ENCLOSURE 4

WCAP-17201-NP

Revision 0

"AC160 Hugh Speed Link Communication Compliance to DI&C-ISG-04 Staff Positions 9, 12, 13 and 15 Technical Report"

(Non-Proprietary)

Westinghouse Non-Proprietary Class 3

WCAP-17201-NP
APP-GW-GLR-149
Revision 0

February 2010

AC160 High Speed Link Communication Compliance to DI&C-ISG-04 Staff Positions 9, 12, 13 and 15 Technical Report

Westinghouse

WCAP-17201-NP
APP-GW-GLR-149
Revision 0

AC160 High Speed Link Communication Compliance to DI&C-ISG-04 Staff Positions 9, 12, 13 and 15 Technical Report

Warren R. Odess-Gillett*
Safety Systems Platform Configuration Management

February 2010

Reviewer: Thomas J. McLaughlin*
Common Q Software Applications II

Approved: John S. Strong*, Program Manager
NuStart/DOE Design Finalization

*Electronically approved records are authenticated in the electronic document management system.

Westinghouse Electric Company LLC
P.O. Box 355
Pittsburgh, PA 15230-0355

REVISION HISTORY

RECORD OF CHANGES

Revision	Author	Description
0	Warren R. Odess-Gillett	Initial issue

TABLE OF CONTENTS

REVISION HISTORY ii

TABLE OF CONTENTS iii

ACRONYMS AND TRADEMARKS iv

DEFINITIONS v

REFERENCES vi

1 INTRODUCTION 1-1
1.1 PURPOSE 1-1
1.2 SCOPE 1-1
2 HSL COMPLIANCE TO ISG-4, POSITIONS 9, 12, 13 AND 15 2-1
2.1 ISG-4, POSITION 9 2-1
2.2 ISG-4, POSITION 12 2-2
2.3 ISG-4, POSITION 13 2-5
2.4 ISG-4, POSITION 15 2-5

ACRONYMS AND TRADEMARKS

Acronyms used in the document are included below to ensure unambiguous understanding of their use within this document.

Acronym	Definition
ABB	Asea Brown Boveri
AC160	ABB Advant® Controller Series 160
CRC	Cyclic Redundancy Check
CS	Communication Section
DCD	Design Control Document
HSL	High Speed Link
I&C	Instrumentation and Control
I/O	Input/Output
ISG	Interim Staff Guidance
NRC	U.S. Nuclear Regulatory Commission
PM646A	Processor Module 646A
PS	Processor Section
RAM	Random Access Memory
SER	Safety Evaluation Report

Advant® is a registered trademark of ABB Process Automation Corporation.

AP1000™ is a trademark of Westinghouse Electric Company LLC.

All other product and corporate names used in this document may be trademarks or registered trademarks of other companies, and are used only for explanation and to the owners' benefit, without intent to infringe.

DEFINITIONS

Term	Definition
Common Q	Common Qualified Platform (see Reference 3)

REFERENCES

1. ML083310185 , "Interim Staff Guidance, Digital Instrumentation and Controls, DI&C-ISG-04, Task Working Group #4, Highly-Integrated Control Rooms – Communications Issues (HICRc)," U.S. Nuclear Regulatory Commission, September 2007.

2. ML092800251, "Letter – Safety Evaluation Report With Open Items For Chapter 7, 'Instrumentation And Control,'" of NUREG-1793, Supplement 2 – AP1000 Design Certification Amendment, October 23, 2009.

3. WCAP-16097-P-A (Proprietary), Rev. 0, "Common Qualified Platform Topical Report," Westinghouse Electric Company LLC.

1 INTRODUCTION

1.1 PURPOSE

In October 2009, the U.S. Nuclear Regulatory Commission (NRC) staff issued the safety evaluation report (SER) with open items (ML092800251, "Letter – Safety Evaluation Report With Open Items For Chapter 7, 'Instrumentation And Control'" [Reference 2]) for Revision 17 of the AP1000 design control document (DCD), Chapter 7. In that SER, the NRC staff evaluated the Common Q high speed link (HSL) communication to the twenty criteria (positions) identified in interim staff guidance #4 (ISG-4) (ML083310185, "Interim Staff Guidance, Digital Instrumentation and Controls, DI&C-ISG-04, Task Working Group #4, Highly-Integrated Control Rooms – Communications Issues (HICRc)" [Reference 1]). Of the 20 criteria, the NRC found sufficient information in WCAP-16097-P-A, "Common Qualified Platform Topical Report" (Reference 3) to assess that 16 of the criteria have been met. They requested additional information to determine whether the four remaining criteria (Positions 9, 12, 13 and 15) have been met. This request was identified as open issue OI-SRP-7.9-ICE-01 in the SER. The purpose of this report is to augment the information that is in the Common Q topical report (Reference 3) in order for the NRC staff to conclude that these four positions are satisfied.

1.2 SCOPE

The scope of this report is to address how the HSL communication described in the Common Q Topical Report (Reference 3) is compliant with ISG-4 Positions 9, 12, 13 and 15.

2 HSL COMPLIANCE TO ISG-4, POSITIONS 9, 12, 13 AND 15

2.1 ISG-4, POSITION 9

ISG-4, Position 9 states:

> "Incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor. These memory locations should not be used for any other purpose. The memory locations should be allocated such that input data and output data are segregated from each other in separate memory devices or in separate pre-specified physical areas within a memory device"

Specifically, the AP1000 Chapter 7 SER (Reference 2) states that insufficient information exists in the Common Q Topical Report (Reference 3) in the following area to conclude that Position 9 is met:

> "The AP1000 DCD and its referenced documents have not specified whether the incoming message data is stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor."

HSL Compliance

[

]a, c

2.2 ISG-4, POSITION 12

ISG-4, Position 12 states:

"Communication faults should not adversely affect the performance of required safety functions in any way. Faults, including communication faults, originating in nonsafety equipment, do not constitute 'single failures' as described in the single failure criterion of 10 C.F.R. Part 50, Appendix A. Examples of credible communication faults include, but are not limited to, the following:

- Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise.
- Messages may be repeated at an incorrect point in time.
- Messages may be sent in the incorrect sequence.
- Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message.
- Messages may be delayed beyond their permitted arrival time window for several reasons, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages.
- Messages may be inserted into the communication medium from unexpected or unknown sources.
- Messages may be sent to the wrong destination, which could treat the message as a valid message.
- Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.
- Messages may contain data that is outside the expected range.
- Messages may appear valid, but data may be placed in incorrect locations within the message.
- Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm).
- Message headers or addresses may be corrupted."

Specifically the AP1000 Chapter 7 SER (Reference 2) states that insufficient information exists in the Common Q Topical Report (Reference 3) in the following area to conclude the Position 12 is met:

> "The AP1000 DCD, and the supporting technical reports, along with the Common Q topical report have not specified whether the messages will be checked to ensure validity of the message (e.g., repeated messages or messages out of sequence.)"

HSL Compliance

Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise.

[

]^{a,c}

Messages may be repeated at an incorrect point in time.

[

]$^{a, c}$

Messages may be sent in the incorrect sequence.

[

]$^{a, c}$

Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message.

[

]$^{a, c}$

Messages may be delayed beyond their permitted arrival time window for several reasons, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages.

[

]$^{a, c}$

Messages may be inserted into the communication medium from unexpected or unknown sources.

[

]a, c

Messages may be sent to the wrong destination, which could treat the message as a valid message.

[

]a, c

Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.

[

]a, c

Messages may contain data that is outside the expected range.

[

]a, c

Messages may appear valid, but data may be placed in incorrect locations within the message.

[

]a, c

Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm).

[

]a, c

Message headers or addresses may be corrupted.

[

]a, c

2.3 ISG-4, POSITION 13

ISG-4, Position 13 states:

> "Vital communications, such as the sharing of channel trip decisions for the purpose of voting, should include provisions for ensuring that received messages are correct and are correctly understood. Such communications should employ error-detecting or error-correcting coding along with means for dealing with corrupt, invalid, untimely or otherwise questionable data. The effectiveness of error detection/correction should be demonstrated in the design and proof testing of the associated codes, but once demonstrated is not subject to periodic testing. Error-correcting methods, if used, should be shown to always reconstruct the original message exactly or to designate the message as unrecoverable. None of this activity should affect the operation of the safety-function processor."

HSL Compliance

[

]a, c

2.4 ISG-4, POSITION 15

ISG-4, Position 15 states:

> "Communication for safety functions should communicate a fixed set of data (called the 'state') at regular intervals, whether data in the set has changed or not."

Specifically, the AP1000 Chapter 7 SER (Reference 2) states that insufficient information exists in the Common Q Topical Report (Reference 3) in the following area to conclude the Position 15 is met:

> "As specified in the Common Q topical report, the staff finds that, although the processing section of the PM646 for performing the safety function operates cyclically, the communication section of the PM646 is event driven, and as such does not communicate a fixed set of data at regular intervals."

HSL Compliance

[

]a, c