RAI Volume 2, Chapter 2.1.1.7, Fifth Set, Number 1: The following questions pertain to DOE's design of the important-to-safety (ITS) controls and instrumentation relied on for safety functions of structures, systems, and components, described in SAR Sections 1.2.3, 1.2.4, 1.2.5, 1.2.6, 1.2.8, 1.3.3, 1.4.1, and 1.4.2. The information is needed to verify compliance with 10 CFR 63.112(f).

Provide information on electrical schematics and technical specifications for interlocks (SAR Section 1.4.2) and sensors/switches for operation (SAR Figures 1.2.4-20), including the component design, design bases, and design criteria (e.g., IEEE, NEC, IEC or NFPA Codes).

SAR Section 1.4.2 describes hardwired interlocks which are part of ITS controls. Also, various Process and Instrumentation Diagrams (e.g., SAR Figure 1.2.4-20) list sensors and switches. However, electrical schematics and technical specifications, including component design, design basis, and design criteria and specific Codes applicable to each ITS control, are not provided.

1. RESPONSE

Electrical schematics and technical specifications of interlocks, sensors, and switches are considered aspects of detailed design and will be developed during a future stage of the design process. The design presented in the SAR was used to perform the preclosure safety analysis (PCSA) and develop nuclear safety design bases and the associated design criteria. The process and instrumentation diagrams (e.g., SAR Figure 1.2.4-20), ventilation and instrumentation diagrams (e.g., SAR Figure 1.2.4-100), control logic diagrams (e.g., SAR Figure 1.2.4-21), and electrical single line diagrams (e.g., SAR Figure 1.4.1-12) in SAR Sections 1.2.3, 1.2.4, 1.2.5, 1.2.6, 1.2.8, 1.3.3, and 1.4.1 provided the information the PCSA used to identify and evaluate important to safety (ITS) controls. As requested in the April 23, 2009, clarification call, a correlation between the ITS control function and the applicable codes or standards is provided in the following discussion.

The nuclear safety design bases for ITS structures, systems, or components (SSCs) are described within SAR Section 1.9 (Tables 1.9-2 through 1.9-7). SSCs are listed at a high level of assembly (e.g., canister transfer machine) rather than for each ITS instrumentation and control component or appurtenance. A description of the PCSA of interlocks, sensors and switches is provided in RAI 2.2.1.1.7-5-002. The nuclear safety design bases and associated design criteria are tabulated in SAR Sections 1.2.3, 1.2.4, 1.2.5, 1.2.6, 1.2.7, 1.2.8, 1.3.3, and 1.4.1 (e.g., SAR Table 1.2.4-4). The ITS subsystems, components and appurtenances are shown on the figures in the SAR sections that describe the facilities and the systems.

Table 1 provides the codes and standards for instrumentation and control components that are expected to fit within the reliability requirements established by the PCSA. The DOE has chosen to adopt standards that were developed to provide criteria and requirements for safety-related SSCs in commercial nuclear power generating stations in order to provide a proven and accepted means for the design of SSCs that are ITS. Using the methods and practices of industry codes

and standards provides established performance levels, accepted levels of reliability, and service factors based on equipment usage and performance. Based on the results of the PCSA and detailed design, appropriate sections of nuclear related codes and standards will be applied. Similarly, appropriate sections of the Institute of Electrical and Electronics Engineers Class 1E requirements will be implemented. Any exceptions to the codes and standards listed in Table 1 will be clarified at the detailed design stage.

2. COMMITMENTS TO NRC

None.

3. DESCRIPTION OF PROPOSED LA CHANGE

None.

4. REFERENCES

BSC (Bechtel SAIC Company) 2007. *Project Design Criteria Document*.000-3DR-MGR0-00100-000-0007. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20071016.0005.

Table 1. Principle Codes and Standards Used in the Design of ITS Controls

Codes & Standards	Applicability
ANSI/ANSHPSSC-6.8.1-1981, *Location and Design Criteria for Area Radiation Monitoring Systems for Light Water Nuclear Reactors*	Radiation monitoring
ANSI/HPS N13.1-1999, *American National Standard Sampling and Monitoring Releases of Airborne Radioactive Substances from the Stacks and Ducts of Nuclear Facilities*	Exhaust air sampling & alarm annunciation
ANSI N42.17B-1989 (R2005). *American National Standard, Performance Specifications for Health Physics Instrumentation-Occupational Airborne Radioactivity Monitoring Instrumentation*	Radiation monitoring
ASME AG-1a-2004. 2005. *Addenda to ASME AG-1-2003, Code on Nuclear Air and Gas Treatment*	HVAC confinement system
ASME NOG-1-2004. 2005. *Rules for Construction of Overhead and Gantry Cranes (Top Running Bridge, Multiple Girder).*	Overhead and gantry cranes
ASHRAE DG-1-93. 1993. *Heating, Ventilating, and Air-Conditioning Design Guide for Department of Energy Nuclear Facilities*	HVAC confinement system
DOE-HDBK-1169-2003. *Nuclear Air Cleaning Handbook*	HVAC confinement system
International Building Code 2000, with Errata to the 2000 International Building Code	Seismic design of electrical and control ITS systems that are not credited with preventing or mitigating seismic event sequences
IEEE Std 308-2001, *IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations* (with the exception that tests are conducted on a 24-month frequency in accordance with Regulatory Guide 1.75, *Criteria for Independence of Electrical Safety Systems*)	Principal design criteria and the design features of ITS power and control systems
IEEE Std 336-2005, *IEEE Guide for Installation, Inspection, and Testing for Class 1E Power, Instrumentation, and Control Equipment at Nuclear Facilities*	Installation, inspection, and testing of ITS power, instrumentation, and control components
IEEE Std 384-1992, *Standard Criteria for Independence of Class 1E Equipment and Circuits*	Isolation and physical separation methods for ITS components
IEEE Std 603-1998, *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations*	Design reliability, qualification, and testability of the ITS power, instrumentation and control systems
NFPA 70, *National Electrical Code*	Design, installation, and wiring of instrument and control systems

Source: BSC 2007, Sections 4.3, 4.6, 4.8, and 4.9

RAI Volume 2, Chapter 2.1.1.7, Fifth Set, Number 2: The following questions pertain to DOE's design of the important-to-safety (ITS) controls and instrumentation relied on for safety functions of structures, systems, and components, described in SAR Sections 1.2.3, 1.2.4, 1.2.5, 1.2.6, 1.2.8, 1.3.3, 1.4.1, and 1.4.2. The information is needed to verify compliance with 10 CFR 63.112(f).

Verify whether the interlocks and sensors/switches meet the features of fail-safe safety, fault tolerance, redundancy, high availability and Diversity and Defense in Depth, and protection against single point of failure, that are equivalent to industry Codes (e.g. IEEE 379 and 603, NEC, IEC or NFPA Codes) for classification of ITS controls as Class 1E equipment.

1. RESPONSE

Working in concert with design development, the preclosure safety analysis (PCSA) evaluated fail-safe features, redundancy, diversity, and protection against single-point failures, as appropriate, to achieve the reliability of important to safety (ITS) equipment specified in the nuclear safety design bases. Based on engineering evaluations and PCSA identification of ITS structures, systems, and components (SSCs), appropriate codes and standards were designated for the ITS SSCs. The response to RAI 2.2.1.1.7-5-001 identifies the codes and standards for use in the design of instrument and control systems and further identifies that exceptions to the codes and standards listed will be clarified at the detailed design stage, based on results of the PCSA and detailed design. Therefore, the specific design features such as fail-safe safety, fault tolerance, redundancy, high availability and Diversity and Defense in Depth, and protection against single point of failure inherent in each of the specified codes and standards will be followed, unless during detailed design, based on the PCSA and design requirements, an exception is warranted. However, the methodology used to determine the appropriate protections differs greatly from methodologies suggested by those codes. The differences are rooted in the risk-informed nature of the design. As such, the reliability analyses performed for the PCSA do not evaluate code and standard specific control system designs, configurations, or logic diagrams, but instead use reliability data sources that provide the historical performance of typical interlocks and sensors/switches within the context of fault tree analysis for the integrated evaluations of SSCs utilizing such components. Accordingly, specific design features such as fail-safe safety, fault tolerance, redundancy, high availability and Diversity and Defense in Depth, and protection against single point of failure, are not modeled explicitly for instrument and control components, but instead are inherent in the reliabilities of the components evaluated. A specific example of how separation is achieved is provided in the response to RAI 2.2.1.1.7-5-003.

The nuclear safety design bases for ITS SSCs are described within SAR Section 1.9 (Tables 1.9-2 through 1.9-7). SSCs are listed at the major component or subcomponent level (e.g., canister transfer machine) rather than specific entries for each ITS subcomponent in the design of the major component. The safety function and the controlling parameters and values are also listed for each identified ITS SSC. The controlling parameters and values of the nuclear safety design bases can be generally grouped into the following categories: (1) the mean frequency of SSC

failure, (2) the specific design features of an SSC, or (3) the mean unavailability of an SSC over time. Use of data from the mean frequency of SSC failure and mean unavailability of an SSC over time in fault tree analysis inherently addresses the reliability requirements associated with the features of fail-safe safety, fault tolerance, redundancy, high availability, diversity, defense in depth, and protection against single points of failure. For example, redundancy in the design is included in the fault tree analyses to achieve the reliabilities found in the controlling parameters and values. The reliability databases inherently reflect the field experience associated with those codes and standards that underlie the design of components in the databases. Specific design features must be satisfied as specified in the nuclear safety design bases; individual codes and standards are not specified as requirements for design.

1.1 PCSA METHODOLOGY FOR DETERMINING MEAN FREQUENCY OF SSC FAILURE OR UNAVAILABILITY

Design information for the PCSA is obtained from design documents, such as design drawings, design reports, block diagrams, process and instrumentation diagrams, ventilation and instrumentation drawings, control logic diagrams, design calculations, mechanical handling design reports, and general arrangement drawings consistent with the guidance of "Preclosure Safety Analysis—Level of Information and Reliability Estimation" (NRC 2007). This information is used to both identify initiating events and to conduct event sequence analyses. When sequences include a level of equipment or SSC assembly that is not directly supported by industry-wide reliability data or failure history records, fault tree analysis is used to disaggregate the higher level of assembly to that level for which reliability data is available. For example, reliability data from the data sources [such as the *Nonelectronic Parts Reliability Data 1995* (NPRD-95)] cannot be directly applied to obtain the frequency of spurious motion of a canister transfer machine. Fault tree analysis, however, disaggregates the canister transfer machine design into those component failure modes (e.g., interlock fails to respond) for which reliability information exists.

The approach for developing these active component reliability estimates is to gather and review industry-wide data and apply Bayesian combinational methods to develop mean values and uncertainty bounds (represented as probability distributions) that best represent the range of the industry-wide information. The reliability databases used in the PCSA represent a broad base of industry codes and standards (e.g., IEEE 379 and 603, NEC, IEC or NFPA Codes). It is preferred that equipment failure rate information be obtained from facilities in the same industry if there is a sufficient experience base and corresponding data from that industry. However, to assure that an adequate statistical database was available for the specific operations conducted at the repository, it was necessary to develop the required data from the experience from both nuclear and nonnuclear industries to represent the repository SSCs. Data sources used for reliability determinations are described in Attachment C of *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis* (BSC 2008a). Therefore, the reliability requirements of the nuclear safety design bases have incorporated the features of fail-safe safety, fault tolerance, redundancy, high availability and diversity and defense in depth, and protection against single point of failures by use of the fault tree analyses.

Furthermore, the scope of the sources selected for this data set is deliberately broad to increase the probability that repository equipment reliability requirements selected as controlling parameters for the nuclear safety design bases would fall within the bounds of variability defined by operational experience across industries. A combined estimate that reflects the uncertainty ranges defined by the data source values has been developed. For the PCSA, Bayesian analysis is used [e.g., per NUREG/CR-6823, *Handbook of Parameter Estimation for Probabilistic Risk Assessment* (Atwood et al. 2003)] to develop "prior" distributions. Prior distributions are appropriate when actual operating experience from the specific facility being analyzed is not yet available. This is the situation with evaluation of the repository handling facilities. The Bayesian approach permits a variety of different sources to be statistically combined and represented as a probability distribution, often documented in terms of a mean or median and standard deviation. These values will be confirmed as part of the maintenance plan development and then updated during operations as operating experience becomes available, as discussed in the Reliability Centered Maintenance Plan described in SAR Section 5.6.4.

1.2 PCSA SPECIFICATION OF SPECIFIC DESIGN FEATURES

In some instances, the nuclear safety design bases require specific design features as part of the evaluation process. For example, for transportation, aging, and disposal, slide gates (identified as Component 060-HTC0-HTCH-00010, 11, Nuclear Safety Design Bases item CR.HTC.09) have a controlling parameter and value that requires that "Closure of the slide gate shall be incapable of breaching a canister" (BSC 2008b, Table C-1). This requirement will be implemented by analyses to confirm that the force of the slide gate on a canister is not capable of exceeding the yield strength of the canister. Therefore, applicable standards for material properties and structural analyses serve to define inputs and methods.

1.3 SUMMARY

The PCSA uses a risk-informed approach to identify ITS SSCs and to determine their controlling parameters and values, rather than using a strict adherence to the traditional application of design criteria. Therefore, informed use of reliability databases with the Bayesian combinational methods to develop probability distributions produces a representation of industry-wide variability that gives high confidence that the nuclear safety design bases controlling parameters and values are achievable given currently available equipment, designed in accordance with the instrument and controls codes and standards presented in the response to RAI 2.1.1.7-5-001.

2. COMMITMENTS TO NRC

None.

3. DESCRIPTION OF PROPOSED LA CHANGE

None.

4. REFERENCES

Atwood, C.L.; LaChance, J.L.; Martz, H.F.; Anderson, D.J.; Englehardt, M.; Whitehead, D.; and Wheeler, T. 2003. *Handbook of Parameter Estimation for Probabilistic Risk Assessment*. NUREG/CR-6823. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20060126.0121.

BSC (Bechtel SAIC Company) 2008a. *Canister Receipt and Closure Facility Reliability and Event Sequence Categorization Analysis*. 060-PSA-CR00-00200-000-00A CACN 001. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080311.0031; ENG.20080331.0007.

BSC 2008b. *Preclosure Nuclear Safety Design Bases*. 000-30R-MGR0-03500-000-000 ACN 03. Las Vegas, Nevada: Bechtel SAIC Company. ACC: ENG.20080312.0036; ENG.20080404.0007; ENG.20080406.0001; ENG.20080417.0001.

Denson, W.; Chandler, G.; Crowell, W.; Clark, A.; and Jaworski, P. 1994. Nonelectronic Parts Reliability Data 1995. NPRD-95. Rome, New York: Reliability Analysis Center.

NRC (U.S. Nuclear Regulatory Commission) 2007. "Preclosure Safety Analysis—Level of Information and Reliability Estimation." Interim Staff Guidance HLWRS-ISG-02. Washington, D.C.: U.S. Nuclear Regulatory Commission. ACC: MOL.20071018.0240.

RAI Volume 2, Chapter 2.1.1.7, Fifth Set, Number 3: The following questions pertain to DOE's design of the important-to-safety (ITS) controls and instrumentation relied on for safety functions of structures, systems, and components, described in SAR Sections 1.2.3, 1.2.4, 1.2.5, 1.2.6, 1.2.8, 1.3.3, 1.4.1, and 1.4.2. The information is needed to verify compliance with 10 CFR 63.112(f).

Clarify how separation of protection and control systems is met for independence and isolation characteristics of ITS controls, especially when ITS interlocks interface with non-ITS controls like Programmable Logic Controllers, Digital Control Management Information Management System logic interlock and various sensors and switches.

1. RESPONSE

The response to RAI 2.2.1.1.7-5-001 identifies the principle codes and standards that are used for controls and instrumentation, and the response to RAI 2.2.1.1.7-5-002 discusses the implementation of design in conjunction with the preclosure safety analysis (PCSA). The instrumentation and control design presented in the SAR was used for the PCSA to identify important to safety (ITS) systems, structures, and components. Based on requirements identified by the PCSA, the separation practices typical of Class 1E control and instrumentation design will be implemented to provide independence and isolation of ITS components (e.g., hardwired interlocks) from non-ITS components such as programmable logic controllers (PLCs) and the digital control and management information system (DCMIS).

The physical separation of circuits and equipment is achieved by the use of ITS structures, separation distance, or barriers, or any combination thereof. Electrical isolation is achieved by the use of separation distance, isolation devices, shielding and wiring techniques, or combinations thereof.

ITS interlocks, sensors, and switches are hardwired; precluding operational control from computer based systems such as PLCs and the DCMIS (see SAR Section 1.4.2). Where redundant ITS sensors and switches are needed to satisfy reliability requirements established by the PCSA, a partitioning design philosophy is used to ensure that no redundant instrumentation or equipment share common input or output modules (see SAR Section 1.4.2.1.1, p. 1.4.2-5, Redundancy). The design of the ITS interlocks and switches for redundancy and reliability incorporates nuclear industry practices and is discussed in SAR Sections 1.4.1.2.1 and 1.4.1.2.8. As an example, SAR Figures 1.2.4-101 and 1.2.4-102 show the redundant trains of ITS confinement heating, ventilation, and air-conditioning in the Canister Receipt and Closure Facility, and SAR Figure 1.2.4-103 shows the logic diagram for this function.

If non-ITS controls utilize the same information as ITS controls, then non-ITS control components, optical signal isolators or some combination thereof, are used by the non-ITS control system as a means to perform the necessary control functions while isolated from, and independent of, the ITS (hardwired) components. As an example, operational limits for lifts and transfer motions are encoded in the DCMIS and provide limits for normal operator controls,

while ITS hardwired limit switches are relied upon to ensure that safety limits for lifts and transfer motions are not exceeded (see SAR Section 1.9.1.12). For example, SAR Figure 1.2.4-36 shows the logic diagram for the cask handling crane main hoist.

SAR Figure 1.2.4-21 represents a typical logic diagram for the Canister Receipt and Closure Facility, Initial Handling Facility and Wet Handling Facility. Figure 1 is an annotated excerpt from SAR Figure 1.2.4-21 and clarifies the functional application of isolation and separation within IEEE Std 308-2001, *IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations,* IEEE Std 384-1992, *Standard Criteria for Independence of Class 1E Equipment and Circuits,* and IEEE Std 603-1998, *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations*. The bold line within Figure 1 demonstrates the isolation and independence characteristics of the ITS system from the non-ITS DCMIS (e.g., the DCMIS individual inputs do not interface with the hardwired ITS system inputs, and the ITS inputs bypass the non-ITS DCMIS). The logic diagram in Figure 1 indicates that a signal from the DCMIS system cannot energize the ITS motor starter coil to open a confinement door or slide gate until the ITS (hardwired) system indicates that each of the confinement doors and slide gate are fully engaged in the closed (fail-safe) position. Stated differently, the ITS components (e.g., switches, interlocks) will only allow one confinement door or slide gate to be open at a time.

In summary, separation and isolation requirements of the ITS controls are derived from the nuclear safety design bases in SAR Section 1.9 and implemented by IEEE Std 308-2001, IEEE Std 384-1992 and IEEE Std 603-1998. ITS hardwired components ensure that limits relied upon to mitigate event sequences are not surpassed.

2. COMMITMENTS TO NRC

None.

3. DESCRIPTION OF PROPOSED LA CHANGE

None.

4. REFERENCES

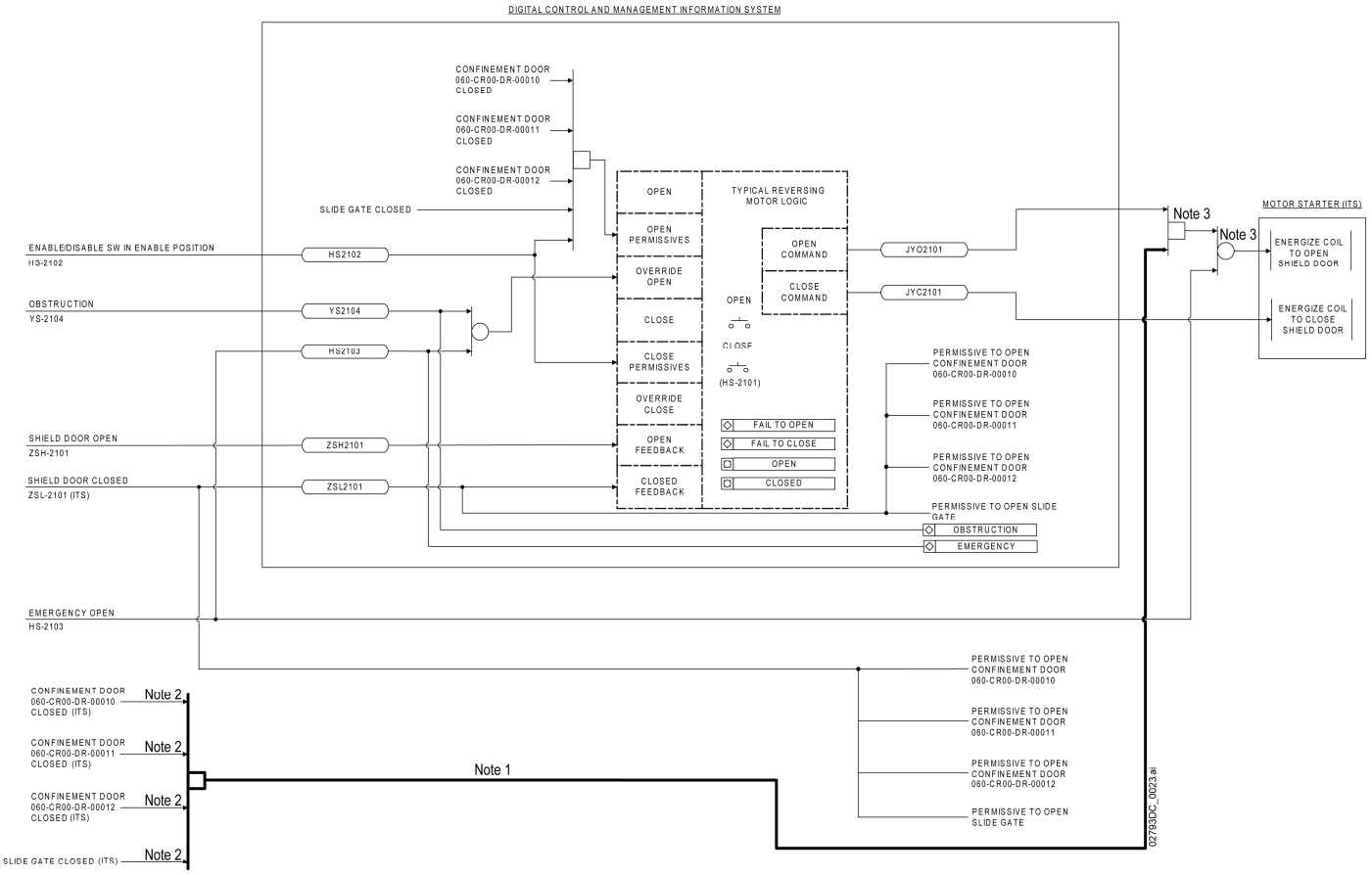
IEEE Std 308-2001. 2002. *IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations*. New York, New York: Institute of Electrical and Electronic Engineers. TIC: 252746.

IEEE Std 384-1992. *Standard Criteria for Independence of Class 1E Equipment and Circuits*. New York, New York: Institute of Electrical and Electronics Engineers. TIC: 258693.

IEEE Std 603-1998. *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations*. New York, New York: The Institute of Electrical and Electronics Engineers. TIC: 242993.

ENCLOSURE 3

Response Tracking Number: 00332-00-00 RAI: 2.2.1.1.7-5-003



Notes:
1. The bolded (thicker) line represents the functional, physical independence and isolation design criteria per IEEE Std 308 and IEEE Std 603.
2. DCMIS inputs are isolated from ITS components per IEEE Std 384.
3. The identified logic components are an integral (hardwired) part of the ITS motor starter.

Figure 1. Annotated Logic Diagram Excerpt of SAR Figure 1.2.4-21 for Clarification of Isolation