NUCLEAR POWER PLANT DESIGN AND CONSTRUCTION CODES AND STANDARDS
(Emphasis on Codes and Standards used in the United States)

Presented to: Office of Atoms for Peace (OAP)

By: Advanced Systems Technology and Management (AdSTM)

Bangkok: November 18 - 22, 2019
MODULE 10

Instrumentation and Control, and Electrical Codes and Standards
U.S. NRC REGULATIONS

• Overall Requirements
  – GDC 2 - Design Bases for Protection Against Natural Phenomena
  – GDC 4 - Environmental and Dynamic Effects Design Bases
  – GDC 5 - Sharing of Structures, Systems, and Components
  – 10 CFR 50.49 “Environmental Qualification of Electrical Equipment Important to Safety for Nuclear Power Plants”

• Instrumentation and control
  – GDC 13
U.S. NRC Regulations

• Electrical Power Systems
  – GDC 17 - Electrical Systems
  – GDC 18 - Inspection and testing of electric power systems
  – 10 CFR 50.65 “Loss of all alternating current power”

• Reactor Protection Systems
  – GDC 20 - Protection system functions
  – GDC 21 - Protection system reliability and testability
  – GDC 22 - Protection system independence
  – GDC 23 - Protection system failure modes
  – GDC 24 - Separation of protection and control systems

• Protection Systems: IEEE 603-1991 required by 50.55a(h)(2)
U.S. NRC Regulations

• Safety Systems
  – IEEE 603-1991 required by 50.55a(h)(3)

• U.S. NRC Review Guidance (NUREG-0800, Standard Review Plan)
  – Chapter 7, Instrumentation and Control
  – Chapter 8, Electrical Systems

• NRC inspection procedures

• Standards and NRC regulations
ELECTRICAL AND I&C CODES

• Institute of Electrical and Electronics Engineers
ELECTRICAL AND I&C CODES

• Institute of Electrical and Electronics Engineers (cont’d)
  – IEEE-344 “IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations”
ELECTRICAL AND I&C CODES

- Institute of Electrical and Electronics Engineers (cont’d)
  - IEEE-765 “IEEE Standard for Preferred Power Supply (PPS) for Nuclear Power Generating Stations (NPGS)”
ELECTRICAL AND I&C CODES

• Institute of Electrical and Electronics Engineers (cont’d)
ELECTRICAL AND I&C CODES

• Instrument Society of America
  • ISA-67.04.01-1994, Setpoints for Nuclear Safety-Related Instrumentation

• Non-IEEE U.S. Standards
  • International Standard Organizations, i.e., International Electro-technical Commission (IEC), IAEA
IEEE-603 Introduction

  - This standard establishes minimum functional design criteria for the power, instrumentation, and control portions of nuclear power generating station safety systems.
  - The safety system criteria are established using a systems approach to the design of the power, instrumentation, and control portion of the safety system, as opposed to a specific engineering discipline approach (that is, electrical, mechanical, or civil).
IEEE-603 Introduction

  - The most important or basic standard which is incorporated by reference in NRC regulation and supplemented by numerous other IEEE Standards on more specific technical issues
IEEE-603 Scope

• Safety systems
  – A safety system is one that is relied upon to remain functional during and following design basis events to ensure:
    • the integrity of the reactor coolant pressure boundary,
    • the capability to shut down the reactor and maintain it in a safe shutdown condition, or
    • the capability to prevent or mitigate the consequences of accidents that could result in potential off-site exposures comparable to the 10 CFR Part 100 guidelines.
IEEE-603 Scope

Safety System

IEEE Std 603-1998

Mechanical Process to Sensor Coupling

Actuated Equipment to Mechanical Process Coupling

Instrumentation and Control, and Electrical Codes and Standards
IEEE-603

• Safety-related electrical systems are designated as Class 1E

  – Class 1E is the safety classification of the electric equipment and systems that are essential to emergency reactor shutdown, containment isolation, reactor core cooling, and containment and reactor heat removal, or are otherwise essential in preventing significant release of radioactive material to the environment.
## IEEE-603

<table>
<thead>
<tr>
<th>Sense and Command Features</th>
<th>Execute Features</th>
<th>Power Sources</th>
</tr>
</thead>
</table>
| Reactor Trip System And Engineered Safety Features | • Process sensors  
• Signal conditioning  
• Decision logic  
• Manual switches  
• Process controls  
• Indicators for operator actions  
• Limit switches  
• Control circuitry | • RTS trip breakers  
• ESF breakers  
• ESF motors, starters  
• ESF pumps  
• ESF motor operated valves, solenoid valves | (Power sources are considered auxiliary supporting features or other auxiliary features) |
| Auxiliary Supporting Features | • Room temperature sensors  
• Component temperature sensors  
• Pressure switches and regulators  
• Potential transformers  
• Under voltage relays  
• Diesel start logic  
• Diesel load sequencing logic  
• Limit switches  
• Control circuitry | • HVAC fans, filters  
• Lube pumps  
• Component cooling pumps  
• Breakers, starters  
• Diesel start solenoid  
• Crank motors | • Air compressors and receivers  
• Batteries  
• Diesel generators  
• Invertors  
• Transformers  
• Buswork  
• Distribution panels |
| Other Auxiliary Features | • Built in test equipment and circuitry  
• Bypass and rest circuitry  
• Electric protective relaying  
• Limit switches  
• Diesel over temperature and lube oil indicator | • Safety system isolation device  
• Breakers to nonessential loads | • Battery chargers  
• Transformers  
• Buswork  
• Distribution panels |
IEEE-603

• The standard does not directly address digital computer-based systems


• IEEE 7-4.3.2 will be discussed later
IEEE-603

• Safety criteria and design requirements

• The standard organizes its requirements into four groups:
  – Safety system criteria
  – Sense and command features
  – Execute features
  – Power sources
IEEE-603 Safety System Criteria

• Single Failure Criterion
  – The safety systems shall perform all safety functions required for a design basis event in the presence of
    • Any single detectable failure within the safety systems concurrent with all identifiable but nondetectable failures.
    • All failures caused by the single failure.
    • All failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions
IEEE-603
Safety System Criteria

• 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.

• Quality
  – Safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program
  – Appendix B to 10 CFR 50, ASME NQA-1, and IEEE 7-4.3.2 for software quality assurance
IEEE-603
Safety System Criteria

• Equipment Qualification
  – Safety system equipment shall be qualified to demonstrate being capable of meeting the performance requirements in the design basis, i.e., seismic qualification, environmental qualification.
  – IEEE Std 323, Qualifying Class 1E Equipment for Nuclear Power Generating Stations
  – IEEE Std 344, Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations
IEEE-603
Safety System Criteria (cont’d)

• Independence
  – Between redundant portions of a safety system
  – Between safety systems and effects of design basis event
  – Between safety systems and other systems
  – IEEE Std 384, Criteria for Independence of Class 1E Equipment and Circuits
IEEE-603
Safety System Criteria (cont’d)

• Capability for Test and Calibration
  – Capability for testing and calibrating safety system equipment shall be provided during power operation and shall duplicate, as practicable, performance of the safety function.

• Information Displays
  – Displays for manually controlled actions
  – System status indication
  – Indication of bypasses
IEEE-603
Safety System Criteria (cont’d)

• Control of Access
  – The design shall permit the administrative control of access to safety system equipment

• Human Factor Considerations
  – Ensure the human operators or maintainers can successfully accomplish the functions assigned to them in the design basis
IEEE-603
Sense and Command Features

• Sense and command features
  – The electrical and mechanical components and interconnections involved in generating those signals associated directly or indirectly with the safety functions.
  – The sense and command features extends from the measured process variables to the execute features’ input terminals.

• Automatic control
  – Means shall be provided to automatically initiate and control all protective actions, except justified otherwise.
IEEE-603
Sense and Command Features

• Manual control
  – Minimize the number of the operator actions and the number of equipment
  – Provide adequate and accessible information displays for manual operation

• 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
IEEE-603
Sense and Command Features

• Operating bypasses
  – Inhibition of the capability to accomplish a safety function that could otherwise occur in response to a particular set of generating conditions
  – Operating bypasses are used to permit mode changes (e.g., prevention of initiation of emergency core cooling during the cold shutdown mode).
  – 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).
IEEE-603
Sense and Command Features

• Maintenance bypasses
  – Removal of the capability of a channel, component, or piece of equipment to perform a protective action due to a requirement for replacement, repair, test, or calibration.
  – Capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass.

• Setpoints
  – The allowance for uncertainties between the process analytical limit and the device setpoint shall be determined using a documented methodology
IEEE-603
Execute Features

• Execute Features
  – The electrical and mechanical equipment and interconnections that perform a function, associated directly or indirectly with a safety function, upon receipt of a signal from the sense and command features.
  – The scope of the execute features extends from the sense and command features output to and including the actuated equipment-to-process coupling.

• 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 the design basis.
IEEE-603
Execute Features

• Manual control
  – Incorporate capability to receive and act upon manual control signals from the sense and command features consistent with the design basis

• Completion of protective action

• Operating bypasses

• Maintenance bypasses
IEEE-603
Power Source Requirements

• Electrical Power Sources
  – IEEE Std 308

• Nonelectrical Power Sources
  – Control air systems
  – Bottled gas systems
  – Hydraulic systems

• Maintenance bypasses
  – The capability of the safety systems to accomplish their safety functions shall be retained while power sources are in maintenance bypass
IEEE-603 Summary

• A basic and overarching IEEE std on the safety system, incorporated by reference in NRC regulations
• Scope – power, instrumentation and control circuitry portion of the safety systems
• Safety system criteria – introducing basic safety principles, i.e., single failure criterion, independence, equipment qualifications, quality assurance
• Additional design and functional requirements for the sense and command features, execute features, and power sources
IEEE 379

• Application of Single-Failure Criterion
  – Purpose and Scope
    • IEEE 603 requires safety systems meet the single failure criterion
    • IEEE 379 provides standards and guidance for establishing conformance with the single-failure criterion requirement
    • IEEE 379 applies to the power, instrumentation and control portions of the safety systems
    • Endorsed by RG 1.53
IEEE 379

• Single Failure Criterion
  – The safety systems shall perform all required safety functions for a design basis event in the presence of the following:
    • Any single detectable failure within the safety systems concurrent with all identifiable, but nondetectable failures.
    • All failures caused by the single failure (cascaded failures)
    • All failures and spurious system actions that cause, or are caused by, the design basis event requiring the safety function
IEEE 379

• Independence and Redundancy
  – The principle of independence is basic to the effective utilization of the single failure criterion

• Identifiable, but non detectable failures
  – Detectable failures: failures that can be identified through periodic testing or can be revealed by alarms or anomalous indication
  – Identifiable, but non detectable failures are those identified by analysis that cannot be detected
  – One objective of design analysis is to identify identifiable but non-detected failures
IEEE 379

• Cascaded Failures
  – Cascade failures are the additional failures caused or expected by from the occurrence of a single failure from any source (e.g., mechanical, electrical, and environmental)
  – Cascaded failures are considered to be a single failure

• Failures caused by design basis events
  – First of all, equipment should be designed, qualified and installed so as to prevent occurrence of such failures
  – If design analysis indicates failures in a safety system results from design basis events, these failures shall be considered as the consequence of the event
IEEE 379

• Design Analysis Procedure
  – Determine the safety function for analysis (e.g., reactivity control, containment, or reactor core heat removal)
  – Identify protection actions available to perform the safety function (e.g., reactor scram, containment isolation, core injection or spray)
  – Determine the safety groups that can meet the safety function
  – Verify the independence of the safety groups identified in the previous step
• Some Special Considerations in Single Failure Analysis
  – Interconnections between redundant channels (e.g., data loggers, test circuitry)
  – System logic
  – Auxiliary supporting features (i.e., instrument air, environmental control)
  – Sensing lines connecting sensors to process system should be included in single failure analysis
IEEE-384

• IEEE-384, “Standard Criteria for Independence of Class 1E Circuits”
  – This standard describes the independence requirements of the circuits and equipment comprising or associated with Class 1E systems.
  – Provides criteria for the independence that can be achieved by physical separation, and electrical isolation of circuits and equipment that are redundant.
  – Endorsed in RG 1.75 subject to several regulatory positions
IEEE-384

• Definitions
  – Independence: the state in which there is no mechanism by which any single design basis event, such as a flood, can cause redundant equipment to be inoperable.
  – Separation distance: Space that has no interposing structures, equipment, or materials that could aid in the propagation of fire or that could otherwise disable Class 1E systems or equipment
  – Safety class structures: Structures designed to protect Class 1E equipment against the effects of the design basis events
IEEE-384

• Definitions
  – Isolation device: A device in a circuit that prevents malfunctions in one section of a circuit from causing unacceptable influences in other sections of the circuit or other circuits.
IEEE-384

• Definitions
  – Associated circuits: Non-Class 1E circuits that are not physically separated or are not electrically isolated from Class 1E circuits by acceptable separation distance, safety class structures, barriers, or isolation devices.
    • Association by connection
    • Association by proximity
    • Association by shared signal source
IEEE-384

• General Independence Criteria
  – Physical separation and electrical isolation are required to maintain the independence of Class 1E circuits and equipment
  – Physical separation shall be achieved by the use of safety class structures, separation distance, or barriers or combination of them
  – Electrical isolation shall be achieved by the use of separation distance, isolation devices, shielding and wiring techniques or combination of them
  – The independence of Class 1E circuits and equipment shall not be compromised by the functional failure of auxiliary supporting features.
IEEE-384

• General Independence Criteria
  – Associated circuits subject to the requirements placed on Class 1E circuits; shall be uniquely identified as such, or as Class 1E
  – The independence of Non-Class 1E circuits from Class 1E and associated circuits are required
  – Class 1E circuits shall be routed or protected so that failure of the mechanical equipment of one division cannot disable Class 1E circuits or equipment essential to the performance of the safety function by the systems of the redundant division(s)
  – Failure of non safety class structures shall not affect the independence and redundancy of Class 1E systems
IEEE-384

• General Independence Criteria
  – Operation of the fire protection systems shall not compromise the independence of Class 1E equipment
  – An electrically generated fire in one Class 1E division shall not cause a loss of functions in its redundant Class 1E division.
  – The independence of redundant Class 1E circuits and equipment shall be such that a fire in a fire hazard area shall not prevent the capability to perform safety functions.
IEEE-384

• Specific Separation Criteria
  – Cables and Raceways
  – Equipment, i.e., standby generating units, DC system, distribution system, containment electrical penetrations, control switch boards
IEEE-384

• Specific Isolation Criteria
  – Power Circuits
    • Class 1E isolation devices shall be applied to interconnections between: Non-Class 1E and Class 1E circuits; associated circuits and non-Class 1E circuits
    • A device is considered to be a power circuit isolation device if it is applied such that the maximum credible voltage or current transient applied to the non-Class 1E side of the device will not degrade below an acceptable level the operation of the circuit on the other side of that device.
IEEE-384

• Specific Isolation Criteria
  – Instrumentation and Control Circuits

• Isolation required for connections between: Class 1E and Non-Class 1E circuits; associated circuits and non-Class 1E circuits; or Class 1E logic circuits of redundant divisions
IEEE-384 SUMMARY

• Maintain the independence of redundant Class 1E equipment and circuits by physical separation and electrical isolation
• Key definitions, i.e., independence, separation space, isolation devices, associated circuits
• General Independence Criteria for different elements, i.e., associated circuits, non-Class 1 circuits, effects of failure of mechanical systems or non safety class structures, operation of fire protection systems, a fire
• Specific Separation Criteria
• Specific Isolation Criteria
IEEE-323 Qualifying Class 1E Equipment for Nuclear Power Generating Stations

• Scope and Purpose
  – In the US, NRC regulations require Class 1E equipment be environmentally qualified to ensure the equipment can perform its safety function during and after a design basis accident
  – The primary objective of qualification is to demonstrate with reasonable assurance that Class 1E equipment can perform its safety function(s) without experiencing common cause failures before, during and after applicable design basis events
IEEE-323 Qualifying Class 1E Equipment for Nuclear Power Generating Stations

• Scope and Purpose
  – IEEE Std 323 is a general standard for qualification of all Class 1E equipment and provides basic qualification requirements, when met, demonstrate and document the ability of the equipment to perform its safety functions under applicable service conditions
  – IEEE 323-1974 endorsed by Reg Guide 1.89
• Qualified Life
  – Definition: The period of time, prior to the start of a design basis event, for which equipment was demonstrated to meet the design requirements for the specified service conditions.
  – The equipment shall be capable of performing the safety function(s) required for design basis events at the end of its qualified life.
  – Qualified life needs to be established for equipment with significant aging mechanisms based on specified service conditions.
  – Qualified life can be demonstrated by aging conditioning.
IEEE-323

• Aging Conditioning
  – The qualification program shall address effect of aging, evaluate their significance, and identify significant aging mechanisms if they exist
  – Significant aging mechanisms: wear and tear, oxidation, and loss of material strength
  – Aging conditioning is a process that replicates in a test sample the degradation of equipment over a period time due to significant aging mechanisms (e.g., thermal, radiation, wear, vibration)
IEEE-323

• Aging Conditioning
  – The intent is to put the test sample in the worst state of degradation that it would experience during the qualified life, prior to the design basis event
IEEE-323

• Margin
  – Margin shall be included in the qualification programs
  – Account for uncertainties in demonstrating satisfactory performance and normal variations in commercial production; uncertainties in measurement and test equipment
  – Margin can be added by increasing the severity of test parameter values, number of tests, or test duration, etc.
IEEE-323

- Principal Qualification Elements:
  - Equipment specification including definition of the safety functions
  - Acceptance criteria
  - Description of the service conditions, including design basis events and their duration
  - Qualification program plan
  - Implementation of the plan
  - Documentation of the result of a qualification program
• Qualification Methods
  – Type testing: subjects equipment to specified service conditions and demonstrates that such equipment can subsequently perform its intended safety function(s) for at least the required operating time.
  – Operational experience: Data from equipment of similar generic design that has successfully operated under known service conditions may be used as the basis for qualifying other equipment to equal or less severe service conditions.
  – Analysis: Requires a logical assessment or a valid mathematical model of the equipment to be qualified.
  – Combined Methods: Equipment may be qualified by any combination of the above three methods
IEEE-323 SUMMARY

• Purpose of Qualification
• Key concepts: qualified life, aging conditions, margin
• Principal qualification elements
• Qualification Methods
IEEE-344 Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations

• Scope and Purpose
  – The objective of the seismic qualification of the Class 1E equipment is to demonstrate that the equipment can meet its performance requirements during and/or following one Safety Shutdown Earthquake (SSE) event preceded by a number of Operating Basis Earthquake (OBE)
  – This Standard describes recommended practices for establishing seismic qualification procedures for Class 1E equipment
IEEE-344 Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations

• Scope and Purpose
  – Endorsed by REG 1.100 with clarifications and exceptions
• Safe Shutdown Earthquake (SSE)
  – An earthquake obtained from the site hazard analysis which evaluates the maximum earthquake potential of a site by considering the regional and local geology and seismology and the physical characteristic of local subsurface materials
  – The SSE is the maximum vibratory ground motion for which certain structures, systems, and components must be designed to remain functional.
IEEE-344

• Operating Basis Earthquake (OBE)
  – An earthquake could reasonably be expected to occur during the life time of the plant
  – The vibratory ground motion for which those features of the nuclear power plant necessary for continued operation without undue risk to the health and safety of the public will remain functional.
IEEE-344

• Qualification Methods
  – Predict the equipment’s performance by analysis.
  – Test the equipment under simulated seismic conditions.
  – Qualify the equipment by a combination of test and analysis.
  – Qualify the equipment through the use of experience data.
• Vibrational aging
  – The purpose of the vibrational aging is to show that the lower levels of normal and transient vibration, associated with plant operation and the lower intensity earthquake that has a higher probability of occurrence, will neither adversely affect an equipment’s performance of its safety function nor cause any condition to exist that, if undetected, would cause failure of such performance during a subsequent SSE.
  – Vibrational aging is required to be performed before the SSE and OBE tests
IEEE-344

• Seismic Aging
  – OBE tests are performed before the SSE tests
  – The number of OBEs shall be justified or shall include five OBEs

• Loading
  – Seismic qualification testing is performed at normal operating conditions (at load, at pressure)
IEEE-344

• Standard Scopes
• Methods of qualification
• Consideration of age-related effects
MODULE 12
IEEE AND ISA STANDARDS
IEEE-336 Installation, Inspection, and Testing Requirements for Power, Instrumentation, and Control Equipment at Nuclear Facilities

• Scope
  – Establish requirements for installation, inspection, and testing of power, instrumentation, and control equipment and systems (included in IEEE 603)
  – During construction phase of a nuclear facility
  – Also applicable to comparable major modifications

• Measures shall be established to verify conformance to specified requirements
IEEE-336

• Controlled plans, procedures, drawings, and documents

• Inspection and test results should be documented and evaluated

• Used with IEEE-603, NQA-1, and ANSI/ANS 3.2
IEEE-336

- Pre-installation Verifications
- Installation
- Verification During Installation
  - Inspections
  - Tests (electrical, physical and chemical, mechanical)
- Post-Installation Verification
  - Inspections
  - Equipment and system tests
- Data analysis and Evaluation
- Documentation and Records
IEEE-338 Criteria for Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems

• Scope
  – Provides design and operational criteria for periodic surveillance testing of safety systems to verify their ability to perform specified safety function(s)
    • Functional tests and checks
    • Calibration verification
    • Time response measurements
IEEE-338 Criteria for Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems

• Scope (cont’d)
  – Addresses system status, test interval, test procedures, and documentation
  – Does not cover maintenance
  – Amplifies the periodic surveillance testing requirements of IEEE-603 and IEEE-308
  – Endorsed in RG 1.118 with exceptions
IEEE-338

• Design Requirements:
  – Test provisions shall demonstrate the functional capability
  – Testable during NPP operation and while shut down
  – Testability shall permit the independent testing of redundant channels and load groups while:
    • maintaining the capability of these systems to respond to actual plant signals, or
    • tripping the output of the channel being tested, if required, or
    • bypassing the equipment consistent with safety requirements and limiting conditions for operation.
IEEE-338

• Periodic Test Program Requirements
  – Scope: functional tests, channel checks, calibration verification tests, response time tests, logic system functional tests
  – Establishes the extent and frequency of testing commensurate with plant safety concerns
IEEE-338

- Periodic Test Program Requirements (cont’d)
  - Accomplishes the objectives including procedures and documentations:
    - Facilitate administration and auditing
    - Identify high failure rates
    - Minimize interference with overall plant operation or compromise of safety
    - Ensure non-concurrent testing of redundant protection channels and load groups
    - Provide a master testing schedule
    - Identify systems, channels, and load groups to be tested
    - Provide tests that simulate the actual operating conditions
IEEE-338

• A functional test shall assure that the tested equipment is capable of performing its design function

• Example: manually starting equipment (for example, motor, pump, compressor, turbine, or engine) and observing proper operation (for example, pressure, flow, temperature, voltage, or speed). Test duration shall be sufficient to achieve stable operating conditions.
IEEE-338

• Response time testing shall be required only on safety systems or subsystems to verify that the response times are within the limits given in the Safety Analysis Report including Technical Specifications

• The response time test should include as much of each safety system, from sensor input to actuated equipment, as is practicable in a single test.
ISA-67.04.01-1994 Setpoints for Nuclear Safety-related Instrumentation

• Purpose and Scope
  – Develop a basis for establishing setpoints for nuclear safety-related instrumentation
  – Define requirements for assuring that setpoints for nuclear safety related instrumentation are established and maintained within specified limits in nuclear power plants and reactor facilities
  – Endorsed in Regulatory Guide 1.105 with exceptions and clarifications
ISA-67.04.01-1994

• Purpose and Scope
  – Nuclear safety-related instrumentation are those essential to the following:
    • Provide emergency reactor shutdown
    • Provide containment isolation
    • Provide reactor core cooling
    • Provide for containment or reactor heat removal
    • Prevent or mitigate a significant release of radioactive material to the environment or is otherwise essential to provide reasonable assurance that a nuclear power plant can be operated without undue risk to the health and safety of the public
• Safety Limit
  – A limit on an important process variable that is necessary to reasonably protect the integrity of physical barriers that guard against the uncontrolled release of radioactivity
  – Safety limits are defined in terms of directly measured process parameters (e.g., pressure, temperature) or calculated variables (e.g., Departure from Nucleate Boiling Ratio)

• Analytical Limit
  – Limit of a measured or calculated variable established by the safety analysis to ensure that a safety limit is not exceeded
  – Safety analysis also establish a specific time after the analytical limit is reached to begin protective actions
ISA-67.04.01-2011 defines Safety Limit as:

• “...a limit on an important process variable that is necessary to reasonably protect the integrity of physical barriers that guard against the uncontrolled release of radioactivity. (See 10 CFR, 50.36[c][1][i][A].)”
ISA-67.04.01-2011

10 CFR 50.36(c) “Technical specifications will include items in the following categories:

• (1) Safety limits, limiting safety system settings, and limiting control settings.
  – (i)(A) Safety limits for nuclear reactors are limits upon important process variables that are found to be necessary to reasonably protect the integrity of certain of the physical barriers that guard against the uncontrolled release of radioactivity. If any safety limit is exceeded, the reactor must be shut down.”
ISA-67.04.01-1994

• Trip Setpoint
  – A predetermined value for actuation of the final setpoint device to initiate a protective action
  – A Final setpoint device is a component, or assembly of components, that provides input to the process voting logic for actuated equipment
  – An allowance shall be provided between the trip setpoint and the analytical limit to ensure a trip before the analytical limit is reached
  – The allowance shall account for all applicable design basis events and process instrument uncertainties
ISA-67.04.01-1994

• Allowable Value
  – A limiting value that the trip setpoint may have when tested periodically, beyond which appropriate action shall be taken
  – The purpose of the allowable value is to identify a value that, if exceeded, may mean that the instrument has not performed within the assumptions of the setpoint calculation
  – A channel whose trip setpoint as-found condition exceeds the allowable value should be evaluated for operability, taking into account the setpoint calculation methodology
• Limiting Safety System Setting (LSSS)
  – Settings for automatic protective devices related to those variables having significant safety functions
  – Assure that protective action is initiated before the process conditions reach the analytical limit, thereby limiting the consequences of a design-basis event to those predicted by the safety analyses
  – Depending on the methodology, the LSSS may be the allowable value, the trip setpoint, or both
  – The LSSS is maintained by the technical specifications (Regulatory Guide 1.105)
Establishment of Setpoints

- Define safety limits (e.g., pressure, temperature, Departure from Nucleate Boiling Ratio)
- Safety analysis: establishing analytical limits
- Determine Limiting Safety System Setpoint, trip setpoints and allowable values accounting for process instrument uncertainties
- Combination of uncertainties
- Documentation of setpoint methods, calculations and instrument data
**ISA-67.04.01-2011**

- Safety limits (SL) are chosen to maintain the integrity of the physical barriers required to prevent the uncontrolled release of radioactivity.

- The analytical limit (AL) is the value of a given process variable at which the safety analysis models the initiation of the instrument channel protective action.

- Conservative ALs demonstrate that the established Safety Limits are not exceeded during normal plant transients, AOOs, and other design basis transients.

- Trip setpoints are chosen to assure that a trip or safety actuation occurs before the process variable reaches the AL.

- The limiting trip setpoint (LTSP) is the least conservative value of the nominal trip setpoint that still protects the AL.
ISA-67.04.01-2011

- Limiting Trip Setpoint = AL – Total Loop Uncertainty (TLU)

- Range of the Nominal Trip Setpoint = AL – TLU – Margin

- The value chosen for Margin is discretionary

- Range for operating transients is selected so the plant does not trip as a result of anticipated operational transients
ISA-67.04.01-2011

• Process variable chosen is Pressurized Water Reactor - Reactor Coolant System (RCS) pressure
  – Technical Specification RCS pressure Safety Limit \( \leq 2735 \) psig (10% > design)
  – RCS Design pressure = 2485 psig
  – Accident Analysis assumes RCS plant trip at 2405 psig = Analytical Limit
  – Technical Specification High Pressure Trip Setpoint \( \leq 2379 \) psig
  – Limiting Trip Setpoint = AL – Total Loop Uncertainty (TLU)
    Assume TLU = 52 psig
    \[ \text{LTSP} = 2405 \text{ psig} - 52 \text{ psig} = 2353 \text{ psig} \]
  – Nominal Trip Setpoint (NTSP) = AL – TLU – Margin (assume 26 psig)
    \[ \text{NTSP} = 2405 \text{ psig} - 52 \text{ psig} - 26 \text{ psig} = 2327 \text{ psig} \]
    NTSP range {<2353 psig (LTSP) to 2327 psig}
  – Normal operating pressure = 2235 psig
  – Range for operating transients < 92 psig
ISA-67.04.01-2011

Safety Limit = 2735 psig
Analytical Limit = 2405 psig

Limiting Trip Setpoint = 2353 psi

The range of Nominal Trip Setpoint is <2353 psig to 2327 psig

Range for Operating Transients is <2327 psig to 2235 psig

Normal Operation = 2235 psig
IEEE Std 7-4.3.2 Digital Computers in Safety Systems

• Purpose and Scope
  – IEEE 603 establishes minimum design and functional requirements for safety systems, including computer systems used in safety systems
  – This Standard supplies additional computer-specific provisions to several IEEE Std 603 requirements
  – Minimum functional and design requirements for computers in a safety system, including computer hardware, software, firmware, and interfaces
  – This standard is endorsed in RG 1.152 with exceptions and clarifications
IEEE 7-4.3.2

• Purpose and Scope (cont’d)
  – RG 1.152 Rev 3 (2011) endorses IEEE 7-4.3.2-2003 with exceptions and clarifications
    • Annex B-F are not endorsed
    • Clarify that software on a safety-related computer system that performs non-safety related functions must be classified as part of the safety system
    • Provide additional guidance on “access control” requirement, on which IEEE 7-4.3.2-2003 does provide guidance in addition to IEEE 603
IEEE 7-4.3.2

- Example nuclear safety related computer system is the Westinghouse Common Q system used for AP1000
- Functions performed include: Core Protection Calculator, Reactor Protection System, Plant Protection System, Post Accident Monitoring Systems, and Engineered Safety Features Actuation System
IEEE 7-4.3.2

• Safety system criteria

<table>
<thead>
<tr>
<th>IEEE 603-1998 Safety Criteria</th>
<th>IEEE 7-4.3.2-2003 Additional Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 Single failure criteria; 5.2 Completion of protection</td>
<td>None</td>
</tr>
<tr>
<td>5.3 Quality</td>
<td>Software development (5.3.1)</td>
</tr>
<tr>
<td></td>
<td>Software tools (5.3.2)</td>
</tr>
<tr>
<td></td>
<td>Verification and validation (V&amp;V) (5.3.3)</td>
</tr>
<tr>
<td></td>
<td>Independent V&amp;V (5.3.4)</td>
</tr>
<tr>
<td></td>
<td>Software configuration management (5.3.5)</td>
</tr>
<tr>
<td></td>
<td>Software project risk management (5.3.6)</td>
</tr>
<tr>
<td>5.4 Equipment qualification</td>
<td>Testing software and diagnostics (5.4.1)</td>
</tr>
<tr>
<td></td>
<td>Qualification of existing commercial computers (5.4.2)</td>
</tr>
<tr>
<td>5.5 System integrity</td>
<td>Design for computer integrity (5.5.1)</td>
</tr>
<tr>
<td></td>
<td>Design for test and calibration (5.5.2)</td>
</tr>
<tr>
<td></td>
<td>Fault detection and self-diagnostics (5.5.3)</td>
</tr>
<tr>
<td>5.6 Independence</td>
<td>5.6</td>
</tr>
<tr>
<td>5.11 Identification</td>
<td>5.11</td>
</tr>
<tr>
<td>5.15 Reliability</td>
<td>5.15</td>
</tr>
<tr>
<td>5.7 Capability for test and calibration; 5.8 Information display; 5.9 Control access; 5.10 Repair; 5.12 Auxiliary features; 5.13 Multi-unit stations; 5.14 human factor</td>
<td>None</td>
</tr>
</tbody>
</table>
IEEE 7-4.3.2

• Quality Assurance
  – Software quality assurance: IEEE std 12207-2008
  – Software quality metrics shall be considered through the software life cycle to assess whether the software quality requirements are met. (IEEE Std 1061-1998)
  – Software tools shall be subject to the same or higher quality life cycle process and/or the same V&V as the safety related software
  • Software tools: a computer program used in the design, development, testing, review, analysis, or maintenance of a program or its documentation.
• Quality Assurance
  – Verification and Validation (V&V)
    • Provide an objective assessment of software products and processes throughout the software life cycle.
    • This assessment demonstrates whether the software requirements and system requirements (i.e., those allocated to software) are correct, complete, accurate, consistent, and testable.
    • Performed in parallel with the software development, not at the conclusion of the software development
    • IEEE Std 1012 “Software V&V”
IEEE 7-4.3.2

• Quality Assurance
  – Independent Verification and Validation (IV&V) is required for safety related software
  – Software configuration management
    • Identification and control of all software designs and code
    • Identification and control of all software design functional data (e.g., data templates and data bases)
    • Identification and control of all software design interfaces
    • Control of all software design changes
IEEE 7-4.3.2

• Quality Assurance
  – Software configuration management (continued)
    • Control of software documentation (user, operating, and maintenance documentation)
    • Control of software vendor development activities for the supplied safety system software
    • Control and retrieval of qualification information associated with software designs and code
    • Software configuration audits
    • Status accounting
IEEE 7-4.3.2

• System Integrity
  – Design for computer integrity
    • Perform its safety function when subject to internal/external conditions having potential for defeating the safety function
    • Failure safe design
  – Design for test and calibration
    • The ability of the system to perform its safety function shall not adversely affected by test and calibration functions
  – Fault detection and self-diagnostic
IEEE-497 Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations

• Scope and Purpose
  — Provide functional and design criteria for accident monitoring instrumentation for nuclear power generating stations
  — Establishes selection, design, performance, qualification, and display criteria
IEEE-497 Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations

– Accident Monitoring Instrumentation are those necessary during the control room operations for
  • Planned operator action to mitigate accident
  • Assessment of plant conditions, safety system performance, and making decisions related to response to abnormal events
  • Achieving and maintaining shutdown following an accident

– References IEEE-603, IEEE-308, IEEE 7-4.3.2, NQA-1, etc.

– Endorsed by NRC Regulatory Guide 1.97
IEEE-497

• Selection of Plant-Specific Variables for Accident Monitoring
  – Type A variables: those providing primary information necessary for planned manually controlled actions
  – Type B variables: provide primary information to control room operators to assess the plant safety functions (reactivity control, core cooling, RCS integrity, containment integrity)
IEEE-497

• Selection of Plant-Specific Variables for Accident Monitoring
  – Type C variables: provide primary information to the control room operators to indicate the potential for breach or the actual breach of fission product barriers (e.g., fuel cladding, reactor coolant system pressure boundary, and containment pressure boundary)
  – Type D variables: provide primary information required in the plant’s procedures and licensing basis documentation (LBD) to indicate the performance of safety systems, required auxiliary support systems, safe shutdown systems, verify safety system status
IEEE-497

• Selection of Plant-Specific Variables for Accident Monitoring
  – Type E variables: provide primary information required for use in determining the magnitude of the release of radioactive materials and to continually assessing such releases.
  – Documentation shall be developed and maintained for the selection of the accident monitoring variables consistent with the plant’s licensing basis.
IEEE-497

• Performance criteria
  – Range
  – Accuracy
  – Response time
  – Required operating time
  – Reliability
  – Documentation of performance criteria
IEEE-497

• Design criteria
  – Single failure (Types A, B & C)
  – Common cause failure (Types A, B & C)
  – Independence and separation (Types A, B & C)
  – Isolation (Types A, B & C)
  – Information ambiguity: the failure of an accident monitoring instrument channel shall not result in information ambiguity that could lead the operator to defeat or fail to accomplish a required safety function (Types A, B & C)
IEEE-497

- Design criteria (cont’d)
  - Power supplies: Class 1E (Types A, B & C)
  - Calibration
  - Testability
  - Direct measurement
  - Maintenance and repair
  - Portable Instruments
IEEE-497

• Qualification criteria
  – Type A variables (seismic: IEEE-344, EQ: IEEE-323)
  – Type B variables (seismic: IEEE-344, EQ: IEEE-323)
  – Type C variables (seismic: IEEE-344, EQ: IEEE-323)
  – Type D variables (seismic: IEEE-344, EQ: IEEE-323)
  – Type E variables (not seismically or environmentally qualified)
  – Portable equipment (not seismically or environmentally qualified)
  – Operating time (for the time the function is required)
  – Documentation of qualification criteria
IEEE-497

• Display criteria
  – Display characteristics
  – Human factors
  – Anomalous indications
  – Continuous vs. on-demand display

• Trend or rate information
• Display identification
• Display location
• Quality Assurance
• Accident monitoring instrumentation for Type A, Type B, and Type C variables shall be designed, manufactured, inspected, installed, operated, and maintained in accordance with ASME NQA-1-2008.
• The level of quality assurance to be applied to accident monitoring instrumentation for Type D and Type E variables shall be selected and documented by the designer to meet the specified performance requirements.
### Table 7.5-2 PAM Main Design Criteria for Each Variable Type

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Type</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Single Failure</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>2. Seismic Qualification</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>3. Environmental Qualification</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>4. Power Supply</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>If required</td>
<td>if required</td>
</tr>
<tr>
<td>5. QA</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6. Independence and Separation</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>7. Information Ambiguity</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>8. Testability</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9. Continuous Display</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>10. Recording</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Note: Yes means it is required.
MODULE 13
IEEE STANDARDS

—Scope

• Class 1E portions of AC and DC power systems
• Instrumentation and Control power systems
• Single and multi-unit stations

— Purpose
  • Provides:
    — Design criteria and features for Class 1E power system,
    — Testing and surveillance requirements for the Class 1E power systems,
    — Criteria for sharing Class 1E power systems in multi-unit stations
    — References IEEE-603 and many other IEEE standards
    — Endorsed in RG 1.32 (except no sharing of dc power systems)
IEEE-308

• Definitions
  – **Division**: The designation applied to a given system or set of components that enables the establishment and maintenance of physical, electrical, and functional independence from other redundant sets of components.
  – **Engineered safety features**: Features of a unit, other than reactor trip or features used only for normal operation, that are provided to prevent, limit, or mitigate the release of radioactive material.
IEEE-308

SWITCHYARD AND TRANSMISSION SYSTEM
(NOT WITHIN SCOPE)

STANDBY GENERATOR

LIA and LIB
LIAa and LIAd
LIBa and LIBd

REDUNDANT LOADS
APPURTEINANCES OF LIA
APPURTEINANCES OF LIB

a = AC LOADS
d = DC LOADS
IEEE-308

• Principal Design Criteria
  – The Class 1E power systems shall be designed to assure that no design basis event causes the following:
    • A loss of electric power to a number of engineered safety features, surveillance devices, or protection system devices so that a required safety function cannot be performed.
    • A loss of electric power to equipment that could result in a reactor transient capable of causing significant damage to the fuel cladding or to the reactor coolant pressure boundary.
    • The required portions of the Class 1E power systems shall be capable of performing their function when subjected to the effects of any design basis event.
IEEE-308

• Principal Design Criteria (cont’d)
  – The variations of voltage, frequency, and waveform (including the effects of harmonic distortion) in the Class 1E power systems during any mode of plant operation shall not degrade the performance of any safety system load below an acceptable level.
  – Independence of redundant equipment and circuits (IEEE-384)
  – Equipment Qualification (IEEE-323)
  – Class 1E power systems must meet single failure criterion (IEEE-379)
IEEE-308

• Supplementary Design Criteria
  – The Class 1E power systems shall support the safety systems by providing acceptable power under the conditions stated in the design basis.
  – Alternating Current Power Systems
    • Distribution System
    • Preferred Power Supply
    • Standby Power Supply
  – Direct Current Power Systems
    • Distribution System
    • Battery Supply
    • Battery Charger
  – Instrumentation and Control Power Systems
  – Execute Features
  – Sense and Command Features
IEEE-308

• Surveillance and Test Requirements
  – Operational status information shall be provided for Class 1E power systems by the following:
    • Instrumentation
    • Indicator lights or annunciators
    • Plant computer
  – Preoperational tests (IEEE-415)
    • Demonstrate that the equipment operates within design limits and that the system is operational and can meet its performance specification.
IEEE-308

• Surveillance and Test Requirements (cont’d)
  – Periodic Testing (IEEE-338)
    • Detect within practical limits the deterioration of the equipment toward an unacceptable condition.
    • Demonstrate that standby power equipment and other components that are not exercised during normal operation of the station are operable.
  • Multi-unit Station Considerations
    – Standby Power Supply Capacity
    – Battery Supply
IEEE-308 SUMMARY

- Scope
- Principal Design Criteria
- Supplementary Design Criteria
- Surveillance and Testing Requirements
- Multi-unit Station Considerations
IEEE-741 Criteria for the Protection of Class 1E Power Systems and Equipment in Nuclear Power Generating Stations

• Scope
  – Establishes protection requirements for Class 1E power systems and equipment
    • Protection from mechanical and electrical damage or failures
    • Includes preoperational testing and surveillance requirements
  – It does not include plant physical protection requirements against events such as pipe whip, fire, dropped load, etc
  – RG 1.63 states that the external circuit protection of electric penetration assemblies should meet IEEE-741
IEEE-741

• General design criteria
  – Prevent disabling safety functions below an acceptable level
  – Operating protective devices on detection of an unacceptable condition
  – Monitoring/transferring preferred power supplies
  – Indicate and identify protective operation
  – Periodic testing to verify logic and protective function
  – Designed to monitor availability of protection control power
  – Periodic testing to verify set points
IEEE-741

• Principal design criteria and requirements
  – AC power distribution systems
  – DC power systems
  – Instrumentation and control power systems
  – Primary containment electrical penetration assemblies
  – Valve actuator motors (direct gear driven)

• Testing and surveillance
  – Preoperational tests
  – Surveillance
IEEE-741, Annexes

A. Degraded voltage protection
B. Guidelines for selection of overload protection for valve actuator motor circuits
C. Auxiliary system automatic bus transfer – protection concerns
D. Use of high-speed magnetic circuit breakers for special application
IEEE-765 Preferred Power Supply (PPS) for Nuclear Power Generating Stations (NPGS)

• **Scope**
  – Provides design criteria of the preferred power supply (PPS) and its interfaces with the Class 1E power system, switchyard, transmission system, and alternate ac (AAC) source.

• **Purpose**
  – Provides PPS requirements for nuclear power generating stations (NPGSs) and guidance in the areas of AAC power source interfaces with the PPS, physical independence of the PPS power and control circuits, and expanded PPS criteria for multi-unit stations.

• **References**  IEEE-308, IEEE-741, and IEEE-1792
IEEE-765, Definitions

Preferred power supply (PPS): The power supply from the transmission system to the Class 1E distribution system that is preferred to furnish electric power under accident and post-accident conditions.

Station blackout: The complete loss of ac electric power to the essential and nonessential switchgear buses in an NPGS (i.e., loss of the PPS concurrent with turbine trip and unavailability of the onsite emergency ac power system). Station blackout does not include the loss of available ac power to buses fed by station batteries through inverters or by AACs.
TYPICAL PLANT ONSITE A/C DISTRIBUTION SYSTEM
IEEE-765, Definitions

• Alternate ac (AAC) source: An alternating current (ac) power source that is available to and located at or nearby a NPGS that meets the following requirements:
  a) It may be connected to the PPS or the onsite emergency ac power system.
  b) It has minimum potential for common-mode failure with PPS or onsite emergency ac power sources.
  c) It is available in a timely manner after the onset of a station blackout.
IEEE-765, Definitions

d) It has sufficient capacity and reliability to operate all systems required for the following:
1) Coping with a station blackout
2) The time needed to bring the plant to and maintain it in a safe shutdown condition (non-design basis accident)
IEEE-765

• General design criteria
  – The PPS shall consist of two or more circuits from the transmission system to the Class 1E distribution system.
  – The PPS is not a Class 1E system.
  – Provides electric power for safety systems and safe shutdown
  – Each circuit shall have sufficient capacity and capability to power the equipment required for design events
  – Availability
    • A minimum of two circuits shall be available
    • At least one should be available automatically to provide power to the Class 1E buses within a few seconds following a design basis accident
IEEE-765

• General design criteria
  – Independence

• The PPS circuits shall be physically independent

• The PPS control circuits shall be physically independent from each other and PPS power circuit
IEEE-765

• General design criteria
  – Design basis
    • Station electric loads and systems serviced
    • Environmental conditions, i.e., wind, lightning, ice
    • Station DBEs and operating incidents that may cause degradation of the PPS
    • Degree of independence and redundancy within the PPS
    • Interfaces of the PPS with the switchyard, Class 1E systems, AAC power source
    • Capability of periodic testing
    • Restoration methodology for realignment of the PPS following the loss of power, etc
IEEE-765

- Interface Requirements
  - Transmission system interface
    - Determine transmission system reliability
    - Design the two transmission lines to minimize their simultaneous loss
    - Conduct transmission system studies
  - Switchyard interface
    - Minimize the probability of a single incident of equipment causing loss of both PPS circuits
    - Provide protection systems to minimize the probability of loss of the PPS
IEEE-765

• Interface Requirements
  – Class 1E power system interface
    • Each circuit may be utilized to supply both Class 1E buses
    • The connection between the PPS and Class 1E circuit breaker shall be made at the input terminals of the Class 1E circuit breaker
    • Adequacy of the transfer scheme shall be demonstrated if automatic bus transfers are used
    • PPS Voltage degradation shall be detectable at the Class 1E bus to which the PPS source is connected, alarmed in the control room, and automatically disconnected from the Class 1E buses
IEEE-765

• Interface Requirements
  – AAC source interface
    • Be maintained electrically open
    • Avoid vulnerability to a likely weather related event or a single failure rendering both the AAC power source and the PPS inoperable
IEEE-765

• Surveillance, control, and test requirements
  – Surveillance
    • Status indication (open-close) of PPS circuit interrupting devices shall be provided in the main control room (MCR)
    • Undervoltage alarms provided in the MCR
    • Voltage degradation alarms provided in the MCR
  – Control of all circuit-interrupting devices shall be provided in the main control room
  – Tests: pre-operational tests, periodic equip/systems tests

• This standard describes the criteria for the application and testing of diesel-generator units as Class 1E standby power supplies in nuclear power generating stations.
IEEE-387

• It provides the principal design criteria, the design features, testing, and qualification requirements for the individual diesel-generator units that enable them to meet their functional requirements as a part of the standby power supply under the conditions produced by the design basis events cataloged in the Plant Safety Analysis.

• Endorsed by RG 1.9, “Application and Testing of Safety-Related Diesel Generators in Nuclear Power Plants “
IEEE-387, EDG
NON-IEEE STANDARDS

Generally applicable to non-safety-related electrical and I&C equipment

• American National Standards Institute
• Association of Electrical and Medical Imaging Manufacturers (NEMA)
• Underwriters Laboratory (UL)
• Insulated Cable Engineers Association (ICEA)
• American Institute for Steel Construction (AISC)
• U.S. Armed Forces (MIL SPEC)

<table>
<thead>
<tr>
<th>Transformers</th>
<th>Battery racks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switchgear</td>
<td>Battery chargers</td>
</tr>
<tr>
<td>Motor Control Centers</td>
<td>Inverters</td>
</tr>
<tr>
<td>Motors and generators</td>
<td>Uninterruptable power supplies</td>
</tr>
<tr>
<td>Cables</td>
<td>Static transfer switches</td>
</tr>
<tr>
<td>Bus ducts and ways</td>
<td>Adjustable speed drives</td>
</tr>
</tbody>
</table>