IEEE Std 603-1991, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations

4.5 The protective actions identified in 4.2 that ***may be controlled by manual means initially or subsequently to initiation. See IEEE Std 497-1981***.[1] The proactive actions are as follows:

4.5.1 The points in time and the plant conditions during which manual control is allowed.

4.5.2 The justification for permitting initiation or control subsequent to initiation solely by manual means.

4.5.3 The range of environmental conditions imposed upon the operator during normal, abnormal, and accident conditions throughout which the manual operations shall be performed.

4.5.4 The variables in item 4.4 that shall be displayed for the operator to use in taking manual action.

This section links to the RG 1.97 Type A analysis for providing selected manual control of primary success path actions for design basis accidents.

6.2 Manual Control

6.2.1 Means shall be provided in the control room to 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.

Division level control is specified, along with group in of signals to minimize operator tasks.

Back to the RG 1.97 analysis.

6.2.2 Means shall be provided in the control room to implement ***manual initiation and control of the protective actions identified in 4.5 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.

6.2.3 Means shall be provided to implement the ***manual actions necessary to maintain safe conditions after the protective actions are completed*** as specified in 4.10. 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.

Manual actions to achieve post event safe shutdown.

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.***

Manual control signals (non-safety) are allowed if there is no adverse impacts.

The RG 1.97 Type A leads to certain required manual controls that must be safety-related to support the design basis. Other non-safety manual controls may be included for backup capability.

[1] Note that IEEE 603-1998 corrects the reference to IEEE Std 497-1981, IEEE Standard Criteria Nuclear Power Generating Stations endorsed by. Regulatory Guide 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants.

Regulatory Guide 1.62, Manual Initiation of Protective Actions

Only system level manual capability is specified here.

C. Regulatory Position

1. Means should be provided for manual initiation of each protective action (e.g., reactor trip, containment isolation) ***at the system level***, regardless of whether means are also provided to initiate the protective action at the component or channel level (e.g., individual control rod, individual isolation valve).

2. Manual initiation of a protective action ***at the system level*** should perform all actions performed by automatic initiation such as starting auxiliary or supporting systems, sending signals to appropriate valve-actuating mechanisms to assure correct valve position, and providing the required action-sequencing functions and interlocks.

3. The switches for manual initiation of protective actions ***at the system level*** should be located in the control room and be easily accessible to the operator so that action can be taken in an expeditious manner.

Regulatory Guide 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants

Criteria for limited set of safety-related component level manual controls.

Type A Variables - Selection Criteria

Type A variables are those variables that provide the primary information required to permit the control room operating staff to:

a) Take specific planned manually-controlled actions for which no automatic control is provided and that are required for safety systems to perform their safety-related functions as assumed in the plant Accident Analysis Licensing Basis.
b) Take specific planned manually-controlled actions for which no automatic control is provided and that are required to mitigate the consequences of an AOO.

Type A variables provide information essential for the ***direct accomplishment of specific safety-related functions that require manual action***. These variables are ***a subset of those necessary to implement the plant specific emergency procedure guidelines*** (EPGs) or the plant specific emergency operating procedures (EOPs) or the plant abnormal operating procedures (AOPs).”

NRC Standard Review Plan

Appendix 7.1-A Acceptance Criteria and Guidelines for Instrumentation and Control Systems Important to Safety

(f) 10 CFR 50.34(f)(2)(xii): Addressing [TMI Action Plan Item II.E.1.2] Auxiliary Feedwater

"Provide automatic and ***manual auxiliary feedwater (AFW) system initiation***, and provide auxiliary feedwater system flow indication in the control room. (Applicable to PWRs only)." System level

(h) 10 CFR 50.34(f)(2)(xviii): Addressing [TMI Action Plan Item II.F.2] Instrumentation for the Detection of Inadequate Core Cooling

"Provide instruments that provide in the control room an unambiguous indication of inadequate core cooling, such as primary coolant saturation meters in PWRs, and a suitable combination of signals from indicators of coolant level in the reactor vessel and in-core thermocouples in PWRs and BWRs."

Review Methods - Instrumentation for the detection of inadequate core cooling should be included in the information systems important to safety and reviewed in accordance with the review guidance provided in SRP Section 7.5. Inadequate core cooling instrumentation should provide unambiguous indication of these conditions. It should provide the operator with sufficient ***information during accident situations to take planned manual actions***, and to determine whether safety systems are operating properly. RG 1.97 Type A

(j) 10 CFR 50.34(f)(2)(xix): Addressing [TMI Action Plan Item II.F.3] Instruments for Monitoring Plant Conditions Following Core Damage

"Provide instrumentation adequate for monitoring plant conditions following an accident that includes core damage."

Review Methods - Instrumentation for monitoring plant conditions following core damage should be included in the information systems important to safety. There should be instrumentation of sufficient quantity, range, availability, and reliability to permit adequate monitoring of plant variables and systems during and after an accident. Sufficient information should be provided to the operator for (1) ***taking planned manual actions to shut the plant down safely***; (2) determining whether the reactor trip, ESF systems, and manually initiated safety-related systems are performing their intended safety functions (i.e., reactivity control, core cooling, and maintaining reactor containment system and containment integrity); and (3) determining the potential for causing a gross breach of the barriers to radioactivity release (i.e., fuel cladding).

(e) GDC 13, "Instrumentation and Control"

"Instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those

variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges."

Review Methods - Review of compliance with GDC 13 should include consideration of the following topics.

- Instrumentation to monitor plant variables and systems - See SRP Sections 7.5 and 7.7.
- Instrumentation to monitor the status of protection systems - See SRP Appendix 7.1-B Subsections 4.9, 4.13, 4.19, or SRP Appendix 7.1-C Subsections 5.8 and 6.5.
- ***I&C for manual initiation of safety functions*** - See SRP Appendix 7.1-B Subsections 4.17 and 4.19, or SRP Appendix 7.1-C Subsections 5.8, 6.2, and 7.2.

References point to IEEE 603 for digital.

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

Diverse manual control is specified at system level.

The display and control features should be designed to satisfy existing regulations, for example, separation and independence requirements for Class 1E circuits (IEEE Std. 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits"); criteria for protection systems (IEEE Std. 279-1971); and specifications for ***manual initiation of protective actions at the systems level*** (Regulatory Guide 1.62, "Manual Initiation of Protection Action").

Safety related manual control is specified at system level.

Appendix 7.1-C Guidance for Evaluation of Conformance to IEEE Std. 603

Clause 4.5 of IEEE Std. 603-1991 describes the ***minimum criteria under which manual initiation and control of protective actions may be allowed***.

RG 1.97 Type A

Failure of computer system hardware or software ***should not inhibit manual initiation of protective functions or the operator performance of preplanned emergency or recovery actions***.

Sets fault tolerance capability for single failures of safety-related equipment and inclusion of DAS for digital common mode failures.

6.2 Manual Control (IEEE Std. 603-1991 Clause 6.2)

Features for ***manual initiation of protective action should conform with Regulatory Guide 1.62***, "Manual Initiation of Protection Action." The review of manual controls should be coordinated with the organization responsible for reviewing human factors to confirm that the functions controlled and the characteristics of the controls (e.g., location, range, type, and resolution) allow plant operators to take appropriate manual actions. The review of manual controls should include confirmation that the controls will be functional (e.g., power will be available and command equipment is appropriately qualified), accessible within the time constraints of operator responses, and available during plant conditions under which manual actions may be necessary.

System level

7.2 Manual Control (IEEE Std. 603-1991 Clause 7.2)

Features for ***manual initiation of protective action should conform with Regulatory Guide 1.62***, "Manual Initiation of Protection Action." The review of manual controls should be coordinated with the organization responsible for reviewing human factors to confirm that the functions controlled and the characteristics of the controls (e.g., location, range, type, and resolution) allow plant operators to take appropriate manual actions. The review of manual controls should include confirmation that the controls will be functional (e.g., power will be available and command equipment is appropriately qualified), and accessible within the time required of the operator during plant conditions under which manual actions may be necessary.

System level

Section 7.2, Reactor Trip System

E. Diversity and defense-in-depth - RTSs should incorporate multiple means for responding to each event discussed in the SAR Chapter 15, "Transient and Accident Analyses." At least one pair of these means for each event should have the property of signal diversity, i.e., the use of different sensed parameters to initiate protective action, in which any of the parameters may independently indicate an abnormal condition, even if the other parameters are sensed incorrectly (see NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems"). The diverse means may actuate the same protective function or different protective functions, and may be automatically or manually activated, consistent with the response time requirements of the function. For digital computer-based RTSs, the applicant/licensee should have performed a defense-in-depth and diversity analysis. Additionally, for advanced reactor design under 10 CFR Part 52, the design should provide for ***manual, system-level actuation of critical safety functions***. SRP BTP 7-19 provides guidance for the review of diversity and defense-in-depth.

Diverse manual control is specified at system level.

Appropriate controls are provided for ***manual initiation of reactor trip***.

Section 7.3, Engineered Safety Features Systems

Appropriate controls are provided for ***manual initiation and control of ESF functions***.

Section 7.4, Safe Shutdown Systems

Plant designs should provide for control in locations removed from the main control room that may be used for ***manual control and alignment of safe shutdown system equipment needed to achieve and maintain hot and cold shutdown***.

Requirements for remote shutdown station.

Section 7.5, Information Systems Important to Safety

Compliance with IEEE Std. 603-1991 - Alarms that are provided for ***manually controlled actions for which no automatic control is provided and that are***

RG 1.97 Type A

required for the safety systems to accomplish their safety functions should be reviewed against the requirements of IEEE Std. 603-1991.

Section 7.7, Control Systems

Relevant to discussion of non-safety VDUs.

Effects of control system failures - The review should confirm that the ***failure of any control system component or any auxiliary supporting system for control systems does not cause plant conditions more severe than those described in the analysis of anticipated operational occurrences*** in Chapter 15 of the SAR. This evaluation should address failure modes that can be associated with digital systems such as software design errors as well as random hardware failures. (The ***evaluation of multiple independent failures is not intended***.)

Use of digital systems - To minimize the potential for control system failures that could challenge safety systems, control system software should be developed using a structured process similar to that applied to safety system software. Elements of the review process may be ***tailored to account for the lower safety significance of control system software***.

Potential for inadvertent actuation - The control systems design should ***limit the potential for inadvertent actuation*** and challenges to safety systems.

The staff review determines that the control systems are ***appropriately isolated from safety systems and would preserve the reliability, redundancy, and independence*** requirements of the protection system.

The conclusions of the analysis of anticipated operational occurrences and accidents as presented in Chapter 15 of the SAR have been used to confirm that ***plant safety is not dependent upon the response of the control systems***. The staff also confirmed that failure of the control systems themselves or as a consequence of supporting system failures, such as loss of power sources, does not result in plant conditions more severe than those described in the analysis of design basis accidents and anticipated operational occurrences.

Non-safety manual controls cannot be used for the primary success path ...

However, the guidance anticipates that non-safety controls exist and can be used for AOOs.

The staff review of control systems considered the features of these systems for both manual and automatic control of the process systems. The staff finds that the features for manual and automatic control facilitate the capability to maintain plant variables within prescribed operating limits. The staff finds that the ***control systems permit actions to be taken to operate the plant safely*** during normal operation, ***including anticipated operational occurrences***, and, therefore, the control systems satisfy the requirements of GDC 19 with regard to normal plant operations.

Section 7.8, Diverse Instrumentation And Control Systems

Diverse manual controls and displays that are provided to comply with the NRC position on D3 as described in the Staff Requirements Memorandum (SRM) regarding SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs.” These systems are to be independent and diverse from the associated digital safety systems(s). The associated operator interfaces

(controls and displays) must be located in the main control room. They are to provide ***manual, system-level actuation*** of critical safety functions and monitoring of parameters that support the safety functions.

Manual initiation capability - The ATWS mitigation systems and DAS should include the capability for initiation from the control room.

Branch Technical Position 7-19, Guidance for Evaluation of Diversity and Defense-In-Depth In Digital Computer-Based Instrumentation and Control Systems

Point 4 A set of displays and controls located in the main control room should be provided for ***manual system-level actuation*** of critical safety functions and for monitoring of parameters that support safety functions. The displays and controls should be independent and diverse from the computer-based safety systems identified in Points 1 and 3.

The diverse means may be an automatic or ***manual non-safety system*** if the system is of sufficient quality to perform the necessary function under the associated event conditions and within the required time.

Section 15.0, Introduction - Transient and Accident Analyses

AOOs, as defined in Appendix A to 10 CFR Part 50, are those conditions of normal operation that are expected to occur one or more times during the life of the nuclear power unit.

The reviewer verifies that the applicant has specified ***only safety-related systems or components for use in mitigating AOO and postulated accident conditions***, and has included the effects of single active failures in those systems and components. The reviewer may consider the licensee's technical justifications for the ***operation of nonsafety-related systems or components (e.g., when they are used as backup protection and when they are not disabled***, except by a detectable, random, and independent failure).

Safety related manual controls must be used for the primary success path; however, non-safety controls can be used for as backup protection for AOOs.