Lockheed Martin Missiles and Fire Control
459 Kennedy Drive, Archbald, Pennsylvania 18403

LOCKHEED MARTIN

August 15, 2013

PROJ 780

Document Control No.: NS-LTA-2013-000059-0

Document Control Desk
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555-0001

Subject: Lockheed Martin Responses to Requests for Additional Information Dated May 15, 2013; Number 3, Item 8. (TAC NO. ME7900)

Dear Mr. Holonich,

By letter dated June 28, 2011, (Agencywide Documents Access and Management System Accession No. ML11201A323), Lockheed Martin Nuclear Systems and Solutions (LMNSS) and State Nuclear Power Automation Systems (SNPAS) submitted Topical Report NuPAC_ED610000-47-P titled "Generic Qualification of the NuPAC Platform for Safety-Related Application" (Proprietary). By letter dated May 15, 2013, the US NRC transmitted Requests for Additional Information (RAI's) to Lockheed Martin for action and response. Attached is Lockheed Martin's response to RAI Number 3 Item Number 8 for US NRC consideration.

If you have any questions related to the attached responses, please contact me at 570-803-2123 at your earliest convenience.

Sincerely,

Patrick J. Troy
Program Licensing Manager
Lockheed Martin
Nuclear Systems and Solutions

D100

PROGRAM NAME: **Cooperative Development of SPRPS and RPS**
DOCUMENT TYPE: **Program Plan (PPL)**
DOCUMENT TITLE: **Software Tool Evaluation Plan**
REFERENCE NUMBER(S): **Contract Number 10HT10500000163**

RELEASE DATE: 08/01/2013
Public Release Authorization per PIRA DAL201306007

Lockheed Martin Global, Inc.
459 Kennedy Drive
Archbald, PA 18403-1598, USA

State Nuclear Power Automation
System Engineering Company
No. 41 Hongcao Road
Shanghai, 200233, PRC

Document Summary:
This document applies to the Lockheed Martin Global Inc. (LMGI) Nuclear Protection and Control (NuPAC) Safety System Software Development effort. The document defines a process for evaluating software tools used in support of development of Safety System Software configuration items (i.e. Programmable Logic and Computer Software Configuration Items) in association with this project. The Programmable Logic/Software Lead is responsible for the preparation and revision management of this document.

TBD/Open Items

To be determined (TBD) and open item information for the program are listed below. This table will contain a listing and description of items that were TBD at time of generation and/or review.

Paragraph	Description	RESPONSIBLE

Revision History

Revision information for the Software Tool Evaluation Plan is listed below. This table will contain a listing and description of changed paragraphs for each succeeding revision.

Revision	Date	Paragraph	Description of Change
-	05/18/2011	All	RELEASE AUTH: ER.2011.03273
A	07/24/2012	All	RELEASE AUTH: ER.2012.02773
			Numerous changes to make the document more generic to cover both Programmable Logic (PL) and Software. Changes also made to incorporate comments from peer reviews both internal and external.
B	08/01/2013		RELEASE AUTH: ER.2013.05303
		1.0	Clarified scope wording
		4.0	Clarified wording, grammatical corrections

TABLE OF CONTENTS

1.0 SCOPE

The process of design, development, test and maintenance of Safety System Software requires the use of support software tools. These tools facilitate software lifecycle activities such as requirements management, architecture and design, code/test and compilation, thereby reducing the amount of time needed to perform these activities. This list of tools also includes those used in configuration management and version control of the Safety System Software. The purpose of this Software Tool Evaluation Plan is to provide the Nuclear Power and Control (NuPAC) program personnel, and those monitoring adherence to process, sufficient confidence that software tools used on the program can serve their intended purposes without negative impact to the final product. Any references to Safety System Software in this document shall mean both Programmable Logic Configuration Items (PLCIs) and Computer Software Configuration Items (CSCIs).

The tools used by the Independent Verification and Validation (I-V&V) team are evaluated in accordance with the independent team's plans.

2.0 INTRODUCTION

The evaluation process must show evidence that the tool will not negatively affect the integrity of design, development or build outputs. Nuclear Regulatory Commission (NRC) Regulatory Guide 1.168, §6.0 states "Tools used in the development of Safety System Software should be handled according to IEEE Std. 7-4.3.2-2003 which defines "software tools" as:

> "a computer program used in the development, testing, analysis, or maintenance of a program or its documentation. Examples include comparator, cross-reference generator, decompiler, driver, editor, flowcharter, monitor, test case generator, and timing analyzer."

IEEE Std 7-4.3.2-2003 further states that:

> "V and V tasks of witnessing, reviewing, and testing are not required for software tools, provided the software that is produced using the tools is subject to V&V activities that will detect flaws introduced by the tool."

Per IEEE Std 7-4.3.2-2003, Paragraph 5.3.2, Software Tools:

- "Used to support software development processes and V and V activities shall be controlled under configuration management."
- "One or both of the following methods shall be used to confirm the software tools are suitable for use:"
  - A test tool validation program shall be developed to provide confidence that the necessary features of the software tool function as required.
  - The software tool shall be used in a manner such that defects not detected by the software tool will be detected by the program V and V activities.
- "Tool operating experience may be used to provide additional confidence in the suitability of a tool, particularly when evaluating the potential for undetected defects."

As it applies to the approach defined in this plan, software tools are computer based programs used to facilitate software lifecycle activities associated with the design, development, test and maintenance of Safety System Software regardless of whether that software product is PLCI or a CSCI. Although tools used in the development of programmable logic do not produce the same outputs as software development tools (i.e. hardware layout as opposed to a software executable), they are nevertheless software based. This approach aligns with the NRC's position, which categorizes software, firmware and programmable logic as common software developed from software based development systems. This implies that they should be treated in a similar fashion. Our approach would also include in-house lifecycle development processes designed to catch defects early in the development phase augmenting the I-V&V activities. The approach outlined in this plan will utilize elements of both methods referenced in IEEE Std 7-4.3.2-2003.

3.0 REFERENCES

Document #	Description
Regulatory Guide 1.168	Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
IEEE Std. 7-4.3.2-2003	IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations
NuPAC_PLCMP61000-001	Programmable Logic – Configuration Management Plan
NuPAC_PLPMP610000-001	NuPAC Programmable Logic Project Management Plan

4.0 EVALUATION PROCESS

As stated earlier, the purpose of this process is to provide confidence that the necessary features of the software tools function as required. The process will also reference the V and V, I-V&V and CI development process activities necessary to detect defects not detected by the software tool. The following conditions apply to the evaluation process:

- The tool under evaluation is commercial-off-the shelf (COTS) software. This evaluation is not applicable to software tools developed in-house. In-house developed software tools require a software development plan.

- Personnel performing this evaluation are knowledgeable in software-based tools and the design and development of Safety System Software.

The conduct of the evaluation is the responsibility of the Lead (or their designee) of the Integrated Product Team (IPT) that uses the tool to perform activities related to their IPT. It is expected that, at a minimum, the following program plans will be updated with the software tools used by the IPT and/or any associated procedures/processes to be executed by the IPT.

- Applicable IPT Configuration Management Plan
- System and Software Quality Assurance Plan
- Applicable IPT Project Management Plan

Process Steps:

1. Identify the software tool and version to be evaluated.
2. Determine its intended purpose in the lifecycle of the Safety System Software item.
3. Ensure the applicable IPTs program plans have been updated to identify the software tool and version.
4. Ensure the applicable IPTs program plans have been updated to identify any procedures/processes to be executed by the IPTs in association with the use of the tool.
5. Determine if the tool needs to undergo evaluation (If the answer is Yes to any of the questions below, the tool requires evaluation);
    a. Criteria
        i. Is the tool used to create or modify source code for the Safety System Software (e.g. Integrated Development Environment, compilers, debuggers, code editors, place and route tools, synthesis tools)?
        ii. Is the tool used to conduct/support Verification and Validation of the Safety System Software?
        iii. Does the tool have the ability to impact the run time execution (e.g. Integrated Development Environment, compilers, debuggers, code editors, place and route tools, synthesis tools)?
        iv. Does the tool simulate other Safety System Software components that interface with the safety system software under development/test?
        v. Does the tool simulate any component of the target environment in which the Safety System Software executes?

vi. Does the output of the tool impact requirements that drive the design, development and test phases of the software lifecycle?

6. If the tool requires evaluation, ensure the applicable IPTs program plans are updated to reference this Software Tool Evaluation Plan.
7. If the tool requires evaluation, the responsible IPT Lead/Designee must conduct the evaluation and complete the Software Tool Evaluation Report form in Appendix A.
8. At the top of the Software Tool Evaluation Report form, record the name of the person(s) performing the evaluation, the date(s) of the evaluation, the tool name, version number and a brief description of the tool and its intended purpose.
9. Section 1 of Appendix A contains questions directed towards the tool supplier. The intent of this section is to provide confidence that the supplier followed appropriate software development practices in the development and maintenance of the tool. During this step, the evaluator must gather sufficient information from the tool supplier to provide confidence that the tool will perform as required. Supporting evidence may include ensuring the supplier follows a well documented and standardized software development process that includes requirements definition/management, version control, verification and validation and defect management and that the supplier tracks and corrects problems reported by users as part of the process of releasing an updated version of the tool. In addition, review of the supplier's test results from verification and validation activities, published reliability reports and documented compliance to certifications relevant to the development of Safety System Software (e.g. SIL, IEEE Std 7-4.3.2-2003) may also be used as evidence. This information may be obtained by an On Site audit of the supplier and/or by phone/email contact where the supplier furnishes the requested information.
    a. If an On Site audit is performed, the IPT Lead/Designee may assemble an audit team consisting of a technical representative familiar with the tool, a quality representative and a representative of the configuration management team.
    b. Additional information as to the pedigree of the tool (e.g. the tool is recognized as an industry standard that has been used successfully on systems where safety is a critical element of historical performance on programs/systems here at Lockheed Martin, the tool supplier is considered an industry leader with a long and documented history, published white papers or other technical documents) may be used to show evidence of the tool's ability to perform its intended purpose without introducing any negative effect to the Safety System Software.

    In Section 2 of Appendix A, the evaluator must verify and record evidence that the NuPAC I-V&V Plans and the Safety System Software development plans identify the V and V and process activities necessary to detect defects not detected by the software tool (e.g. the conduct of peer/code reviews, documented coding standards, conducting functional level simulation runs, timing analysis, code coverage).
10. A summary of the results of the evaluation must be documented in Section 3 of the Software Tool Evaluation Report.
11. Additional information may be included as an attachment to the Software Tool Evaluation Report form.
12. Approval signatures of the key stakeholders must be recorded in Section 4 of the Software Tool Evaluation Report.
13. New versions of the support software tools used on the program must be evaluated by the IPT members to determine the need to migrate to the new tool version.
    a. A recommendation as to whether or not to upgrade to a new version will be made based on a review of the release notes for the new version, the business rhythm of the program and an assessment of the potential impact of the changes.
    b. Once a recommendation to upgrade has been made, an assessment of the associated cost and schedule impact will be made and, if necessary, program risk will be documented in the risk registry.
    c. The recommendation and supporting assessment data will be presented to Program Management for final decision.

5.0 DEFINITIONS AND ACRONYMS

Acronym	Definition

CSCI	Computer Software Configuration Item
COTS	Commercial-Off-The Shelf
IEEE	Institute of Electrical and Electrical Engineers
I-V&V	Independent Verification and Validation
LMGI	Lockheed Martin Global Inc.
NuPAC	Nuclear Protection and Control
PL	Programmable Logic
PLCI	Programmable Logic Configuration Item
RPS	Reactor Protection System
SIL	Safety Integrity Level
SNPTC	State Nuclear Power Technology Corporation
SW	Software
V&V	Verification and Validation
NRC	Nuclear Regulatory Commission

6.0 APPENDIX A – SOFTWARE TOOL EVALUATION REPORT FORM

LOCKHEED MARTIN 国家核电 SNPTC 国核自仪系统工程有限公司 STATE NUCLEAR POWER AUTOMATION SYSTEM ENGINEERING COMPANY

Software Tool Evaluation Report

Program:			
Evaluator Name:		**Evaluation Date:**	
Tool Name:			
Tool Version:			
Tool Description:			
Intended uses:			
Section 1: Product Assurance	**Y/N**	**Comments**	**Evidence**
Is the software tool supplier an approved supplier to LMGI?			
Was the software tool developed under a Software Quality Assurance Plan?			
Was the software tool development process documented (e.g. Software Requirements Specification, Software Design Description, Coding Standards, etc.)? Are the documents maintained in a program repository?			
Is there a verification and validation procedure in place?			
Is there a procedure for tracking, documenting, and resolving defects reported by users?			
Is there a regression test performed prior to release of a new revision?			
Is the software tool under supplier's configuration control?			
Does supplier provide tool support services?			
Enter user base for comparison (e.g. safety related application uses, number of users, etc.).			
Section 2: Operational Evaluation		Comments	Evidence
As a minimum, the software tool evaluation process shall verify the following methods are in place to identify defects not detected by the software tool itself. Record results from similar projects that used the tool.			
A documented I-V&V plan and evidence that the plan is adhered to by the I-V&V team.			
SDP/PLDP details the development processes followed by the SW/PL development teams.			
Perform code reviews of the PL/Software configuration item (PL/SW).			
Perform functional level simulations and code coverage (PL).			
Perform unit testing of the software component (PL/SW).			
Perform functional level testing of the Software configuration item (PL/SW).			
Perform post place & route simulations (PL).			
Perform hardware level testing (PL/SW).			

LOCKHEED MARTIN 国家核电 SNPTC 国核自仪系统工程有限公司 STATE NUCLEAR POWER AUTOMATION SYSTEM ENGINEERING COMPANY

Software Tool Evaluation Report

Program:	
Evaluator Name:	**Evaluation Date:**
Tool Name:	
Tool Version:	
Tool Description:	
Intended uses:	

Section 3: Evaluation Results

- ☐ Tool is acceptable for all the indended uses identified above.
- ☐ Tool is acceptable except for the indended uses identified below.
- ☐ Tool is unacceptable for all the indended uses identified above.

Unacceptable intended uses:

Section 4: Approval Signatures

IPT Lead:	**Date:**
IPT Designee:	**Date:**
QA Engineer:	**Date:**