Supplemental Information to WCAP-18461, Revision 1, "Common Q Platform and Component Interface Module System Elimination of Technical Specification Surveillance Requirements" (Non-Proprietary)

April 2020

Westinghouse Electric Company
1000 Westinghouse Drive
Cranberry Township, PA 16066

No	Section Reference	Page	Comment	Westinghouse Responses
1	3.5	3 3	The revised BTP 7-17 evaluation conclusion now states "SNC stated that it is not possible to verify self-diagnostic functions as part of surveillance testing during operation because it would require creating destructive faults within the I&C system". Though this is a quote out of the Vogtle LAR safety evaluation, it is a statement made by the licensee and not the NRC. The NRC staff does not agree with the interpretation being made that the BTP criterion calls for complete functional testing of the self-diagnostic functions. Instead, the BTP states that the licensee should confirm execution of self-diagnostic tests during plant operation. The NRC staff does not agree with this assessment of this criterion or the justification for not meeting it. The BTP does not require 100% functional testing of the self-diagnostic functions as the topical report states. Instead, the BTP requires these functions to be verified (operational) during periodic tests. That is how we have applied this criterion in the past. This interpretation is also consistent with the NRO safety evaluation of the Vogtle LAR because that evaluation also required the licensee to perform periodic checks of the SD functions. No such periodic checks are mentioned in the WCAP. The NRC has never agreed to this statement that SNC made. For the evaluation the NRC staff is looking to see if the licensee's activities will confirm that the self-diagnostics that are being credited for surveillance elimination are functioning correctly. This is not just a back-up to fault identification. In the draft supplement provided by Westinghouse on 3/25/2020, a new licensee required action is being included that would require licensees to describe actions that will be performed to add assurance (defense-in-depth) that faults are captured and investigated. This is not the same as confirming that the self-diagnostics that are being credited for surveillance elimination are functioning correctly. This issue therefore remains unresolved.	WCAP 18461 will be updated as follows: <u>Section 5.4 Update</u> "Additionally, routine plant personnel actions will be necessary to ~~add assurance (defense-in-depth) that faults are captured and investigated~~ assure adequate operation of the Common Q subsystem and the CIM/SRNC subsystem diagnostic functions that are credited. This includes (but are not limited to) operator rounds and MCR board walkdowns, as well as system health checks performed by system engineering on a periodic basis. The result of the system engineer checks will be summarized in system health reports, and any adverse condition will be captured in plant condition reports. Should it be determined that a diagnostic problem is identified as part of the Common Q platform, a condition report (CR) would be filed by the licensee and transmitted to Westinghouse who will then take the appropriate corrective actions to resolve the issue." <u>LRA_8 Update</u> "LRA_8 – The licensee will provide a description of plant administrative controls that will provide assurance ~~(defense-in-depth)~~ that diagnostic faults are captured and investigated. This may include items such as operator rounds and system engineer monthly reports that evaluate and document the health, errors, and adequate operation of the Common Q subsystem. In doing so, the anticipated actions in Section 5.4 of this WCAP will be met."
2	Appendix C	C-1	There is no Licensee Required Action (LRA) to perform operational checks of the self-diagnostic functions that are being credited for surveillance elimination. The draft supplement adds a licensee required action, but the objective of this action does not meet the criteria of BTP 7-17; to confirm execution of the automatic tests during plant operation. This issue therefore remains unresolved.	WCAP-18461 will be modified as stated in the response to comment 1.
3	Appendix C	C-1	Old LRA 5 has been deleted. The NRC would like to know why this LRA was no longer required.	LRA_5 was moved to Appendix B in WCAP-18461 Revision 1, since it should be a requirement of the system (see the Record of Changes).
4	Appendix D	D-1 through D-54	Deletion of Channel Check surveillances will not be allowed for systems that do not include ITPs. The TS mark-ups or the LRAs should include instructions to licensees so that these surveillances are not inadvertently deleted.	It is explicitly stated within WCAP-18461 Revision 1 that the ITP is necessary (Section B.1, third bullet) to remove channel checks. LRA_1 was updated to address the ITP and LRA_7 was written to explicitly address the ITP. Additionally, the Channel Check Elimination Sections (7.1.1 and 7.2.1) specifically call out the [ ]^{a,c} that is leveraged to eliminated Channel Checks as the [ ]^{a,c}
5	General	4.1.1,	1) The topical report makes no mention of [ ]^{a,c}. These functions were discussed in the Vogtle LAR and supplement. The NRC needs information on these self-diagnostic functions in order to credit them as a basis for surveillance elimination.	1) [ ]^{a,c}

No	Section Reference	Page	Comment	Westinghouse Responses
			2) Section 5.1 does discuss [ ]a,c. Are these the same as [ ]a,c [ ]a,c? Why are these functions omitted from the platform Topical Report, or are these new terms being used to describe functions that are discussed in the platform TR? If the latter is the case, then please explain exactly which platform functions constitute these [ ]a,c	2) [ ]a,c
6	4.3.1	4 4	The TR states: "IEC 60880 is comparable to IEEE 7-4.3.2, and the staff has found IEC 880 to be an acceptable equivalent". This statement originated in the original Common Q safety evaluation but has been replaced in the updated SE. The NRC does not consider IEC 880 to be an equivalent to IEEE 7-4.3.2. As such, the NRC evaluates all digital systems to the criteria of IEEE 7-4.3.2 alone.	Section 4.3.1 which refers to previous NRC evaluations of the Common Q platform, including the initial safety evaluation of the Common Q platform, will be deleted. In its place, WCAP-18461 will point to the NRC staff's evaluation of the quality of the Common Q self-diagnostics discussed in the SER for the Vogtle 3&4 LAR 19-001 (specifically Section 3.3.1.3 of the SER). The update will read as follows: *"~~4.3.1 Common Q Topical Report – NRC Safety Evaluation~~* ~~The Common Q Platform diagnostics were developed under a robust process that was reviewed by the NRC. In 2000, the NRC issued a safety evaluation report (ML003740165, Bibliography 1) on the Common Q Topical Report (CENP-396-P, Rev. 01 which is the predecessor to WCAP-16097-P-A, Reference 7). In that report the NRC acknowledged receipt of Westinghouse document GKWF700777, "Design and Life Cycle Evaluation Report on Previously-Developed Software in ABB AC160, I/O Modules and Tool Software" (Bibliography 2) in support of the commercial dedication of the AC160.~~ ~~The safety evaluation report states that the, "AC160 PDS [Previously Developed Software] is composed of the AC160 software, S600 I/O Module(s) software, and ABB Tool software. The evaluation is based on the requirements specified in International Electrotechnical Commission (IEC) standard IEC-60880, "Software for Computers in the Safety Systems of Nuclear Power Stations." IEC 60880 is referenced in IEEE 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations". IEC 60880 is comparable to IEEE 7-4.3.2-2003, and the staff has found standard IEC 880 to be an acceptable equivalent."~~ ~~The Design and Lifecycle Evaluation (DLCE) applies to all aspects of the PDS including the system software that executes the nuclear application program and the diagnostics integrated with the system software. In other words, the same software quality approach applied to both aspects of the system software.~~ "In the NRC SER for the Vogtle 3&4 LAR 19-001 (ML19297D159, Reference 44), the NRC staff evaluated the quality of the self-diagnostics within the PMS (Section 3.3.1.3 of the SER) and concluded that there is "reasonable assurance that the self-diagnostic functions of the Common-Q based PMS subsystem will perform as designed" as well as "reasonable assurance that the CIM-SRNC self-diagnostic functions will perform as designed." These are the same Common Q and CIM-SRNC diagnostics credited in this report."
7	4.2	4 3	The TR states that the AP1000 PMS is single failure tolerant since the two systems contain the same Common Q equipment. The NRC does not agree with the assertion that PMS is single failure compliant just because the equipment is Common Q. The equipment type is not the basis for a system being SFC compliant.	It is agreed that just because the PMS used the Common Q platform it cannot be extrapolated that the Common Q based PPS described in the WCAP can be considered single failure tolerant. As such, this paragraph will be updated as follows: "With the methodology for eliminating SRs within this report, the diagnostics must cover these postulated failure modes. This is done by starting with the AP1000 PMS Failure Modes and Effects Analysis (FMEA) (WCAP-16438-P, "FMEA of AP1000 Protection and Safety Monitoring System," Reference 21)~~, which shows that the PMS is single failure tolerant (which is used within this topical report to demonstrate that the generic PPS is single failure tolerant since the two systems contain the same Common Q equipment).~~ The Failure Modes, Effects, and Diagnostics Analyses (FMEDAs) listed in Section 6 are based on the failure modes outlined in Reference 21, and these tables demonstrate diagnostic coverage for the aforementioned failure modes~~. By doing so, this establishes that the PPS will still be single failure tolerant.~~"

No	Section Reference	Page	Comment	Westinghouse Responses
8	4.3.2	4 3	Though the supplemental information in ML19280E414 is referred to in this section, there is no mention of Vogtle's commitment to perform operational checks of SDs via Conduct of Operations and System Health Checks which are described on pages 8 and 9 of the supplement. This implies that these SD checks are not needed. The NRCs safety evaluation for LAR 19-001 uses Conduct of Operations activities and System Health checks described in the supplement as a basis for its approval. "the NRC staff determined that the approaches described in the supplemented LAR meet the intent of the acceptance criteria in BTP 7-17 for checking and monitoring the PMS self-diagnostic functions during operation." The following are additional quotes from the Vogtle license amendment request safety evaluation. Section 3.3.2.3 of the LAR safety evaluation states the following: "The SNC LAR supplement contained information related to the PMS system alarm functionality and plant administrative controls that will be implemented to assure continued monitoring of the PMS system to assure adequate operation of the system diagnostic functions." "In the absence of the either divisional or system alarms, there will also be operator rounds and system engineer's monthly reports that evaluate and document the health, errors, and faults of system." "During the audit activities, the staff discussed the system features, including system alarm functions, and additional administrative controls planned to be implemented to ensure the continued adequate functionality of the PMS system diagnostic functions during operations with the cognizant SNC and WEC staff. Based on those discussions, the licensee provided a supplement to the LAR to document the system features and administrative controls, as described herein, to address continued functionality of the credited PMS diagnostic functions." "Additionally, as part of normal control room operator rounds additional observations are taken and are recorded via the Unit Control Log. These include: checking for proper PMS node heartbeats for each division; checking the safety visual displays for each division for health status; and unit control log entry of conditions such as, control panel walkdowns, unexpected alarms, entry into abnormal or emergency operating procedures, and recording reactor trip or ESF actuations and protective relay actuations." "The NRC staff further noted that monthly PMS system health reports will be prepared by the PMS system engineer using data from the various internal PMS event logs including system operation and error tracking. If results from these reports indicate issues with any self-diagnostic functions, they will be further evaluated and dispositioned in accordance with the licensee's design control and corrective action programs. In cases where such issues affect the Common-Q diagnostic functions, these will be recorded for inclusion in the ABB Tracker system." "The NRC staff reviewed the SNC LAR supplement which provided a description of the on-going SNC Vogtle plant operations and maintenance personnel verification activities for the PMS system diagnostics and confirmed the SNC LAR supplement adequately incorporated the system self-check features and plant administrative activities necessary to assure adequate operation of the PMS Common-Q subsystem, and the PMS CIM/SRNC subsystem diagnostic functions credited in the SNC LAR."	Section 5.4 and LRA_8 were added via the topical report supplement to address this. See additional discussion in Items 1 and 2 of this comment resolution form.

No	Section Reference	Page	Comment	Westinghouse Responses
			" **On the basis of the NRC staff audit activities and supplemental information provided in the SNC LAR** supplement associated with incorporation of PMS self-diagnostic functions and plant administrative activities necessary to assure adequate operation of the PMS Common-Q subsystem, and the PMS CIM/SRNC subsystem self-diagnostic functions credited in the SNC LAR, the staff finds that these diagnostic functions credited in the SNC LAR, will be adequately evaluated using rigorous processes in accordance with Appendix B requirements, and provide reasonable assurance of continuous on-going detection of faults in the diagnostic functions of the PMS Common-Q subsystem and the CIM/SRNC subsystem."	
9	4.4	4 7	The description of MTP diagnostics and Annunciation relies on the existence of an ITP. Therefore, for systems that do not include ITPs, MTP diagnostic functions cannot be credited for surveillance elimination. If Westinghouse would like to credit MTP or OM diagnostics capabilities in absence of ITPs then additional information describing these functions without reliance on ITPs will be necessary. Otherwise, the approval will exclude surveillance elimination for any functional check that relies on MTP self-diagnostic functions for systems that do not use ITPs.	The following WCAP supplemental information was intended to address this comment (underlining added for emphasis): **LRA_1 –** Identification of where the licensee's plant-specific architecture deviates from the architecture described within Appendix A of this topical report, along with an analysis of the contrast between the two (e.g., an alternative to the ITP functions listed in this topical report if the licensee's architecture does not include an ITP). **LRA_7 –** When applying this WCAP, if the licensee's safety system architecture does not consist of an ITP, the licensee will need to provide a description of how failures identified by self-diagnostics will be reported to plant operators.
10	4.4	4 8	The description of CIM Fault Diagnostic Path relies on the existence of an ITP. Therefore, for systems that do not include ITPs, SIM diagnostic functions cannot be credited for surveillance elimination. If Westinghouse would like to credit CIM diagnostics capabilities in absence of ITPs then additional information describing these functions without reliance on ITPs will be necessary. Otherwise, the approval will exclude surveillance elimination for any functional check that relies on CIM self-diagnostic functions for systems that do not use ITPs.	See response to Comment 9.
11	Tables 5.1-1 through 5.1-6, 5.2-1, 5.2-2, 6.2 through 6.11	5 3 through 6 17	Most faults listed in these tables contain a reliance on the ITP for annunciation and several of the faults rely on the IPT for failure detection functions. For systems that do not contain ITPs alternate means of providing annunciation or fault detection must be provided. Will new tables be created for systems that do not have ITPs since these FMEDAs will clearly will not support such systems?	If a system didn't have an ITP (e.g., WF3 CPCS) the tables would need to be revised/augmented in a LAR to provide an alternative to the ITP.
12	Appendix B	B 1	There are four assumptions that clearly rely on presence of an ITP. While the first can be addressed by retaining manual channel check SRs, the remaining assumptions, though invalid for systems that have no ITP are unresolved. Provide additional information to explain how invalid assumptions in the appendix can be addressed for those systems for which no ITP will be included. PAMS, CPC, Diesel Sequencer stand-alone systems. Explain how the FMEDA tables would be used for these systems since they rely heavily on ITP functionality.	See above comment resolutions items regarding discussions of the ITP in the WCAP.

No	Section Reference	Page	Comment	Westinghouse Responses
13	Appendix B	B 3	When a stand-alone Diesel Load Sequencer system is installed, the appendix proposes elimination of existing channel check and replacing it with a channel operability check. If the system has an ITP, then why couldn't the ITP perform the same cross channel checks as is done for all other safety functions of the PMS? Will stand alone DLS system include an ITP?	See above comment resolutions items regarding discussions of the ITP in the WCAP. Note that the most recent Common Q implementation of a DLS included an ITP.
14	Appendix B 2 4	B 4	The Section titled, NUREG-1431 TADOT / NUREG-1432 Channel Functional Test (Trip Logic Tests) states the following: [ ]a,c 1) What specific surveillance test in the NUREGs will include performance of this test? 2) Shouldn't this also be an LRA in Appendix C?	3) Calibration is a likely choice by the licensee. 4) LRA_3 will be revised to state that the TS assumptions section of Appendix B should be reviewed to ensure they are being met when applying this WCAP. This update will state: "**LRA_3** – Identification of licensee's plant-specific functions that deviate from those within the applicable standard technical specifications (NUREG-1431/NUREG-1432) will need to be analyzed to remove the applicable SRs. The analysis/methodology in this topical report provides a framework for this task. Additionally, the licensee needs to ensure that the assumptions made regarding the TS in Appendix B.2 are met in the current licensing basis, otherwise necessary changes will need to be implemented."
15	Appendix D	D 2	The change to the definition of Channel Calibration will affect all instrumentation in the plant and not just the Common Q PMS or RPS or CPCS. Other systems may still require a more inclusive definition like the pre change version. There may also need to be more than one definition provided depending on the system. This fact should be explained somewhere such as in a LRA or a PSAI in the NRC safety evaluation.	The appendix markups are only there for information purposes, as stated in the leadup paragraph which states, "These markups are provided as a framework for how to markup TS based on the analyses provided within this topical report". There are other items that might not be applicable to the specific plant within the TS markups, but we wouldn't be able to account for all deviations within this topical report. Also note the following text from Appendix C "LRA_6: When applying this WCAP, the licensee needs to document that any existing interdependencies between surveillance requirements that may be impacted by the elimination of an SR is addressed in the technical specification bases."
16	3.5	3 4	Regarding the third bullet item on this page: 5) What specific hardware SDs are being referred to in the first sentence? 6) What specific supervisory tests are confirming functionality for which hardware SDs? 7) Are the [ ]a,c examples of hardware SDs or are they examples of supervisory tests of other hardware SDs? 8) Based on the first sentence, the [ ]a,c function seem to be hardware tests for which some supervisory tests are used to verify functionality. What another hardware-based SD does not have a corresponding supervisory test in place to verify functionality?	5) The parenthetical note in this sentence states that these self-diagnostics are the [ ]a,c 6) These are explained in the bulleted list on this page in the WCAP (Page 3-4) [ ]a,c 7) They are hardware self-diagnostics, but they are also monitored by test functions. 8) [ ]a,c