

Westinghouse Non-Proprietary Class 3

WCAP-17266-NP
Revision 0

August 2010

Common Q Platform Generic Change Process



WCAP-17266-NP
Revision 0

Common Q Platform Generic Change Process

William J. Catullo, Jr.*
Regulatory Compliance & Plant Licensing

August 2010

Reviewer: Matthew A. Shakun*
Safety Systems Platform Configuration Management

Approved: Mark J. Stofko*, Manager
Safety Systems Platform Configuration Management

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

LIST OF CONTRIBUTORS/REVIEWERS

Rev	Name and Title	Date
0	Matthew A. Shakun Engineer, Safety Systems Platform Configuration Management	August 2010
0	Warren R. Odess-Gillett Fellow Engineer, Safety Systems Platform Configuration Management	August 2010
0	Christine P. Scardina-Gazzo Project Manager, Reactor Protection Systems IV	August 2010
0	Richard M. Manazir, Jr. Technical Program Manager, Maintenance	August 2010
0	Mark J. Stofko Manager, Safety Systems Platform Configuration Management	August 2010
0	Martin P. Ryan Principal Engineer, Safety Systems Platform Configuration Management	August 2010
0	Jenna L. Tyger Technical Editor, Technical Communications	August 2010

REVISION HISTORY**RECORD OF CHANGES**

Revision	Revision Made By	Description	Date
0	William J. Catullo, Jr.	Original Issue	See EDMS

DOCUMENT TRACEABILITY & COMPLIANCE

Created to Support the Following Document(s)	Document Number	Revision
N/A		

OPEN ITEMS

Item	Description	Status
None.		

DETAILED RECORD OF CHANGES**Revision 0****August 2010****Description:**

This is the original issue of this document.

TABLE OF CONTENTS

LIST OF FIGURES	vi
LIST OF ACRONYMS AND TRADEMARKS.....	vii
1 PURPOSE	1-1
2 SCOPE	2-1
3 GENERIC CHANGE PROCESS	3-1
3.1 OVERALL PROCESS	3-3
3.1.1 Screening Process	3-3
3.1.2 Evaluation Process.....	3-4
3.2 IMPLEMENTATON	3-5
3.2.1 Design Process – Hardware.....	3-5
3.2.2 Design Process – AC160 Platform Software.....	3-6
3.2.3 Design Process – QNX® Platform Software.....	3-6
4 REPORTING	4-1
5 REFERENCES	5-1

LIST OF FIGURES

Figure 3-1	Common Q Generic Change Process Flow Diagram.....	3-2
Figure 3-2	Hardware Design Process Cross-Functional Diagram.....	3-8
Figure 3-3	Example – Modified [] ^{a,c}	3-9
Figure 3-4	AC160 Platform Software Design Process Cross-Functional Diagram.....	3-11
Figure 3-5	QNX Platform Software Design Process Cross-Functional Diagram.....	3-12

LIST OF ACRONYMS AND TRADEMARKS

The following abbreviations and acronyms are defined below to allow an understanding of their use within this document.

Acronym	Definition
ABB	Asea Brown Boveri
AC160	Advant [®] Controller 160
ATR	Approved Topical Report
CCB	Change Control Board
[] ^{a,c}
Common Q	Common Qualified
[] ^{a,c}
EMC	Electromagnetic Compatibility
FMEA	Failure Modes and Effects Analysis
GOI	Generic Open Item
LAR	License Amendment Request
NRC	Nuclear Regulatory Commission
NRR	Office of Nuclear Reactor Regulation
PSAI	Plant-Specific Action Item
QSSKG	QNX [®] Software Systems GmbH & Co. KG
RAI	Request for Additional Information
SER	Safety Evaluation Report
SPM	Software Program Manual
SSPCM	Safety System Platform Configuration Management
SSPE	Safety System Platform Engineering
V&V	Verification and Validation

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

QNX[®] is a registered trademark of QNX Software Systems GmbH & Co. KG (“QSSKG”) and is used under license by QSS.

All other products 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.

1 PURPOSE

Managing changes to a safety system platform after the initial U.S. Nuclear Regulatory Commission (NRC) Safety Evaluation Report (SER), and how these changes are reviewed by the NRC in a timely fashion, has been a topic of concern over the past several years especially for digital software-based safety systems. The Westinghouse Common Qualified (Common Q) Platform received its SERs from the NRC's Office of Nuclear Reactor Regulation (NRR) that encompassed a) the Topical Report including closeout of generic open items (GOIs) in February 2003 (Reference 1), and b) the Software Program Manual in September 2004 (Reference 3). Since this time, Westinghouse has been managing platform changes [

] ^{a,c}. Any plant-specific action items (PSAIs) listed in the Approved Topical Report SER have been addressed in customer license amendment requests (LARs).

In order to better manage the approval of platform changes, a Common Q Platform Generic Change Process has been developed to permit implementation of changes to the platform that have [

] ^{a,c}. This process will consist of various screening and evaluation criteria that will be assessed early in the design phase to determine if the platform change [

] ^{a,c} on a safety system project during the plant installation phase.

2 SCOPE

The scope of the Common Q Platform Generic Change Process includes those changes (modifications or new additions) that affect the standard Common Q platform. Plant-specific changes (by either Westinghouse or end-users) are []^{a,c}.

3 GENERIC CHANGE PROCESS

The Common Q Generic Change Process will address changes affecting either the []^{a,c}. Specifically, the Common Q Generic Change Process will address changes in the following areas:
[

] ^{a,c}

Figure 3-1 illustrates the various assessment, decision, and documentation steps involved in the Common Q Generic Change Process.

a,c

Figure 3-1 Common Q Generic Change Process Flow Diagram

3.1 OVERALL PROCESS

3.1.1 Screening Process

As detailed in Figure 3-1, when a change is initiated on the Common Q Platform, it is assessed against predefined screening criteria depending on whether or not it is a []^{a,c} change. If the change does not meet specific screening criteria, it “screens-out”; that is, []

[]^{a,c}. The basis for this assessment shall be verified, approved, and documented such that it can []^{a,c}.

If the change meets specific screening criteria, it “screens-in” and is further assessed to determine if it meets predetermined criteria that would []^{a,c} during the plant installation phase. If it does, then a change summary shall be prepared and included in a []^{a,c}. If the change “screens-in,” but does not []^{a,c}, then a detailed engineering analysis (evaluation) shall be performed to determine if the change requires []^{a,c}.

Screening Criteria – []^{a,c}

If the change affects the []^{a,c} or involves a []^{a,c}, then a detailed engineering analysis shall be performed.

Screening Criteria – []^{a,c}

Due to the complex, interdependent nature of software modifications, []^{a,c} shall be further evaluated to determine if the change []^{a,c}.

Screening Criteria – []^{a,c}

[]^{a,c} and shall be evaluated to determine if the change []^{a,c}, including: []

[]^{a,c}

Screening Criteria – []^{a,c}

The following criteria shall be used to determine if the platform change shall []^{a,c}

[

] ^{a,c}

3.1.2 Evaluation Process

If the platform change “screened-in,” does not meet the [^{a,c}, and the detailed engineering analysis (evaluation) does not meet [^{a,c}; that is, the change [^{a,c}. The basis for this assessment shall be verified, approved, and documented such that it can [^{a,c}.

If the change meets specific evaluation criteria, it [^{a,c} and a change summary shall be prepared and included in [^{a,c}, and listed in the [^{a,c}.

Evaluation Criteria – [^{a,c}

If the detailed engineering analysis identifies any [^{a,c} the following, then the platform change shall be [^{a,c}.
[

] ^{a,c}

Evaluation Criteria – []^{a,c}

If the []^{a,c} identifies that the software change []^{a,c}, then the change shall be []^{a,c}.

Evaluation Criteria – []^{a,c}

If the evaluation of []^{a,c} identifies any []^{a,c} that []^{a,c}, then the change shall be []^{a,c}.

It is important to ensure that the []^{a,c} remains a []^{a,c} and that improvements are not []^{a,c} in order to []^{a,c} requiring NRC approval. Therefore, additional []^{a,c} shall be applied to changes affecting the []^{a,c} as follows:

[]^{a,c}

3.2 IMPLEMENTATON

The Common Q Generic Change Process should be closely integrated with the []^{a,c} in order ensure that:

[]^{a,c}

3.2.1 Design Process – Hardware

Figure 3-2 is a cross-functional flow chart that depicts the current Common Q Platform hardware design process along with the responsible safety system functional discipline tasked with each action as shown in black (solid lines). The additional actions associated with the Common Q Generic Change Process are shown in red (dashed lines).

When a hardware change is required, it is first []^{a,c} and then a []^{a,c} is performed. In order to evaluate the change in terms of its impact on the []^{a,c}, an additional task shall be added such that the Safety System Platform Configuration Management (SSPCM) function assesses the hardware change against the []^{a,c}. This will ensure that decisions and/or evaluations regarding the change take into account its []^{a,c} in the hardware design process.

When the change reaches the []^{a,c} approval stage, the SSPCM function shall ensure (by means of approval of the []^{a,c} that the final design that implements the change has been properly assessed for any []^{a,c} before it is released for manufacturing. Figure 3-3 illustrates an example of how a []^{a,c} can be integrated into the existing []^{a,c} that provides a simple, straightforward means to ensure that the various platform hardware screening and evaluation criteria are considered or addressed prior to the approval of the change.

In addition, the SSPCM function shall update the platform's []^{a,c} such that it can support either an []^{a,c} sometime in the future.

3.2.2 Design Process – AC160 Platform Software

Figure 3-4 is a cross-functional flow chart that depicts the current Common Q Platform AC160 software design process along with the responsible safety system functional discipline tasked with each action as shown in black (solid lines). The additional actions associated with the Common Q Generic Change Process are shown in red (dashed lines).

When an AC160 platform software change is being considered []^{a,c}, the Supplier []^{a,c} the issue and then generates an associated []^{a,c}. The Safety System Platform Engineering (SSPE) function meets []^{a,c} with the Supplier (Asea Brown Boveri {ABB}) to []^{a,c}. Those AC160 platform software changes that are deemed []^{a,c} are reviewed and discussed in detail by the Westinghouse []^{a,c}. In order to evaluate the change in terms of its impact on the Common Q Platform []^{a,c}, an additional task shall be added such that the SSPCM function assesses the software change against the []^{a,c}. This will ensure that decisions and/or evaluations regarding the change take into account its []^{a,c} in the software design process.

[]^{a,c} of the AC160 platform software change is then performed. SSPCM shall provide []^{a,c} before the Supplier finalizes the []^{a,c}. When the software revision is []^{a,c}, SSPE prepares a []^{a,c}, which now shall require []^{a,c} by the SSPCM function to ensure that final software design properly []^{a,c}.

The SSPCM function shall also update the platform's []^{a,c} such that it can support either an []^{a,c} sometime in the future.

3.2.3 Design Process – QNX® Platform Software

Figure 3-5 is a cross-functional flow chart that depicts the current Common Q Platform QNX software design process along with the responsible safety system functional discipline tasked with each action as shown in black (solid lines). The additional actions associated with the Common Q Generic Change Process are shown in red (dashed lines).

When a QNX platform software change is being considered, the Supplier (QNX Software Systems GmbH & Co. KG {QSSKG}) []^{a,c}. The SSPE function meets []^{a,c} with the Supplier to []^{a,c}. Those QNX platform software changes that are deemed []^{a,c} are reviewed and discussed in detail by the Westinghouse []^{a,c}. In order to evaluate the change in terms of its impact on the Common Q Platform []^{a,c}, an additional task shall be added such that the SSPCM function assesses the software change against the []^{a,c}. This will ensure that decisions and/or evaluations regarding the change take into account its []^{a,c} in the software design process.

The SSPE function then determines if []^{a,c} to address the software issue. If a []^{a,c}, then SSPE will first assess then []^{a,c}. If a []^{a,c} does not exist, the Supplier will prepare a []^{a,c}, and then SSPE will []^{a,c} and prepare a []^{a,c}. The []^{a,c} shall require []^{a,c} by the SSPCM function to ensure that final software design properly []^{a,c}.

The SSPCM function shall also update the platform's []^{a,c} such that it can support either an []^{a,c} sometime in the future.

Figure 3-2 Hardware Design Process Cross-Functional Diagram

Figure 3-3 Example – Modified []^{a,c}

a,c

Figure 3-3 Example – Modified [**] ^{a,c} (cont.)**



Figure 3-4 AC160 Platform Software Design Process Cross-Functional Diagram



Figure 3-5 QNX Platform Software Design Process Cross-Functional Diagram

4 REPORTING

In order to keep the NRC []^{a,c} in an appropriate

[]^{a,c}, the []^{a,c} shall, at a minimum, be []

[]^{a,c} if both of the following situations have occurred:

[]^{a,c}

5 REFERENCES

Following is a list of references used throughout this document. Unless stated otherwise, the latest revision is applicable.

1. NRC Safety Evaluation Report, "Safety Evaluation by the Office of Nuclear Reactor Regulation Related to the Westinghouse Common Qualified Platform Closeout of Generic Open Items and Approve Changes to Topical Report CENPD-396-P, Rev. 01, Common Qualified Platform," February 24, 2003.
2. WCAP-16097-P-A, Rev. 0, "Common Qualified Platform Topical Report," including Appendices 1, 2, 3, 4, Westinghouse Electric Company LLC, May 2003.
3. NRC Safety Evaluation Report, "Final Safety Evaluation for Topical Report WCAP-16096-NP-A, Revision 1, "Software Program Manual for Common Q Systems" (TAC NO. MC2294)", September 28, 2004.
4. WCAP-16096-NP-A, Rev. 1A, "Software Program Manual for Common Q Systems," Westinghouse Electric Company LLC, December 2004.