



FRAMATOME ANP

An AREVA and Siemens Company

FRAMATOME ANP, Inc.

February 8, 2005
NRC:05:007

Document Control Desk
ATTN: Rules and Directives Branch
Office of Administration
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555-0001

Comments on Draft Regulatory Guide DG-1130

Framatome ANP (FANP) submits the following comments on the draft regulatory guide DG-1130 identified in the Federal Register on December 16, 2004 (69 FR 75359).

GENERAL COMMENTS

1. The draft RG as presently structured does not adequately address the overall development or review process for cyber security for programmable digital equipment. The section on cyber security should not be all encompassing. Different levels of cyber security methods should be placed on firmware, software with no communication capabilities, software with only internal communication capabilities, software with internal and external but without offsite communication capabilities and software with internal and external including offsite communication capabilities. Furthermore, the cyber security section should discuss licensee developed application software versus vendor developed application software. The RG should also provide a discussion on cyber security methods for commercially developed digital platforms where the software life cycle does not follow the normal pattern. We see no significant benefit in relating cyber security to the software life cycle. There is no defined purpose or desired result stated within the cyber security section. Because of the significance of cyber security, the many communication paths for software, and the different development processes, FANP believes that there should be a separate document developed that discusses cyber security. This document should be the result of a joint-effort with both the nuclear industry and the NRC staff as participants. It is recommended that this draft RG only make a reference to the topic with the stated intent of developing future cyber security guidance.

COMMENTS ON DISCUSSION SECTION

2. In the fourth paragraph it is stated that "With respect to software diversity, experience indicates that independence of failure modes may not be achieved in cases where multiple versions of software are developed from the same software requirements." This statement was used in the last revision of the Regulatory Guide. Does this statement refer to the same experience, which was a graduate student experiment of the 1990 time frame? It would be helpful if the NRC could site some recent experience over the last five years that has proven this point. With the proper method of software program development using the same software requirements, experience should indicate that common mode failure modes could be eliminated or greatly reduced.

3. Since firmware is also considered to be software (footnote 1), the statement in paragraph 7 that "controls of both physical and electronic access to system software and data should be provided to prevent changes by unauthorized personnel" is too broad. We do not believe that cyber security for software versus firmware can be treated in the same manner. A differentiation should be drawn between the two. (See 1 above)

4. In paragraph 10, Item (f), it is stated that the NRC does not endorse the concept of quantitative reliability goals as a sole means of meeting its regulations for reliability of digital computers in safety systems. It should be acknowledged that there is an industry-wide program to use risk-informed means as a method for showing that digital common-mode failures are not a significant source of concern for many transients and accidents. The NRC has participated in this effort and is aware of the program and the initial conclusions.

COMMENTS ON REGULATORY POSITION SECTION

General- The discussion that follows in this section tends to be somewhat confusing. It is not clear if the discussion is centering on the vendor's development of the operational software or if the discussion is centered on the vendor's (or the licensee's) development of the application software. Normally the user (the term should be changed to licensee for all cases in the draft RG) is not involved in any of the initial stages of the software life cycle. The licensee is not actively involved until the installation and check out phase of the life cycle. Comments 6 and 7 below are based on this assumption.

5. In Section 2 "Security", it is stated that the "Quality Assurance organization should conduct periodic audits to determine the effectiveness of the digital safety system security program." This recommendation is redundant to the recommendation discussed in Section 2.8.2, "Quality Assurance". The statement should be removed from Section 2 and retained in Section 2.8.2.

6. In Section 2.1 "Concepts Phase", it is stated in part that the user and developer should perform security risk analysis for the concept phase. The user (licensee) is not usually involved at this stage of a digital system design. The concept stage is normally the sole domain of the vendor. The term user should be removed.

7. In Section 2.2.1 "System Features" the term user (licensee) should be removed for the same reasons as in #6 above.

8. In Section 2.4.2 "Development Activities" it is stated in part that the developer and the user (licensee) should review the possibility for deliberate modification of software. The licensee is usually not in a position to provide this review. The term user (licensee) should be deleted or declared optional.

9. In Section 2.8 "Maintenance Phase" the retirement phase discussion should be moved to Section 2.9 "Retirement Phase."

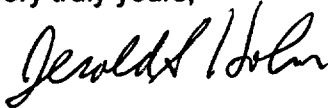
SUMMARY

In summary, the entire cyber security section should be deleted and only a passing reference to the subject retained. New guidance regarding cyber security should be developed and not just as an "add on" to an existing RG. The subject is sufficiently important and complex to merit a

more considered set of guidance. A significant joint effort should be undertaken to publish comprehensive cyber security guidance that covers present and planned uses of software in nuclear plants.

Framatome ANP appreciates this opportunity to comment on the draft Regulatory Guide. If you have any questions concerning the comments, please contact Jerry Mauck at (301) 596-9334.

Very truly yours,



Jerald S. Holm, Director
Regulatory Affairs

cc: M. C. Honcharik
Project 728