Westinghouse

Nuclear Safety Advisory Letter

This is a notification of a recently identified potential safety issue pertaining to basic components supplied by Westinghouse. This information is being provided so that you can conduct a review of this issue to determine if any action is required.

1000 Westinghouse Drive, Cranberry Township, PA 16066

Subject: **AC160 Processor Module Stall Timers Not Activated as Described in Licensing Basis**	Number: **NSAL-17-2**
Basic Component: AC160 Processor Modules	Date: July 5, 2017
Substantial Safety Hazard or Failure to Comply Pursuant to 10 CFR 21.21(a)	Yes ☐ No ☒ N/A ☐
Transfer of Information Pursuant to 10 CFR 21.21(b)	Yes ☐
Advisory Information Pursuant to 10 CFR 21.21(d)(2)	Yes ☐

SUMMARY

Westinghouse has discovered that a diagnostic feature known as "stall timers" used in the Asea Brown Boveri (ABB) Advant Controller 160 (AC160) processor module (PM), was not activated as described in the Westinghouse report on the common qualified (Common Q™[1]) platform (References 1 and 2). By design, this feature provides diagnostic functions following a severe software fault and is not required for the system to perform its safety-related functions. Despite that this feature had not been activated as intended, Westinghouse concluded that there is no impact to the safety-related function or operability of the affected safety systems.

Additional information, if required, may be obtained from Christopher Phillips, (860) 731-6309 or phillics@westinghouse.com

Author:	Reviewer:	Manager:
William J Smoody Regulatory Compliance	John S. Galembush Regulatory Compliance	James A. Gresham Regulatory Compliance
Verifier: Christopher S. Phillips Safety System Platforms	Verifier: Brandon M. Taylor Safety System Platforms	

[1] Common Q is a trademark of Westinghouse Electric Company LLC, its affiliates and/or its subsidiaries in the United States of America and may be registered in other countries throughout the world. All rights reserved. Unauthorized use is strictly prohibited. Other names may be trademarks of their respective owners.

ISSUE DESCRIPTION

The AC160 programmable logic controller is used to perform safety-related functions for multiple new and operating plant applications as listed in Table 1. The safety-related algorithms execute on the processing section of the PM, which is the main processor of the AC160 platform.

The PM was designed with four separate stall timers; sometimes known as watchdog timers:

1. Software stall timer (also known as the software watchdog timer or central processing unit [CPU] watchdog timer): internal to the microprocessor
2. Hardware stall timer (also known as the external hardware watchdog timer or external CPU watchdog timer): external to the microprocessor
3. Window watchdog timer: located on the processing section (PS) of the PM, external to the microprocessor, which controls the single watchdog timer relay
4. Window watchdog timer: located on the communication section (CS) of PM, external to the microprocessor, which controls the single watchdog timer relay

These timers serve to provide some level of annunciation in the event the PM encounters a severe software fault. As described in WCAP-16097-P-A, (References 1 and 2), when activated, the stall timers (1 and 2, above) reset the PM and display a diagnostic code on the front of the PM. The independent window watchdog timers (3 and 4, above) also actuate a watchdog timer relay which is available on the front of the PM for project-specific use. In general, the watchdog timer relay is used for annunciation of a PM failure or for partial reactor trip, depending on the specific application.

Westinghouse discovered that the software stall timer (1) was never activated in the AC160 base software designed by ABB. Based on the base software implementation, the inactivated software stall timer (1) also disabled the hardware stall timer (2); therefore, both stall timers were not activated, even though the window watchdog timers (3 and 4) remain fully functional. The window watchdog timers are a diverse and non-software based watchdog that will actuate for the same and other severe software faults that the stall timers (1 and 2) would respond to, but will not reset the PM. It is these window watchdog timers that were credited for closing Generic Open Item 7.3 in Reference 1. This is documented in U.S. Nuclear Regulatory Commission (NRC) Document ML030550776 (Reference 3) page 13, Item 3.

This issue affects both variants of ABB processor modules PM646A and PM646B; however, PM646B is not described in the Common Q topical report (References 1 and 2). In applications that use redundant PM646B PMs, the PM voter will detect a severe software fault and automatically switch to the redundant PM.

TECHNICAL EVALUATION

If the software stall timer was activated, the PM would respond to a severe software fault, such as an endless loop with all interrupts disabled. This would occur as follows: The software stall timer would halt the application and then restart the PM where it would display a diagnostic code '09' on the PM seven-segment display. In addition, the PM would cease to transmit data on all communication channels which would be detected by each PM in communication with the failed module. The affected PMs would indicate a failure of the communication link and this would alert the operator. When investigated, this would lead to the failed PM. The failed PM hardware stall timer would actuate causing a hard-wired reset of the processor and the window watchdog timers would also timeout and actuate the watchdog timer relay.

Because the software stall timer was not activated, the PM instead responds to severe software fault as follows: The PM ceases to transmit data on all communication channels which would be detected by each

PM in communication with the failed module. Communication ceases because a software fault that would cause the software stall timer to respond (if activated) would also cease communication from the PM. Communication tasks are initiated by the operating system. The same task that initiates system tasks, communication tasks, or application tasks also resets the stall timer. If that task is prevented from resetting the stall timer, then the system tasks, communication tasks, and applications tasks are also halted. The receiving PMs indicate a failure of the communication link and this alerts the operator. When investigated, this would lead to the failed PM. The window watchdog timers also timeout and actuate the watchdog timer relay. The PM continues to display the normal operating 'P1' state and will not automatically restart.

The difference between "activated" and "not-activated" stall timers is that when not activated a diagnostic code '09' would not be displayed on the PM seven segment display to aid in the troubleshooting of the condition. In addition, the PM does not automatically halt the application and restart the PM to the error state. Neither the diagnostic error code nor the automatic halt and restart functions are necessary for the overall system to respond to this or to other similar abnormal situations, nor are these required for the overall system to perform its safety function. The diagnostic code is below the level of detail needed for normal plant operation. It is not needed by plant operators to react to a severe software fault, only for further diagnosis and troubleshooting.

SAFETY SIGNIFICANCE

Westinghouse concluded that the not-activated stall timers do not impact the overall safety function of the systems identified in Table 1 and the affected plants can continue to operate. Westinghouse has reviewed each application of the AC160. In each case, the operator and/or system would be made aware of a severe software fault that would have caused the stall timers to respond (if activated), either because the application monitors the watchdog timer relay (actuated by the window watchdog timers) or by a loss of communication from the failed PM. If the stall timers were activated, they would only provide diagnostic information if the PM encountered a severe software fault. The not-activated stall timers do not prevent the system from performing any safety-related function, nor impact the timing of any safety-related functions.

AFFECTED PLANTS

The safety-related systems listed are affected by this issue.

Table 1

Plant	System
A.W. Vogtle Units 3 & 4 Haiyang Units 1 & 2 Sanmen Units 1 & 2 V.C. Summer Units 2 & 3	PMS: protection and safety monitoring system
Dungeness B (Reactors 21 & 22)	BFZC: boiler feed zone control RZC: reactor zone control RSU: reactor start up LOW S/H: low superheat trip and feed valves GAG: gag movement supervision PDS: primary display system, alarms and indications. (conventional display tableau)
Beznau Units 1 & 2 (AUTANOVE project)	For each of the reactors, two Category A diesel sequencers
Calvert Cliffs Units 1 & 2 Krsko Unit 1 Watts Bar Unit 2	PAMS: post-accident monitoring system
Palo Verde Units 1, 2, & 3	CPCS: core protection calculator system

Plant	System
Shin-Kori Units 1 & 2 Shin-Wolsong Units 1 & 2	CPCS DPPS: digital plant protection system DESFAS-AC: digital engineered safety features actuation system–auxiliary cabinet
A.W. Vogtle Units 1 & 2	SFS: safety features sequencer
Barakah Units 1, 2, 3, & 4 Shin-Kori Units 3 & 4	PPS: plant protection system ESF-CCS: engineered safety features-component control system QIAS-P: qualified indication and alarm system-PAMI CPCS
Hanul (Ulchin) Units 5 & 6	DPPS DESFAS-AC
Oskarshamn Unit 1 Ringhals Unit 2	RPS: reactor protection system

NRC AWARENESS

Westinghouse has not notified the NRC about this issue.

RECOMMENDED ACTIONS

Westinghouse is planning a Common Q topical report revision that will remove reference to the inactive stall timers. Westinghouse recommends that affected plants review their licensing basis to determine if reference is made to these stall timers specifically, or to the Common Q topical report (References 1 and 2) generally. If so, Westinghouse recommends either taking exception to this feature or updating the licensing basis by citing the revised topical report after it is approved by the NRC. At this time, Westinghouse does not have a timeline for the submittal of the revised Common Q topical report to the NRC.

Westinghouse also recommends that affected plants review their failure modes and effects analysis to determine if the inactive stall timers are referenced as mitigation for a failure. If so, Westinghouse recommends referring to one or more of the other means of detecting a PM failure, such as the watchdog timer relay, communication heartbeats to other PMs, and other monitored communication from the PM as mitigation for that failure.

If an affected plant believes their PM has encountered a severe software fault but continues to display the diagnostic code 'P1,' Westinghouse recommends verifying if the watchdog timer relay normally closed contacts have opened. If so, reset the PM manually using the reset button. If the problem persists, replace the PM with a spare.

REFERENCES

1. Westinghouse Report WCAP-16097-P-A, Revision 0, "Common Qualified Platform Topical Report," May 2003
2. Westinghouse Report WCAP-16097-P-A, Revision 3, "Common Qualified Platform Topical Report," February 2013
3. NRC Document ML030550776, "Acceptance of the Changes to Topical Report CENPD-396-P, Rev. 01, 'Common Qualified Platform,' and Closeout of Category 2 Open Items (TAC No. MB2553)"