Westinghouse Electric Company
Engineering, Equipment and Major Projects
1000 Westinghouse Drive
Cranberry Township, Pennsylvania 16066
USA

U.S. Nuclear Regulatory Commission
Document Control Desk
11555 Rockville Pike
Rockville, MD 20852

Direct tel: (412) 374-4643
Direct fax: (724) 720-0754
e-mail: greshaja@westinghouse.com

LTR-NRC-13-61

August 15, 2013

Subject: Submittal of "Comments on Draft Safety Evaluation for 6002-00301, Revision 4, 'Advanced Logic System Topical Report,' (Project # 779/TAC No. ME4454)"

References:

1. NRC Letter, A. J. Mendiola (NRC) to J. A. Gresham (Westinghouse), "Draft Safety Evaluation on the Topical Report 6002-00301, 'Advance Logic System Topical Report' (TAC No. ME4454)"

Reference 1 requested that Westinghouse review the draft Safety Evaluation (SE) for 6002-00301, Revision 4 to identify proprietary information and to comment on issues of fact or clarity. Accordingly, Westinghouse comments are provided in Enclosure 1.

Very truly yours,

John T. Conne for

James A. Gresham, Manager
Regulatory Compliance

Enclosure

D099

Comments on Draft Safety Evaluation for 6002-00301, Revision 4, "Advanced Logic System Topical Report" (Project # 779/TAC No. ME4454)

Page	Section	Status	Draft SE	Comment
3	2.0 REGULATORY EVALUATION	Typo	The NRC staff also considered the application-specific 10 CFR Part 50, Appendix A, General Design Criterion, when evaluating the topical report for use in safety systems, as follows: o GDC 1, "Quality Standards and Records" o GDC 2, "Design Basis for Protection Against Natural Phenomena" o GDC 4, "Environmental and Dynamic Effects Basis" o GDC 13, "Instrumentation and Control" o GDC 20, "Protection Systems Functions" o GDC 21, "Protection System Reliability and Testability" o GDC 22, "Protective System Independence" o GDC 23, "Protection System Failure Modes" o GDC 24, "Separation of Protection and Control Systems" o GDC 25, "Protection System Requirements for Reactivity Control Malfunctions" o GDC 29, "Protection Against Anticipated Operational Occurrences"	GDC 2, "Design Bases for Protection Against Natural Phenomena" GDC 4, "Environmental and Dynamic Effects Bases" GDC 20, "Protection System Functions" GDC 22, "Protection System Independence"
3	2.0 REGULATORY EVALUATION	Typo	The NRC staff evaluated the topical report using applicable portions of the following guidance: • RG 1.22, "Periodic Testing of Protection Actuation Functions," Revision 0, describes a method acceptable to the NRC staff for inclusion of actuation devices in the periodic tests of the protection system during reactor operation.	RG 1.22, "Periodic Testing of Protection System Actuation Functions,"
13	3.1.2 Development and Operational Concept Overview	Clarification	Once an ALS platform-based instrument has been programmed for plant-specific use and delivered to the applicant or licensee, ALS platform design features prevent the applicant or licensee from altering either the standardized or application-specific FPGA logic. Furthermore, ALS platform design features prevent the maintenance workstation from modifying any non-operationally adjustable settings required to remain constant so the equipment remains capable of performing its application-specific instrument functions.	The scope/intent of the following statement , "altering either the standardized or application-specific FPGA logic", is assumed to mean that an applicant or licensee cannot change the actual HDL/RTL. It is assumed that it does not prevent the applicant or licensee to flash application logic onto an ALS-102 CLB or flash an NVM to configure an IO board. It is important for the applicant or licensee to have the capability to flash ALS-102 CLBs or IO board NVMs to configure spares to minimize spare part inventory. For clarification WEC recommends the following sentence be added before "Further more,...: This does not preclude the licensee from flashing certified files, supplied by the manufacturer, onto ALS onsite inventory. The flashing of certified files, using licensee administrative procedures, includes configuring boards for specific use via the NVM, and loading application-specific logic onto the CLB FPGA.
29 30 31	3.2.1 Overview of the ALS Platform's Use of the FPGA Technology	Typo	Comparisons between typical discrete low-scale integrated circuits, which may be more familiar, to FPGAs, which may be less familiar, can help to understand the FPGA technology and provide further insights despite a fundamental difference between the two.	"Large Scale Integrated circuits (LSI)" or "Small Scale Integrated circuit (SSI)" is widely used.
36	3.2.1 Overview of the ALS Platform's Use of the FPGA Technology	Clarification	For a typical µP design, dedicated diagnostic routines execute in an attempt to detect failures. The ALS platform FPGAs implement dedicated FSMs to perform diagnostics. SEUs and Single Event Latch-ups (SELs) can corrupt a memory location or other internal register within a µP and result in unpredictable behavior. This characteristic is undesirable from a safety assessment perspective. To address this concern, µP-based designs typically include a watchdog timer, which is reset at a prescribed program control point, as a mechanism to ensure and restore normal program control flow when it is lost. A watchdog timer is not applicable to FPGAs developed with constraints similar to the ALS platform FPGAs. The ALS platform FPGAs implement parallel FSMs with diversity to perform functions redundantly. The comparison of independent diverse FSM results ensures functional operability or results in annunciation of an alarm for operator action, similar to a watchdog timer timeout.	A watchdog timer is applied for RAB in ALS Platform. "Each RAB slave implements a communication watchdog time-out and "HALT" function for RAB communications." in Topical Report Page 2-31. "Each RAB slave implements a communication watchdog time-out and "HALT" function for RAB communications." in Draft SE Page 67. "The means of detection include watchdog timer, checksum for firmware and program integrity, read/write memory tests, communications monitoring, configuration validation, heartbeat, and self-diagnostics or surveillance test support features." in Draft SE Page 69.

Page	Section	Status	Draft SE	Comment
36	3.2.1.1 Technology Comparison	Typo	Table 3.2.1.1-1 identifies general characteristics that affect a SE based on the technology with which a safety system is implemented. For each general characteristic, the table presents a relative comparison of four alternative implementation technologies: Relay Logic, Discrete Low Scale Integrated (LSI) Circuits, µP, and FPGA. The table also summarizes attributes of the ALS platform FPGA development that the manufacturer has included to enhance the base FPGA technology and provide a degree of mitigation against perceived weaknesses.	"Large Scale Integrated circuits (LSI)" or "Small Scale Integrated circuit (SSI)" is widely used.
39	3.2.2 Standardized Circuit Boards	Typo	AN NRC staff review of a digital safety system requires a system description to explain how the components of the system interact to accomplish the design function from the perspective of integrated hardware and FPGA logic programs. This description facilitates subsequent NRC staff reviews and evaluations against applicable acceptance criteria. The "ALS Topical Report" (Reference 32) limits the components to seven standardized circuit boards, a backplane, and chassis. Section 3.1 of this SE provides descriptions of these components and their intended use in consideration of the "ALS Topical Report" appendices that depict notional applications of these components for several safety-related digital safety systems.	"An"
46	3.2.5 Application-Specific FPGAs	Clarification	When an applicant or licensee identifies FPGA design variants within its specifications, the manufacturer has indicated the application-specific FPGA development processes for each standardized ALS-102 FPGA variant will follow a development process equivalent to the one described and evaluated in Section 3.2.4 of this SE	WEC recommends the following wording for clarification: When an applicant or licensee identifies FPGA design variants within its specifications, the manufacturer has indicated the application-specific FPGA development processes applied to each standardized ALS-102 FPGA variant will follow a development process equivalent to the one described and evaluated in Section 3.2.4 of this SE.
63	3.4.1 Response Time	Typo	When performing the application-specific analysis to budget the timing requirement(s) as depicted "ALS Topical Report" 2.7-1, each response time performance requirement should be analyzed to address the following response time delay elements, as applicable: 1. The maximum as-built and as-configured Input Delay time for the Input Board; 2. The maximum time between consecutive accesses to the Input Board; 3. The maximum RAB transaction time to acquire the input data; 4. The maximum as-built and as-configured Logic Delay time for the Core Logic Board; 5. The maximum time between consecutive accesses to the Output Board; 6. The maximum RAB transaction time to provide the output data; and, 7. The maximum as-built and as-configured Output Delay time for the Output Board.	Insert the word "Figure": When performing the application-specific analysis to budget the timing requirement(s) as depicted in "ALS Topical Report" Figure 2.7-1, each response time performance requirement should be analyzed to address the following response time delay elements, as applicable:
69	3.4.3 Self-Diagnostics, Test and Calibration Capabilities	Typo	IEEE Std 603-1991 Clause 5.7 references IEEE Std 338-1987, "Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems" for the testing of Class 1E systems, and RG 1.118, "Periodic Testing of Electric Power and Protection Systems," endorses with exceptions IEEE Std 338-1987 as a method acceptable to the NRC staff for meeting the Commission's regulations with respect to periodic testing of electric power and protection systems. Furthermore, RG 1.22, "Periodic Testing of Protection Actuation Functions," describes a method acceptable to the NRC staff for inclusion of actuation devices in the periodic tests of the protection system during reactor operation.	Furthermore, RG 1.22, "Periodic Testing of Protection System Actuation Functions," describes a method acceptable to the NRC staff for inclusion of actuation devices in the periodic tests of the protection system during reactor operation.
74	Table 3.5-1 Docketed ALS Platform FMEA and Reliability Information	Typo	Document ID Title Reference 6002-30212 ALS-302 FPA, FMEA, and Reliability Analysis 57	Document ID Title Reference 6002-30212 ALS-302 FPA, FMEA, and Reliability Analysis 62
105	3.9 Diversity and Defense-in-Depth	Typo	10 CFR Part 50, Appendix A, GDC 21, "Protection Systems Reliability and Testability," requires, in part, "no single failure results in the loss of the protection system." GDC 22, "Protection System Independence," requires, in part, "the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions ..not result in loss of the protection function ... Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function." GDC 24, "Separation of Protection and Control Systems," requires, in part, "interconnection of the protection and control systems shall be limited so as to assure safety is not significantly impaired." GDC 29, "Protection Against Anticipated Operational Occurrences," requires, in part, defense against anticipated operational transients "to assure an extremely high probability of accomplishing ... safety functions."	, GDC 21, "Protection System Reliability and Testability,"
125	3.10.2.5 IEEE Std 603-1991 Clause 5.5 – System Integrity	Typo	As described in Section 3.5 of this SE, the manufacturer performed a failure modes and effects analysis (FMEA) for each of the seven ALS platform standardized circuit boards. The NRC staff reviewed the FMEAs (References 56, 57, 68, 74, 80, 86, and 92) to confirm the platform design features provide capabilities that allow construction of a safety system with the ability to fail in a safe state. Nevertheless, an assessment of the application specifications for a full system design is necessary to demonstrate fulfillment of the requirement to fail in a safe state, when applicable.	Reference 57 should be Reference 62: The NRC staff reviewed the FMEAs (References 56, 62, 68, 74, 80, 86, and 92) to confirm the platform design features provide capabilities that allow construction of a safety system with the ability to fail in a safe state.

Page	Section	Status	Draft SE	Comment
183	5.0 REFERENCES	Typo	CSI Corporate Documents 27. 9000-00000, "CSI Quality Assurance Manual," Revision 6, dated November 11, 2011 (Proprietary - ML11320A102) 28. 9000-00311, "Electronics Development Procedure," Revision 4, dated July 29, 2010 (Proprietary - ML102160485) 29. NA 4.50, "Electronics Development Procedure," Revision 0, August 31, 2012 (Proprietary - ML12332A311) 30. 9000-00313, "FPGA Development Procedure," Revision 4, September 6, 2012 (Proprietary - ML12332A315) 31. NA 4.51, "FPGA Development Procedure," Revision 1, January 13, 2013 (Proprietary - ML13036A400)	31. NA 4.51, "FPGA Development Procedure," Revision 1, January 1, 2013 (Proprietary - ML13036A400)