Enclosure 22 to ET 07-0022

IEEE Standard 603-1998 Analysis

MAIN STEAM & FEEDWATER ISOLATION SYSTEM (MSFIS) CONTROLS REPLACEMENT

IEEE STANDARD 603-1998 ANALYSIS

REVISION 0

PROJECT MANAGER - GREGG CLARKSON
MANAGEMENT SPONSOR - PATRICK GUEVEL
EXECUTIVE SPONSOR - TERRY GARRETT

Wolf Creek Nuclear Operating Corporation
PO Box 411
1550 Oxen Lane, NE
Burlington, KS 66839

Table of Contents

1 Introduction

1.1 Purpose

The purpose this document is to provide an analysis of how the replacement Main Steam and Feedwater Isolation System (MSFIS) controls utilizing the Advanced Logic System (ALS) platform meet the requirements of IEEE Std 603-1998.

1.2 References

1.2.1 IEEE Std 323-1983 (Reaff 1996), IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations

1.2.2 IEEE Std 352-1987 (Reaff 1993), IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems

1.2.3 IEEE Std 379-1994, IEEE Standard Application of the Single Failure Criterion

1.2.4 IEEE Std 384-1992 (Reaff 1997), IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits

1.2.5 IEEE Std 577-1976 (Reaff 1992), IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations

1.2.6 IEEE Std 603-1998, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations

1.2.7 IEEE Std 627-1980 (Reaff 1996), IEEE Standard for Design Qualification of Safety Systems Equipment Used in Nuclear Power Generating Stations

1.2.8 IEEE Std 7-4.3.2-1993, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations

1.2.9 RTCA DO-254/EUROCAE ED-80, Design Assurance Guidance for Airborne Electronic Hardware

1.2.10 WCNOC ALS MSFIS Diversity and Defense-in-Depth Analysis

2 Analysis of IEEE 603-1998

The following provides the results of an IEEE Std 603-1998 analysis of the replacement MSFIS controls using the ALS platform. The paragraph numbers and text are directly from IEEE Std 603-1998 for easy reference to the standard.

5. Safety system criteria

The safety systems shall, with precision and reliability, maintain plant parameters within acceptable limits established for each design basis event. The power, instrumentation, and control portions of each safety system shall be comprised of more than one safety group of which any one safety group can accomplish the safety function.

Conclusion:

The ALS MSFIS will provide an increased level of reliability and better response time than the existing equipment. The present WCGS MSFIS architecture of two (2) safety groups will be retained.

5.1 Single-failure criterion

The safety systems shall perform all safety functions required for a design basis event in the presence of

a) Any single detectable failure within the safety systems concurrent with all identifiable but non- detectable failures.

b) All failures caused by the single failure.

c) All failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions.

Conclusion:

The ALS MSFIS System Reliability Analysis (SRA) includes a failure modes and effects analysis (FMEA) which shows that the criterion is met for all creditable single failures and all failures caused by the single failure.

5.2 Completion of protective action

The safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion. Deliberate operator action shall be required to return the safety systems to normal. This requirement shall not preclude the use of equipment protective devices identified in Clause 4, item k) of the design basis or the provision for deliberate operator interventions. Seal-in of individual channels is not required.

Conclusion:

This functionality exists in the current design and will be retained in the ALS MSFIS. After a trip signal (ESFAS input or ALL CLOSE input) is received, the trip signal must first no longer be present and then operator action (OPEN switch on MCB) is required to re-open the valves.

5.3 Quality

Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program (See ASME NQA-1-1994). Guidance on the application of this criteria for safety system equipment employing digital computers and programs or firmware is found in IEEE Std 7-4.3.2-1993.

Conclusion:

The design entity, CS Innovations, works under the quality assurance processes of RTCA DO-254, which the FAA has accepted for flight critical ASIC/FPGA designs and WCNOC considers to be equivalent to the software design process of IEEE Std 7-4.3.2-1993. Refer to Chapter 3 (page 21) of this document, "Mapping of IEEE Std 603-1998 to IEEE Std 7-4.3.2-2003 and DO-254".

5.4 Equipment qualification

Safety system equipment shall be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis. Qualification of Class 1E equipment shall be in accordance with the requirements of IEEE Std 323-1983 and IEEE Std 627-1980. Guidance on the application of this criteria for safety system equipment employing digital computers and programs or firmware is found in IEEE Std 7-4.3.2-1993.

Conclusion:

The ALS MSFIS equipment is being qualified and dedicated for Class 1E service by the project's 10 CFR 50 Appendix B supplier, Nutherm International (NI). Seismic and EMC qualification testing was performed with all of the ALS MSFIS components functioning and FPGA configurations representative of those used in actual operation, in accordance with IEEE Std 7-4.3.2 paragraph 5.4.1. The NI commercial grade dedication program includes the requirements of IEEE Std 7-4.3.2 paragraph 5.4.2.

5.5 System integrity

The safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. Guidance on the application of this criteria for safety system equipment employing digital computers and software or firmware is found in IEEE Std 7-4.3.2-1993.

Conclusion:

The ALS MSFIS is designed to perform its safety function when subjected to conditions, external or internal, that have significant potential for defeating the safety function. Input and output failures, improper recovery actions, electrical input voltage and frequency fluctuations, and maximum credible number of coincident signal changes have been included in the design vendors acceptance testing and the Appendix B suppliers Factory Acceptance Test (FAT). ALS MSFIS failures will not preclude the system from performing its safety function. System restart or reset will not result in the ALS MSFIS being inhibited from performing its safety function, and this will also be demonstrated in the FAT. Test functions, both continuous self test and test mode operation, will not affect the ability of the system to perform its specified safety function.

5.6 Independence

5.6.1 Between redundant portions of a safety system

Redundant portions of a safety system provided for a safety function shall be independent of, and physically separated from, each other to the degree necessary to retain the capability of accomplishing the safety function during and following any design basis event requiring that safety function.

Conclusion:

The ALS MSFIS will be installed in the existing Group 1 and Group 4 cabinets, maintaining the current

safety group separations. New switches installed on the Main Control Board (MCB) to control both trains include physical barriers which meet the requirements of IEEE Std 384-1992.

5.6.2 Between safety systems and effects of design basis event

Safety system equipment required to mitigate the consequences of a specific design basis event shall be independent of, and physically separated from, the effects of the design basis event to the degree necessary to retain the capability of meeting the requirements of this standard. Equipment qualification in accordance with 5.4 is one method that can be used to meet this requirement.

Conclusion:

The ALS MSFIS equipment has been seismically qualified by the 10 CFR 50 Appendix B supplier.

5.6.3 Between safety systems and other systems

The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in Clause 4, item h) of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.

Conclusion:

There are no changes from the existing design which currently meets this criteria.

5.6.3.1 Interconnected equipment

a) *Classification.* Equipment that is used for both safety and nonsafety functions shall be classified as part of the safety systems. Isolation devices used to effect a safety system boundary shall be classified as part of the safety system.

b) *Isolation.* No credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and following any design basis event requiring that safety function. A failure in an isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system.

Conclusion:

The only interconnection to non-safety related equipment is with the ALS Service Unit (ASU) used for test and maintenance. This connection is through a USB port. Any connections (ASU or any other device) made on this port are alarmed in the Control Room, and administrative controls prevent connection of the ASU unless the train is in a maintenance bypass. Functionally, the ASU is a "read-only" device; it cannot modify or control any of the ALS MSFIS functions.

5.6.3.2 Equipment in proximity

a) *Separation.* Equipment in other systems that is in physical proximity to safety system equipment, but that is neither an associated circuit nor another Class 1E circuit, shall be physically separated from the safety system equipment to the degree necessary to retain the safety systems' capability to accomplish their safety functions in the event of the failure of non-safety equipment. Physical separation may be achieved by physical barriers or acceptable separation distance. The separation of Class 1E equipment shall be in accordance with the requirements of IEEE Std 384-1992. (See [B1].)

b) *Barrier.* Physical barriers used to effect a safety system boundary shall meet the requirements of 5.3, 5.4 and 5.5 for the applicable conditions specified in Clause 4, items g) and h) of the design basis.

Conclusion:

There are no changes from the existing design which currently meets this criteria.

5.6.3.3 Effects of a single random failure

Where a single random failure in a nonsafety system can result in a design basis event, and also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure. See IEEE Std 379-1994 for the application of this requirement.

Conclusion:

There are no changes from the existing design which currently meets this criteria.

5.6.4 Detailed criteria

IEEE Std 384-1992 provides detailed criteria for the independence of Class 1E equipment and circuits [B1]. IEEE Std 7-4.3.2-1993 provides guidance on the application of this criteria for the separation and isolation of the data processing functions of interconnected computers.

Conclusion:

As described above, the IEEE Std 7-4.3.2-1993 requirements have been applied to the ASU service and test connection.

5.7 Capability for testing and calibration

Capability for testing and calibration of safety system equipment shall be provided while retaining the capa- bility of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practi- cable, performance of the safety function. Testing of Class 1E systems shall be in accordance with the requirements of IEEE Std 338-1987. Exceptions to testing and calibration during power operation are allowed where this capability cannot be provided without adversely affecting the safety or operability of the generating station. In this case:

— Appropriate justification shall be provided (e.g., demonstration that no practical design exists),
— Acceptable reliability of equipment operation shall be otherwise demonstrated, and
— The capability shall be provided while the generating station is shut down.

Conclusion:

The ALS MSFIS will include a maintenance bypass function for each main steam isolation valve (MSIV) and main feedwater isolation valve (MFIV). When a single train is in bypass, the other train will still have the capability to perform the MSFIS safety function. The ASU will provide complete visibility for a technician to diagnose faults to the board level and to recall operating history through the event recorder function.

5.8 Information displays

5.8.1 Displays for manually controlled actions

The display instrumentation provided for manually controlled actions for which no automatic control is provided and the display instrumentation required for the safety systems to accomplish their safety functions shall be part of the safety systems and shall meet the requirements of IEEE Std 497-1981 [B10]. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator.

Conclusion:

There are no changes from the existing design which currently meets this criteria.

5.8.2 System status indication

Display instrumentation shall provide accurate, complete, and timely information pertinent to safety system status. This information shall include indication and identification of protective actions of the sense and command features and execute features. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator. The display instrumentation provided for safety system status indication need not be part of the safety systems.

Conclusion:

The ALS MSFIS includes a "Summary Trouble Alarm" for each train on the MCB. This will activate on any system fault.

5.8.3 Indication of bypasses

If the protective actions of some part of a safety system have been bypassed or deliberately rendered inoper- ative for any purpose other than an operating bypass, continued indication of this fact for each affected safety group shall be provided in the control room.

a) This display instrumentation need not be part of the safety systems.

b) This indication shall be automatically actuated if the bypass or inoperative condition is expected to occur more frequently than once a year, and is expected to occur when the affected system is required to be operable.

c) The capability shall exist in the control room to manually activate this display indication.

Conclusion:

The ALS MSFIS includes a STATUS indicator for each train on the MCB. This will indicate if any valve is in bypass mode.

5.8.4 Location

Information displays shall be located accessible to the operator. Information displays provided for manually controlled protective actions shall be visible from the location of the controls used to affect the actions.

Conclusion:

The Summary Trouble Alarm and Status indicators are located on the MCB alarm and status panels in the same locations as for the existing system.

5.9 Control of access

The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.

Conclusion:

Physical access is controlled by plant security. Administrative controls limit access when the ASU is connected.

5.10 Repair

The safety systems shall be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.

Conclusion:

The ALS MSFIS contains extensive on-line, continuous self-test, failure detection and isolation and off-line diagnostic aids.

5.11 Identification

In order to provide assurance that the requirements given in this standard can be applied during the design, construction, maintenance, and operation of the plant, the following requirements shall be met:

a) Safety system equipment shall be distinctly identified for each redundant portion of a safety system in accordance with the requirements of IEEE Std 384-1992 and IEEE Std 420-1982.

No changes to existing safety group identification (cabinet nameplates and color-coded wiring).

b) Components or modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety system do not themselves require identification.

There are no changes from the existing design which currently meets this criteria.

c) Identification of safety system equipment shall be distinguishable from any identifying markings placed on equipment for other purposes (e.g., identification of fire protection equipment, phase identification of power cables).

There are no changes from the existing design which currently meets this criteria.

d) Identification of safety system equipment and its divisional assignment shall not require frequent use of reference material.

There are no changes from the existing design which currently meets this criteria.

e) The associated documentation shall be distinctly identified in accordance with the requirements of IEEE Std 494-1974 [B9].

There are no changes from the existing design which currently meets this criteria.

f) The versions of computer hardware, programs, and software shall be distinctly identified in accordance with IEEE Std 7-4.3.2-1993.

Each board in the ALS MSFIS includes a non-volatile memory device which is read by the FPGA and contains setpoint data and board identification information. The setpoint information can be read by the ASU. FPGA build information is created when the FPGA image is generated and is integral to the FPGA logic. This can be read from the Joint Test Action Group (JTAG) port associated with each FPGA.

Conclusion:

The ALS MSFIS meets the identification requirements of IEEE Std 603-1998.

5.12 Auxiliary features

Auxiliary supporting features shall meet all requirements of this standard.

Other auxiliary features that perform a function that is not required for the safety systems to accomplish their safety functions, and are part of the safety systems by association (i.e., not isolated from the safety system) shall be designed to meet those criteria necessary to ensure that these components, equipment, and systems do not degrade the safety systems below an acceptable level. Examples of these other auxiliary features are shown in Figure 3 and an illustration of the application of this criteria is contained in Annex A.

Conclusion:

As one element of the Engineered Safety Feature Actuation System (ESFAS), the ALS MSFIS does not contain any auxiliary features as defined here. The complete ALS MSFIS has been designed to meet this standard.

5.13 Multi-unit stations

The sharing of structures, systems, and components between units at multi-unit generating stations is per- missible provided that the ability to simultaneously perform required safety functions in all units is not impaired. Guidance on the sharing of electrical power systems between units is contained in IEEE Std 308-1991. Guidance on the application of the single failure criterion to shared systems is contained in IEEE Std 379-1994.

Conclusion:

WCGS is a single unit site and therefore this criteria is not applicable.

5.14 Human factors considerations

Human factors shall be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operator(s) and maintainer(s) can be successfully accomplished to meet the safety system design goals, in accordance with IEEE Std 1023-1988.

Conclusion:

Human factors considerations were a major design goal. All operator information is available on the front panels. Controls and indicators are clearly labeled and grouped, and show the state of the system for efficient evaluation of system status.

5.15 Reliability

For those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved. IEEE Std 352-1987 and IEEE Std 577-1976 provide guidance for reliability analysis. Guidance on the application of this criteria for safety system equipment employing digital computers and programs or firmware is found in IEEE Std 7-4.3.2-1993.

Conclusion:

The quantitative reliability goal established for the ALS MSFIS was to exceed the 2 year mean time between failure (MTBF) of the existing MSFIS equipment. An SRA was performed in accordance with IEEE Std 352-1987 and IEEE Std 577-1976. IEEE Std 7-4.3.2-1993 was not applied as the system does not contain software or firmware. The SRA is currently being updated to capture the final design, however the reliability goal has been far exceeded.

5.16 Common cause failure criteria

Plant parameters shall be maintained within acceptable limits established for each design basis event in the presence of a single common cause failure (See IEEE 379-1994). IEEE Std 7-4.3.2-1993 provides guidance on performing an engineering evaluation of software common cause failures, including use of manual action and non-safety-related systems, or components, or both, to provide means to accomplish the function that would otherwise be defeated by the common cause failure.

Conclusion:

The ALS MSFIS meets this criteria. Refer to the Diversity and Defense-in-Depth analysis.

6. Sense and command features—functional and design requirements

In addition to the functional and design requirements in Clause 5, the requirements listed in 6.1 through 6.8 shall apply to the sense and command features.

6.1 Automatic control

Means shall be provided to automatically initiate and control all protective actions except as justified in Clause 4,

item e). The safety system design shall be such that the operator is not required to take any action prior to the time and plant conditions specified in Clause 4, item e) following the onset of each design basis event. At the option of the safety system designer, means may be provided to automatically initiate and control those protective actions of Clause 4, item e).

Conclusion:

This requirement is not applicable to the extent that the MSFIS does not automatically initiate protective actions, however as an element of the ESFAS, the MSFIS provides automatic MSIV and MFIV closure, without operator intervention, when commanded via the ESFAS trip input.

6.2 Manual control

Means shall be provided in the control room to

a) Implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment consistent with the constraints of 5.6.1.

b) Implement manual initiation and control of the protective actions identified in Clause 4, item e) that have not been selected for automatic control under 6.1. The displays provided for these actions shall meet the requirements of 5.8.1.

c) Implement the manual actions necessary to maintain safe conditions after the protective actions are completed as specified in Clause 4, item j). The information provided to the operators, the actions required of these operators, and the quantity and location of associated displays and controls shall be appropriate for the time period within which the actions shall be accomplished and the number of available qualified operators. Such displays and controls shall be located in areas that are accessible, located in an environment suitable for the operator, and suitably arranged for operator surveillance and action.

Conclusion:

MCB MSFIS control functions are provided (essentially unchanged from the existing system) which meet this requirement.

6.3 Interaction between the sense and command features and other systems

6.3.1 Requirements

Where a single credible event, including all direct and consequential results of that event, can cause a non- safety system action that results in a condition requiring protective action, and can concurrently prevent the protective action in those sense and command feature channels designated to provide principal protection against the condition, one of the following requirements shall be met:

a) Alternate channels not subject to failure resulting from the same single event shall be provided to limit the consequences of this event to a value specified by the design basis. Alternate channels shall be selected from the following:

1) Channels that sense a set of variables different from the principal channels.

2) Channels that use equipment different from that of the principal channels to sense the same variable.
3) Channels that sense a set of variables different from those of the principal channels using equipment different from that of the principal channels.
4) Both the principal and alternate channels shall be part of the sense and command features.

b) Equipment not subject to failure caused by the same single credible event shall be provided to detect the event and limit the consequences to a value specified by the design bases. Such equipment is considered a part of the safety system. See Figure 5 for a decision chart for applying the requirements of this clause.

Conclusion:

No change from the existing system of two (2) trains of MSFIS.

6.3.2 Provisions

Provisions shall be included so that the requirements in 6.3.1 can be met in conjunction with the require- ments of 6.7 if a channel is in maintenance bypass. These provisions include reducing the required coinci- dence, defeating the non-safety system signals taken from the redundant channels, or initiating a protective action from the bypassed channel.

Conclusion:

No change from the existing system. Only one (1) train of MSFIS is required to close a valve.

6.4 Derivation of system inputs

To the extent feasible and practical, sense and command feature inputs shall be derived from signals that are direct measures of the desired variables as specified in the design basis.

Conclusion:

No change from the existing system. Each train of ALS MSFIS utilizes independent inputs from switches on the MCB and valve position instrumentation on the valve actuators.

6.5 Capability for testing and calibration

6.5.1 Checking the operational availability

Means shall be provided for checking, with a high degree of confidence, the operational availability of each sense and command feature input sensor required for a safety function during reactor operation. This may be accomplished in various ways; for example:

a) By perturbing the monitored variable,
b) Within the constraints of 6.6, by introducing and varying, as appropriate, a substitute input to the sensor of the same nature as the measured variable, or
c) By cross-checking between channels that bear a known relationship to each other and that have read- outs available.

Conclusion:

ALS MSFIS continuous self-test functions include all of the MSFIS inputs, and the existing manual system test capabilities are retained. This includes complete testing of the safety function, from the ESFAS input to the valve actuation outputs.

6.5.2 Assuring the operational availability

One of the following means shall be provided for assuring the operational availability of each sense and command feature required during the post-accident period:

a) Checking the operational availability of sensors by use of the methods described in 6.5.1.
b) Specifying equipment that is stable and the period of time it retains its calibration during the post- accident time period.

Conclusion:

ALS MSFIS provides continuous self-test features and extensive redundancy within each train. Failures are annunciated in the Control Room.

6.6 Operating bypasses

Whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall automatically accomplish one of the following actions:

a) Remove the appropriate active operating bypass(es).
b) Restore plant conditions so that permissive conditions once again exist.

c) Initiate the appropriate safety function(s).

Conclusion:

This requirement is not applicable. The ALS MSFIS does not include any operating bypass functions.

6.7 Maintenance bypass

Capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass. During such operation, the sense and command features should continue to meet the requirements of 5.1 and 6.3.

NOTE—For portions of the sense and command features that cannot meet the requirements of 5.1 and 6.3 when in main- tenance bypass, acceptable reliability of equipment operation shall be demonstrated (e.g., that the period allowed for removal from service for maintenance bypass is sufficiently short, or additional measures are taken, or both, to ensure there is no significant detrimental effect on overall sense and command feature availability).

Conclusion:

If one train of ALS MSFIS is in maintenance bypass, the other train retains the capability to perform the safety function. Administrative controls prevent both trains from being in bypass simultaneously.

6.8 Setpoints

The allowance for uncertainties between the process analytical limit documented in Clause 4, item d) and the device setpoint shall be determined using a documented methodology. Refer to ANSI/ISA S67.04-1994.

Where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions, the design shall provide positive means of ensuring that the more restrictive setpoint is used when required. The devices used to prevent improper use of less restrictive setpoints shall be part of the sense and command features.

Conclusion:

This requirement is not applicable to ALS MSFIS. There are no analog inputs or setpoints.

7. Execute features (functional and design requirements)

In addition to the functional and design requirements in Clause 5, the requirements listed in 7.1 through 7.5 shall apply to the execute features.

7.1 Automatic control

Capability shall be incorporated in the execute features to receive and act upon automatic control signals from the sense and command features consistent with Clause 4, item d) of the design basis.

Conclusion:

There are no changes from the existing design which currently meets this criteria.

7.2 Manual control

If manual control of any actuated component in the execute features is provided, the additional design features in the execute features necessary to accomplish such manual control shall not defeat the requirements of 5.1 and 6.2. Capability shall be provided in the execute features to receive and act upon manual control signals from the sense and command features consistent with the design basis.

Conclusion:

No change from the existing system. The ALS MSFIS inputs are prioritized in the logic, with the ESFAS/ALL CLOSE input having the highest priority.

7.3 Completion of protective action

The design of the execute features shall be such that, once initiated, the protective actions of the execute features shall go to completion. This requirement shall not preclude the use of equipment protective devices identified in Clause 4, item k) of the design basis or the provision for deliberate operator interventions. When the sense and command features reset, the execute features shall not automatically return to normal; they shall require separate, deliberate operator action to be returned to normal. After the initial protective action has gone to completion, the execute features may require manual control or automatic control (i.e., cycling) of specific equipment to maintain completion of the safety function.

Conclusion:

Following receipt of an ESFAS close signal, an MSIV or MFIV cannot be opened until the ESFAS signal is no longer present. This is consistent with the logic of the existing system.

7.4 Operating bypass

Whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall automatically accomplish one of the following actions:

a) Remove the appropriate active operating bypass(es).

b) Restore plant conditions so that permissive conditions once again exist.

c) Initiate the appropriate safety function(s).

Conclusion:

This requirement is not applicable. The ALS MSFIS does not include any operating bypass functions.

7.5 Maintenance bypass

The capability of a safety system to accomplish its safety function shall be retained while execute features equipment is in maintenance bypass. Portions of the execute features with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass (i.e., reducing temporarily its degree of redundancy to zero), the remaining portions provide acceptable reliability.

Conclusion:

If one train of ALS MSFIS is in maintenance bypass, the other train retains the capability to perform the safety function. Administrative controls prevent both trains from being in bypass simultaneously.

8. Power source requirements

8.1 Electrical power sources

Those portions of the Class 1E power system that are required to provide the power to the many facets of the safety system are governed by the criteria of this document and are a portion of the safety systems. Specific criteria unique to the Class 1E power systems are given in IEEE Std 308-1991.

Conclusion:

There are no changes from the existing design which currently meets this criteria.

8.2 Non-electrical power sources

Non-electrical power sources, such as control-air systems, bottled-gas systems, and hydraulic systems, required to provide the power to the safety systems are a portion of the safety systems and shall provide power consistent with the requirements of this standard. Specific criteria unique to non-electrical power sources are outside the scope of this standard and can be found in other standards.[11] [B4, B5]

Conclusion:

Non-electrical power sources are not utilized by this system and therefore, this requirement is not applicable.

8.3 Maintenance bypass

The capability of the safety systems to accomplish their safety functions shall be retained while power sources are in maintenance bypass. Portions of the power sources with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass (i.e., reducing temporarily its degree of redundancy to zero), the remaining portions provide acceptable reliability.

Conclusion:

If one train of the NK DC bus feeding the MSFIS is in a maintenance bypass, the other MSFIS train retains the capability to perform the safety function. Administrative controls prevent both trains from being in bypass simultaneously.

3 Mapping of IEEE Std 603-1998 to IEEE Std 7-4.3.2-2003 and DO-254

IEEE Std 603-1998 criteria	IEEE Std 7-4.3.2-2003 additional requirements	DO-254 requirements
4. Safety system design basis	Safety system design basis, Annex B	Hardware Safety Assessment 2.3
5. Safety system criteria	Annex B	Hardware Design Process 5.0, Appendix B
5.1 Single-failure criterion	None	Hardware Safety Assessment 2.3.1, Appendix B
5.2 Completion of protective action	None	None
5.3 Quality	Software development (5.3.1) Software tools (5.3.2) Verification and validation (5.3.3) Independent V&V (IV&V) requirements (5.3.4) Software configuration management (5.3.5) Software project risk management (see 5.3.6), Annex D and Annex F	Hardware Development - 3.0, 4.0, 5.0, V&V – 6.0, Config Mgmt – 7.0,\ Process Assurance – 8.0,
5.4 Equipment qualification	Testing software and diagnostics (see 5.4.1) Qualification of existing commercial computers (5.4.2), Annex C	Qualification of COTS components – 11.0
5.5 System integrity	Design for computer integrity (5.5.1) Design for test and calibration (5.5.2) Fault detection and self-diagnostics (5.5.3), Annex B and Annex C	Detailed Design Process 5.3.2
5.6 Independence	Independence (5.6), Annex E	Appendix A, Appendix B
5.7 Capability for test and calibration	None	Detailed Design Process 5.3.2
5.8 Information displays	None	None
5.9 Control of access	None	None
5.10 Repair	None	None
5.11 Identification	Identification (5.11)	None
5.12 Auxiliary features	None	None
5.13 Multi-unit stations	None	None
5.14 Human factor considerations	None	None
5.15 Reliability	Reliability (5.15) , Annex F	Hardware Safety Assessment 2.3.1, Conceptual Design 5.2.2,

IEEE Std 603-1998 criteria	IEEE Std 7-4.3.2-2003 additional requirements	DO-254 requirements
		V&V Analysis 6.3.2, Hardware Design Data 10.3.1, COTS Components 11.2.1
6. Sense and command feature—Functional design requirements	None	None
7. Execute feature—Functional design requirements	None	None
8. Power source requirements	None	None