED COMPONENT AND PARAMETER ALARMS

Composed Component Alarms

Composed component alarms are based upon combinations of conditions, including plant operating mode, indicative of an unsatisfactory condition of the component.

Composed Parameter Alarms

Rationale: Composed parameter alarms are based upon combinations of conditions, including plant operating mode, indicative of a process representation parameter value deviation exceeding a setpoint.

Trend Arrow

Rationale: The trend arrow was chosen as an effective and simple method to quickly inform the operator of static or changing trend conditions for important parameters and to reduce the amount of display space (relative to continual displays of trend graphs) required to do so. The trend arrow is used for indication and alarm of immediate conditions and does not supplant trend graphs provided on DIAS indicators or the DPS Historical Data Storage and Retrieval System, which are used for operator review of system performance over a period of time.

Composed Trend Graph

Rationale: The composed trend graph basis is to provide the operator with information of a current and historical nature which directly supports decision-making and analysis required for normal and emergency procedures.

3.3 DOCUMENT DESCRIPTION

This section merely summarizes the organization of Sections 4.0 through 11.0, and does not require bases.

4.0 GENERIC INFORMATION PRESENTATION METHODOLOGY

Rationale: It is taken as self-evident that standardization of information display and access reduces operator workload associated with accessing and processing information. The bases for conventions in this section are generally included in the description of the feature in the CCISD, and/or can be found in the indicated sections of Reference 2. Additional rationale is provided below for some cases.

TEXT AND DATA

Rationale: Labels, abbreviations and acronyms, and units were judged to be the principal text and data elements requiring standardization.

References: Reference 2 - 2.2, 2.4, 2.5

PROCESS REPRESENTATIONS

Rationale: Display designs are initially developed based upon physical plant layout and design documents (e.g., P & ID's). Standard display formats were developed as defined in Sections 6 - 10 of the CCISD. Initial display designs are subject to modification during design reviews, task analysis, and validation and verification.

GRAPH LAYOUT AND INFORMATION PRESENTATION

References: Reference 2 - 2.3.5

4.1 DISPLAY PAGE CREATION CRITERIA

Rationale: Guidelines for display page creation are established for consistency among display formats. Consistency is needed to reduce operator search and analysis, which otherwise would unnecessarily increase because of variability among display formats and layout methods.

DATA CONTENT/DISPLAY PAGE DENSITY GUIDELINES

References: Reference 2 - 4.1

GRAPH CREATION CRITERIA

References: Reference 2 - 2.4

4.2 COLOR AND SHAPE CODING CONVENTIONS

References: Reference 2 - 2.3

COMPONENT CODING SUMMARY

Rationale: The four characteristics of position/status, control, alarm, and data quality are sufficient to characterize the component state for operator task needs.

COMPOSED SYSTEM STATES

Rationale: The composed system states are used on IPSO and certain CFM and other system monitoring display pages to represent systems whose operating status is important to the understanding and comprehension of the information provided on the display page, but whose mimic would not fit on available display "real-estate".

5.0 INTEGRATED PROCESS STATUS OVERVIEW (IPSO)

References: Reference 1: Sections 5.5.1, 5.8; Reference 5: Section 4.4.8.2

Rationale: Advanced control rooms including Nuplex 80^{+} rely on selectable information, much of which is typically presented on CRT's. Although effective in providing detailed information to the operators, the operators' ability to obtain a "feel" for the plant is diminished. An overview display provides the operating staff with the information necessary to develop an overall assessment of plant operation. Also, the overview display consideration is an EPRI requirement (Ref. 5, Section 4.4.8, Integrating Displays and Mimics) and is supported by studies at the Halden Reactor Project in Norway.

5.1 IPSO REPRESENTATIONAL CHARACTERISTICS AND FEATURES

Rationale: The basis of the IPSO design is that the operator's overall assessment of plant status can adequately be characterized by the status of a limited set of critical safety functions, power production functions, and the success paths that are used to maintain or restore those functions, including availability monitoring of safety systems per Reg. Guide 1.47. The information provided on IPSO is based upon this approach to plant overview display design. In addition, the design meets the top-level Safety Parameter Display System (SPDS) continuous display requirements per NUREG 0737, Supplement 1.

5.2 DISPLAY CRITERIA FOR IPSO

References: Reference 2 - 2.2, 2.3, 2.4, 2.5, 4.1; Reference 3

5.3 SYSTEMS REPRESENTED ON IPSO

References: Reference 4 - 4.0

Rationale: The systems chosen for representation on IPSO are the major heat transport path systems and success paths that are required to support the critical functions. Other, less important, plant systems or functions were judged to be unnecessary for the IPSO design. Further discussion is provided in Ref. 4.

5.4 SAFETY INFORMATION ON IPSO

References: Reference 4 - 3.2, 4.0

6.0 CRT DISPLAY PAGES: ARRANGEMENT AND ACCESS

References: Reference 1 - 5.5.4; Reference 2 - 4.0

6.1 NAVIGATION BETWEEN DISPLAY PAGES ON THE CRT'S

References: Reference 1 - 5.5.4; Reference 2 - 3.4.9, 4.2; Reference 5 - 4.4.9.3

6.2 OTHER METHODS OF NAVIGATION: POINT POKE

Rationale: The point-poke method of navigation is helpful in directly providing the operator with information related to a component or parameter, without the operator having to search among menu options or directories. Also, point-poke is the means by which important information can be directly accessed, but which is not provided on another display page.

6.3 CFM DISPLAYS

Rationale: The CFM Level 1 pages provides more detail on the critical function matrix presented on IPSO; this helps guide the operator to the appropriate Level 2 critical function display page. The CFM Level 2 display pages are provided to give the operator summary information on the status checks for a critical function, and the success path availability and performance status for maintenance or restoration of that function. The displays are developed and organized to be consistent with Emergency Procedure Guidelines.

7.0 DISCRETE INDICATION DISPLAYS

References: Reference 1 - 5.5.2, 5.5.3; Reference 2 - 2.3, 4.0, 5.0

7.1 DISCRETE INDICATION PRESENTATIONS AND ACCESS

Rationale: The choice of using single process representation parameters, that are validated, meets task analysis requirements, while reducing stimulus overload and task loading that would otherwise result from presentation of multiple sensor channels that represent a single plant parameter. Trends are provided on discrete indicators when task analysis indicate the trend is useful for routine monitoring or abnormal event diagnosis. Auto-ranging (with operator notification) results from the above approach of giving the operator a single process representation parameter (vs. many), and avoids having to have a process representation parameter displayed to the operator for each range. Cross validation of DPS and DIAS displayed values is performed to ensure consistency and avoid operator confusion. Temperature compensation of levels is provided so that the same process representation parameter is valid for both "hot" and "cold" conditions.

INFORMATION ACCESS

Rationale: DIAS provides menus for monitoring of individual sensors so that the operator can have discretionary access to all sensor values that are being used for calculation of the process representation parameter value. This is primarily required for continued operation with the failure of the DPS (i.e., CRT information is not available). It also allows an individual sensor to be chosen by the operator for display in analog bar graph format in the event that the algorithm is not able to calculate a process representation value.

TOUCH BUTTON PHILOSOPHY

Rationale: Touch button interaction with DIAS displays was chosen as an effective use of available technology for flat-panel displays, versus other possibilities such as command languages (keyboard), or trackball (with cursor). Also see Reference 2, Section 3.4.9.

7.2 DEDICATED PARAMETER DISPLAYS

Rationale: The trend/analog page was designed to give a generally complete (process representation value, quality flag, PAMI correlation flag, range scale, normal operating range delimiters, analog bar graph, trend-time-scale, and trend graph) display of a single process parameter. The menu page was designed to supplement the trend/analog page to give operator access to the individual sensor values and enable operator selection of an individual sensor when the validation algorithm cannot calculate a process representation value.

7.3 MULTIPLE PARAMETER DISPLAYS

Rationale: The multiple parameter display is designed to support normal operation and continued operation without the DPS system. They do not have trends because trend information is not critical for parameters selected for this type of display, and because of the number of values required to be displayed. Note that dedicated DIAS displays with trends are available with DPS unavailability.

8.0 ALARM INFORMATION IN NUPLEX 80+

References: Reference 1 - 5.3, 5.8; Reference 2 - 2.0, 5.0; Reference 4 - 4.3

8.1 GENERIC ALARM PROCESSING CHARACTERISTICS

References:

Partitioning:	Reference 2 - 5.3.1 (a), (d)
Mode Dependency:	Reference 2 - 5.1.1 (c)
Equipment Status Dependency:	Reference 2 - 5.1.1 (c)
Acknowledgement:	Reference 2 - 5.4.1 (a)
Messages:	Reference 2 - 5.1.1 (e), 5.4.1 (a)
Prioritization:	Reference 2 - 5.1.2
Operator Aids:	Reference 2 - 5.1.2 (c)

8.2 ALARM STATUS AND PRESENTATION METHODS

References:

Annunciator States:	Reference 2 - 5.1.3
Representations:	Reference 2 - 5.1.2 (e)
Flash Coding:	Reference 2 - 5.3
Audible Information:	Reference 2 - 5.2
Flash Suppression:	Reference 2 - 5.4.1
Unacknowledged Alarm Buffer:	Rationale: This provides alarm handling to allow display on MMI devices of the most pertinent alarm information.

8.3 ALARMS PRESENTED ON CRT'S

ALARM ACCESS VIA CRT MENU AND DIRECTORY PAGES

Rationale: Use of the navigation method, i.e., Menu's and Directories, was judged to be an appropriate and effective method to assist the operator in locating the display page(s) on which the source(s) of the alarm could be located. The method is direct and rapid, in contrast to solely using other methods such as requiring the operator to first go to an alarm list, or having the operator choose the appropriate display page(s) on his/her own judgement.

ALARM ACKNOWLEDGEMENT

SINGLE ALARMS **(Rationale):**

1. Tiles: This method chosen was selected to be consistent with the DIAS method.

2. Display Page Descriptors: This method was selected to allow alarm acknowledgement in the context of related process information and to be consistent with the "Point-Poke" method of lower-level information and display page choices.

MULTIPLE ALARMS **(Rationale):**

3. Unacknowledged Alarms List: This method was chosen so that when more than one alarm comes in, the operator has a method to rapidly review and acknowledge multiple alarms.

4. Display Page Descriptors: This method allows the operator to quickly go through acknowledgement of all alarms associated with a given display page descriptor in the context of related process information.

5. DIAS Alarm Tile: This method allows the operator to acknowledge and view alarm conditions using the same method (via CRT) that would be used had he chosen to acknowledge the DIAS alarm tile.

METHODOLOGY FOR LOWER LEVEL ALARMS TO "FILTER UP" TO HIGHER LEVELS

Rationale: The described method was chosen as an appropriately logical method to direct an operator for alarm acknowledgement, when an alarm can feasibly be displayed on more than 1 display page. The examples provided in the CCISD show the implementation of the bases provided in the CCISD.

CRT ALARM LISTS

References: Reference 5 - 4.3.4; Reference 4 - 4.3.4.8.1

Rationale: The prioritized list, hierarchial group list and time sequential list were chosen to provide alarm organizations that support the operator in accessing alarm information to assist in finding the source(s) of faults or responding to alarm conditions.

OPERATOR AIDS

References: Reference 2 - 5.1.2 (c)

OPERATOR ESTABLISHED ALARMS

References: Reference 1 - 5.3; Reference 5 - 4.3.2.4; Reference 4 - 4.3.2.4

HISTORICAL DATA STORAGE AND RETRIEVAL: HDSR

Rationale: The retention of alarm history and other parameter data points is necessary to review and analyze plant evolutions, either for diagnostic or optimization purposes.

8.4 ALARM DISPLAY ON ALARM TILES

References:

Alarm Tile and List Pages:	Reference 1 - 5.3
	Reference 2 - 5.3.1 (a), (d)
Alarm Conditions:	Reference 1 - 5.3
	Reference 2 - 5.1.2, 5.1.3, 5.3

9.0 COMPONENT CONTROL REPRESENTATION/INFORMATION

References: Reference 1 - 5.4, 5.5.6

Rationale: Standardization of component control representations and information lessens the number of different types of status indications and control logics which the operator was required to remember on prior, unstandardized control rooms. Nuplex 80+ design selections are "encompassing" for the types of plant components described in the CCISD which are used in the System 80+ plant design. If any specific component and its operation are found to not be encompassed by the standard design of this section, either a new category for a standard would be developed, or, as is more likely, a modification to a standard design would be made so that it encompassed the component.

9.1 MAN-MACHINE INTERFACE FEATURES

No CCISD entries.

9.1.1 Switch Types

Rationale: Momentary type switches are easily replaced without affecting component control, and facilitate bumpless transfer of control between the Main Control Room (MCR) and the Remote Shutdown Panel (RSP). The three types of control switches are sufficient to provide physically distinguishable interfaces to the types of equipment for which MCR and RSP switches will be provided.

9.1.2 Valves

Rationale: The designs described in the CCISD for the categories and sub-categories of valves were based upon the types of valves on the System 80+ plant that are controlled via Nuplex 80*.

9.2 COMPONENT CONTROL CHARACTERISTICS/CONTROL STRATEGIES

No CCISD entries.

9.2.1 ESFAS Control Signals

References: Reference 1 - 5.7

Rationale: ESFAS signals are generated at a system level by automatic sensing of plant conditions, or by the operator. The operator is given the capability to override the ESFAS signal to an activated component (only after the ESFAS signal is generated) in order to respond to specific plant conditions and/or to undertake recovery operations after an abnormal event. If the operator action to override the ESFAS signal results in an improper equipment lineup, alarms are generated.

9.2.2 Bypassed or Inoperable Status Monitoring

References: Reference 1 - 5.7

9.2.3 ESF Activation Status Monitoring

References: Reference 1 - 5.7

9.3 INTERLOCKS AND ACTUATION SIGNALS

No CCISD entries.

9.3.1 Interlock Signals

Rationale: "Interlocks" are provided in Nuplex 80$^+$ as permissive functions that inhibit an operator action and cannot be overridden by the operator. They are distinguished from the class of "activation" signals (9.3.2), which in some cases can be overridden by the operator. Interlocks are used to prevent high risk actions from occurring due to equipment failures or operator error.

9.3.2 Actuation Signals

References: Reference 1 - 5.5.6

Rationale: The design approaches selected were chosen to encompass the actuation and override conditions required for System 80$^+$ plant equipment.

9.4 OPERATOR SELECTED AUTOMATIC CONTROL SIGNALS

References: Reference 1 - 5.56

Rationale: The design approaches selected in 9.4 were chosen to encompass the automatic control mode selection options required for operator interface with System 80$^+$ plant equipment.

9.5 STANDBY CONTROL FUNCTIONS

References: Reference 1 - 5.5.6

Rationale: The design approaches selected in 9.5 were chosen to encompass the standby control functions required for System 80+ plant equipment.

9.6 PROCESS SIGNAL OR COMPONENT SELECTION

Rationale: One switch and status indicator per available process instrumentation channel was chosen to enable clear and positive selection and status of the operator's choice of input to the component control logic.

9.7 SUBGROUP CONTROLS

Rationale: Because subgroup control functional modes (on, auto off) are similar to individual component control functional modes (on, auto, off), status indicator designs for both were selected to be consistent where practical, so that variability in approaches to subgroup control is reduced.

COMPONENT DISCREPANCY

Rationale: Component discrepancies are individually indicated to the operator via "Operator Aids" (see 8.2 of the CCISD), because the effects of the discrepancies are manifested as alarms by composed system status and alarms as described in Section 8.2.

10.0 PROCESS CONTROLLERS

References: Reference 1 - 5.5.5

Rationale: Process controllers are designed to reduce the number of separate auto/manual control stations with which the operator must interact. Panel space is saved, cross-channel checking is accommodated, and easier control loop interaction for multiple related controls is provided.

11. SYSTEM OPERATORS MODULES

Reference: Reference 1 - 5.5.5.E

Rationale: As noted in the CCISD, operators modules are provided for control of specific systems or functions where the type of operator tasks or system control are better suited for control using physical control devices or task-oriented discrete indication and control devices. In addition, the CCS operator's modules provide access to all CCS controls and indication, and are used in the event of a failure of any CCS discrete controls or process controllers.

12.0 REFERENCES

1. Nuplex 80+ Advanced Control Complex Design Bases, NPX80-IC-DB-790-01, January 4, 1990.

2. Human Factors Engineering Standards, Guidelines, and Bases for System 80+, NPX80-IC-DR-791-02.

3. NUREG-0700

4. System Description for Critical Function and Success Path Monitoring in Nuplex 80+, NPX80-IC-SD790-02, Rev. 01.

5. EPRI ALWR Evolutionary Plant Utility Requirements Document.

ATTACHMENT 3

PLANT DESIGNERS OPERATIONAL SUPPORT
INFORMATION PLAN
FOR THE ABB SYSTEM 80+