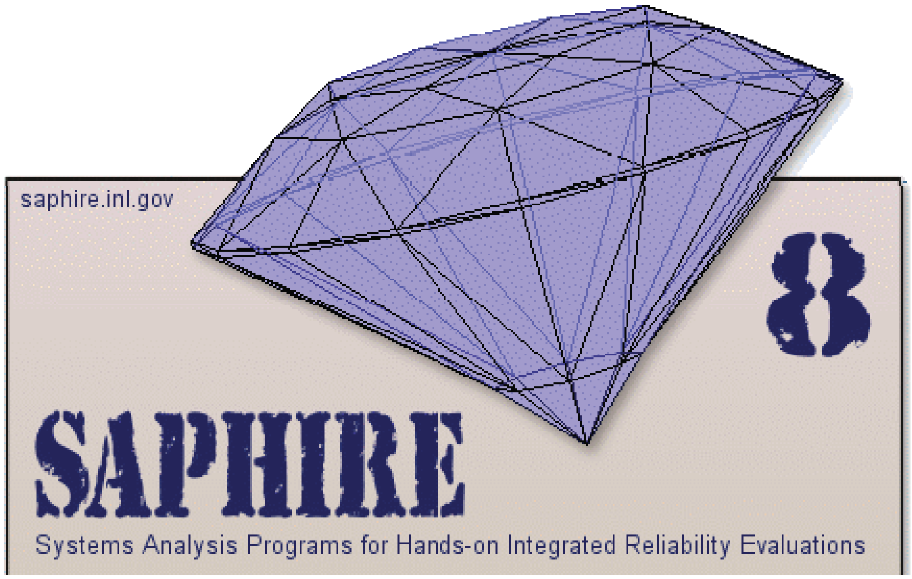
INL/EXT-09-17069
Rev. 1

Independent Verification and Validation of SAPHIRE 8 Software Design and Interface Design

March 2010


saphire.inl.gov
8
SAPHIRE
Systems Analysis Programs for Hands-on Integrated Reliability Evaluations

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

INL/EXT-09-17069
Rev. 1

Independent Verification and Validation of SAPHIRE 8 Software Design and Interface Design

March 2010

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Nuclear Regulatory Commission
Washington, DC 20555
Project Number N6423

Table of Contents

1.0 Executive Summary

The purpose of the Independent Verification and Validation (IV&V) role in the evaluation of the SAPHIRE 8 software design and interface design is to assess the activities that results in the development, documentation, and review of a software design that meets the requirements defined in the software requirements documentation. The IV&V team began this endeavor after the software engineering and software development of SAPHIRE had already been in production. IV&V reviewed the requirements specified in the NRC Form 189s to verify these requirements were included in the SAPHIRE Version 8 Software Verification and Validation Plan (SVVP) Volume I (INL/EXT-05-00821) section 4 Design Specification.

The requirements for IV&V review were extracted primarily from the NUREG/BR-0167 Software Quality Assurance Program and Guidelines, but also included an examination of best software engineering methods provided in the IEEE Standard for Software Verification and Validation. IV&V developed a checklist that mapped these requirements with these standards which was used in the evaluation. The evaluation criteria and the results of the assessment are identified in section 4 of this document.

Traceability of requirements is the greatest of these concerns. Requirements traceability is essential to all software development activities. Without a well documented Requirements Traceability Matrix (RTM), design components may be overlooked, and test cases missed.

For IV&V to properly evaluate the RTM to assess the mapping of the test cases to design components and to requirements as documented in the SAPHIRE Version 8 SVVP, IV&V had to obtain requirements from the Statement of Work documents (Form 189s) and develop the RTM. This action could place IV&V's "independence" role into question. The intent of IV&V in developing the RTM is strictly for use in evaluation and not intended for use by the development team. However, the RTM will be included as documentary evidence in the IV&V report provided to the sponsor and the INL Project Manager.

Per the requirements and document outline provided in the SAPHIRE 8 Software Independent Verification and Validation Plan (INL/EXT-09-15649), this report and all subsequent reports will be included as attachments and/or background evidence of the evaluation as well as the results of the assessment.

2.0 Background Information

NUREG/BR-0167, Software Quality Assurance Program and Guidelines, requires the development of Software Design Documentation that specifies the overall structure of the software so that it can be translated into code. The Software Design Documentation includes a description of the major elements of the software as they relate to the requirements; a description of the theoretical basis, physical model, mathematical model, control flow, data flow, control logic, and data structure; and an identification and detailed definition of the software units and data elements of the software architecture.

This report provides an evaluation of the Software Design Documentation. The Software Design Documentation is intended to provide the development, documentation, and review of the software design that meets the requirements defined in the Software Requirements Documentation to meet the contractual commitments prepared by the sponsor; the Nuclear Regulatory Commission.

Independent Verification and Validation (IV&V) evaluates and assesses the processes and products developed during each phase of the Software Development Life Cycle (SDLC). The SAPHIRE 8 development team is implementing a "spiral" rapid application approach to the product development. One of the roles that IV&V performs, regardless of the development methodology, is to analyze products developed throughout the development process. The intent is to provide a level of confidence to the sponsor that the quality of the software product and supporting documentation is built into the software, not tested in. Evaluating the supporting documentation for each product is one aspect of providing this level of confidence.

IV&V supports and is complementary to the Quality Assurance, Project Management, and product development activities. To achieve this support, IV&V must also evaluate the processes identified in the documentation to ensure that the development team is implementing the processes and methodology that ensures a high-level software product.

Due to the spiral approach implemented for the software development, it is expected that the Software Design Documentation will evolve as the SAPHIRE 8 product matures. Therefore, IV&V will evaluate each iteration of the Software Design Documentation.

To provide direction in the evaluation process, IV&V has developed a checklist to support the requirements for the SDLC. The Project Plan requirements used for the analysis of the Software Design Documentation is contained in a checklist that is included in the SAPHIRE 8 Software Independent Verification and Validation Plan (INL/EXT-09-15649). The evaluation criteria for the Software Design Documentation have been extracted from the checklist contained in the "IV&V Plan" and included in section 4 of this report. A summary of the findings is provided in section 3.

3.0 Summary of Findings

An Independent Verification and Validation evaluation of the Software Verification and Validation Plan – Volume I, section 4 Design Specification, Document ID: INL/EXT-05-00821 and the Software Verification and Validation Plan – Volume II, Document ID: INL/EXT-05-00821 for SAPHIRE 8 was performed using the checklist contained in section 4.0 of this document. The checklist was extracted from the SAPHIRE 8 Software Independent Verification and Validation Plan Document ID: INL/EXT-09-15649. A requirements traceability analysis was performed to trace design components to requirements, and requirements and design components to test cases. The results of the requirements traceability analysis is in attachment NRC Form 189 Requirements Table.xls.

Section 3.1 refers to the specific parts of the NUREG/BR-0167 Software Quality Assurance Program and Guidelines requirements the SAPHIRE 8 Software Verification and Validation Plan – Volume I section 4 failed to satisfy. Of the 15 criteria listed in the checklist contained in section 4.0 of this document 4 failed. Section 3.2 of the Summary of Findings lists minor corrections for the Software Verification and Validation Plan – Volume I section 4 Design Specification and section 3.3 of the Summary of Findings list minor corrections for the Software Verification and Validation Plan – Volume II.

3.1 NUREG/BR-0167 Findings

The following provides the corrections needed for the failed criteria in the checklist supplied in section 4.

Criteria 1 – Section 4.1.2 Project Controls and section 4.1.5 do not contain any design information. Provide design information to complete these sections.

Section 4.1.8 External Events Design and section 4.7 Phase Mission Design need to supply design information leading into the following sub-sections to provide consistency with the other sections.

Section 4.4.5 End State Object Design first sentence states "*End State objects are currently under development*", and then starts "*The end state object represents the declarations…*" Section 4.5.9 General Analysis Design specifies "*This analysis is currently in the development stage of design*" then goes into the General Analysis Design. Provide corrections and add design information to complete these sections.

The consistency of detail between sections describing design information varies. Some sections are very brief and others go into great detail. Provide consistency of design information detail.

Criteria 2 – Section 4.1.2 Project Controls and section 4.1.5 do not contain any design information. Provide design information to complete these sections.

The Requirements Traceability Matrix (RTM) as presented in the SAPHIRE Version 8 Software Verification and Validation Plan – Volume II, Appendix D Requirements Traceability Matrix, (INL/EXT-05-00821) is incomplete and currently does not show the traceability between software design components and software requirements.

The design components are not uniquely identified.

Criteria 9 – The Requirements Traceability Matrix (RTM) as presented in the SAPHIRE Version 8 Software Verification and Validation Plan – Volume II, Appendix D Requirements Traceability Matrix, (INL/EXT-05-00821) is incomplete and currently does not show the traceability between software design components and software requirements. The RTM does not list design components that map to requirements. The test cases as listed in the RTM are incomplete ("NA", "None", "To be determined").

The design components are not uniquely identified.

Criteria 12 – IV&V passed this criterion based on "*the Data Dictionary has been developed*". The Data Dictionary does not contain information that defines items computed in the code, what they are and what they do. Define in the Data Dictionary items computed in the code, what they are and what they do.

Criteria 13 – Refer to document Independent Verification and Validation Of SAPHIRE 8 Software Requirements Project Number: N6423 U.S. Nuclear Regulatory Commission, Document ID: INL/EXT-09-16789 Revision 1.

In order for the requirements to be testable and traceable through the software life cycle the individual requirements need to be uniquely identified. In order to uniquely identify the requirement, identify each requirement in section 2 Software Requirements and section 3 Interface Requirements Specification as a "functional (e.g., FR-01)", "performance (e.g., PR-01)", "design constraint (e.g., DCR-01)", "attribute (e.g., AR-01)", or "external interface (e.g., IR-01)" requirement.

3.2 SVVP – Volume I section 4 Design Specification Findings

The following provides minor corrections for the Software Verification and Validation Plan – Volume I, section 4 Design Specification.

1. Throughout the document.
   When referring to SAPHIRE Version 8, "8" is used and "8.0" is used.
   IV&V suggests using "SAPHIRE Version 8" or "SAPHIRE 8" to be consistent with the rest of the document.

2. Page 26, section 4.1.2 Project Controls.
   This section does not contain any design information.
   Provide design information to complete this section.

3. Page 28, section 4.1.5 Project-Wide Search Design.
   This section states "*This functionality is currently in the concept stage of design.*"
   Provide design information to complete this section.

4. Page 31, section 4.1.8 External Events Design.
   Provide design information leading into the following sub-sections to provide consistency with the other sections.

5. Page 33, 4.1.8.2 Basic Event Model Type Modifications.
   Figure 2 is referenced.
   Figure 2 with the "*applicability*" option is not found.

6. Page 34, section 4.1.8.2 Basic Event Model Type Modifications.
   Figure 4.2.1.8.3 is referenced.
   Figure 4.2.1.8.3 is not found.

7. Page 34, section 4.1.8.2 Basic Event Model Type Modifications.
   Figure 4.2.1.8.4 is referenced.
   Figure 4.2.1.8.4 is not found.

8. Page 39, section 4.1.8.5 Showing Model types for User Interaction.
   The caption for the figure on this page is at the top of the page in the right hand column. IV&V suggest aligning the caption below the figure.

9. Page 41, section 4.2 Application Program Interface (API) Design, last paragraph.
   The paragraph specifies "*A list of the currently existing API interface modules are listed in the Requirements Traceability Matrix, Appendix D, Section 16.*"
   Section 16 is not found.

10. Page 43, section 4.3.2 SAPHIRE 8.0 Database Design, last sentence.
    The sentence "*The tables are named as follows and a copy of the database schema can be found in the Appendices.*"
    The database schema is found in Appendix F.

11. Page 44, section 4.3.2 SAPHIRE 8.0 Database Design list of database schema found in Appendix F.
    The Table Names "EvenTemp", "Util", "UtilCF", "UtilRep", and "Utility" are found in Appendix F Database Schema for SAPHIRE 8 but are not in this list of database schema.
    Provide corrections as necessary.

12. Page 44, section 4.3.2 SAPHIRE 8.0 Database Design list of database schema found in Appendix F.
    The list of database schema found in Appendix F specifies the table name "PDSMasks", the list of database schema specifies the table name "PDSMask".
    Provide corrections as necessary.

13. Page 44, section 4.3.2 SAPHIRE 8.0 Database Design list of database schema found in Appendix F.
    The list of database schema found in Appendix F specifies the table name "SliceRul", the list of database schema specifies the table name "SliceRule".

Provide corrections as necessary.

14. Page 44, section 4.3.2 SAPHIRE 8.0 Database Design list of database schema found in Appendix F.
    The Table Name "Categories" is not found in Appendix F Database Schema for SAPHIRE 8.
    Provide corrections as necessary.

15. Page 48, section 4.4.3 Fault Tree Object Design, last paragraph.
    The sentence "*Identifying including name and description are included on each graphical representation of an object.*"
    IV&V suggest changing the sentence to" *Identifying name and description are included on each graphical representation of an object.*"

16. Page 49, section 4.4.3 Fault Tree Object Design.
    The sentence containing "…in the solution space defined by the model types being analyses."
    IV&V suggest changing the word "*analyses*" to "*analyzed*".

17. Page 51, section 4.4.5 End State Object Design.
    This section states "*End state objects are currently under development.*"
    Provide design information to complete this section.

18. Page 61, section 4.5.3 Uncertainty Importance.
    Second paragraph containing the sentence "*By selecting one of the seven importance measure tabs on the tabbed dialog, each events' importance measures will calculated for the…*"
    IV&V suggest changing the sentence to "*By selecting one of the seven importance measure tabs on the tabbed dialog, each events' importance measures will **be** calculated for the…*"

19. Page 67, section 4.5.8 ECA Analysis Design.
    The sentence "*The implementation of this Subtask is described below and in 4.5.12.*"
    Is "4.5.12" referring to a section or a figure? Neither is found.
    Provide corrections as necessary.

20. Page 69, section 4.5.8.1 Initiating Event Assessments Design.
    First paragraph the sentence "*This type of analysis is the same as what existed in previously in GEM.*"
    IV&V suggest changing the sentence to "*This type of analysis is the same as what existed previously in GEM.*"

21. Page 70, section 4.5.9 General Analysis Design.
    This section states "*This analysis is currently in the development stage of design.*"
    Provide design information to complete this section.

22. Page 78, section 4.6 Embedded Macro Design.
    The first sentence in the fifth paragraph specifies references section 4.8.
    IV&V believes this should be section 4.9.

23. Page 85, section 4.7.2 Basic Event Phase Modifications.
    The sentence "*A basic event will be able to "cloned" so that…*"
    IV&V suggests changing the sentence to "*A basic event will be able to **be** "cloned" so that…*"

24. Page 92, section 4.7.4.2 Case 2, Sequence 4.
    Third paragraph, the sentence "*However, we can not a successful recovery…*"
    IV&V suggests changing the sentence to "*However, we can not **have** a successful recovery…*"

25. Page 93, section 4.7.4.2 Case 2, Sequence 2.
    Third paragraph, the sentence "*Consequently, this cut set **is** must be adjusted…*"
    IV&V suggests changing the sentence to "*Consequently, this cut set must be adjusted…*"

26. Page 94, section 4.8 Common Cause Failure Module Design.
    Fourth bullet.
    IV&V suggests changing "*Selected*" to "*Select*".

27. Page 100, section 4.8.5 CCF Adjustments via Boolean Reduction.
    The second sentence references "equation 5-4".
    This equation was not found.

28. Page 122 and page 123, section 4.9.2 Basic Event Model Type Modifications.
    Reference is made to "*Figure 4.8..4*".
    IV&V suggests changing the figure number to "*Figure 4.8.4*".

29. Page 123, section 4.9.4 Analysis Capabilities Specific to EE Models.
    Reference is made to "*Figure 4.8.55*".
    This figure is not found.

30. Page 123, section 4.9.4 Analysis Capabilities Specific to EE Models.
    Reference is made to "*(Figure)*" and "*(Figure7)*".
    Provide corrections as necessary.

31. Page 128, section 4.9.5 Showing Model types for User Interaction.
    Reference is made to "*(Figure8)*".
    Provide corrections as necessary.

32. Page 129, section 4.9.6 Adding an EE Accident Matrix.
    Second sentence from the bottom, the reference to "*(.cvs)*".
    IV&V believes this should be "*(.csv)*".

33. Page 131, section 4.9.6 Adding an EE Accident Matrix.
    Second sentence from the bottom.
    IV&V believes "*bellow*" should be "*below*".

34. Page 134, section 4.10.1 Enhanced sequence model development.
    This section contains a bullet with no information.

35. Page 135, section 4.10.1.3 Ability to assign a phase via decision/logic rules.
    Reference is made to "*Rev 2 of the "SAPHIRE Phase-Aware Design Specification*".
    Provide a document id for this document.

36. Pages x and xi, FIGURES.
    The list of figures twice references "*Figure 4*".
    Provide corrections as necessary.

37. Pages x, FIGURES.
    The list of figures twice references "*Figure 4.5.2.2*".
    Provide corrections as necessary.

38. Pages x, FIGURES.
    The list of figures contains "*Table 1. CCF Analysis Table for the three-component (1-of-3 success criteria) example*" and "*Table 2 CCF Analysis Table for the three-component (2-or-3) success criteria) example*".
    Provide corrections as necessary.

39. Page 25, section 4 Design Specification.
    Provide reference to Figure 4.

40. Page 26, section 4.1 Graphical User Interface (GUI) Design.
    Provide reference to Figure 4.1.

41. Page 29, section 4.1.6 User Selectable Constants Design.
    Provide reference to Figure 4.1.6-1.

42. Page 29, section 4.1.6 User Selectable Constants Design.
    Provide reference to Figure 4.1.6-2.

43. Page 30, section 4.1.6 User Selectable Constants Design.
    Provide reference to Figure 4.1.6-3.

44. Page 31, section 4.1.7 Workspace Selection Design.
    Provide reference to Figure 4-3.

45. Pages 31 and 32, section 4.1.8.1 General Model type Information.
    This section contains a table specifying the general model type information.
    IV&V suggest adding a table caption to this table, providing reference to the table and adding the table to the list of TABLES in the table of contents.

46. Page 32, section 4.1.8.2 Basic Event Model Type Modifications.
    Figure 4.1.8.2.1 is not included in the list of FIGURES in the table of contents or referenced in the document.

Provide reference to the figure and add the figure to the list of FIGURES in the table of contents.

47. Page 33, section 4.1.8.2 Basic Event Model Type Modifications.
    Figure 4.1.8.2.2 is not included in the list of FIGURES in the table of contents or referenced in the document.
    Provide reference to the figure and add the figure to the list of FIGURES in the table of contents.

48. Page 34, section 4.1.8.2 Basic Event Model Type Modifications.
    Figure 4.1.8.2.3 is not included in the list of FIGURES in the table of contents or referenced in the document.
    Provide reference to the figure and add the figure to the list of FIGURES in the table of contents.

49. Page 35, section 4.1.8.2 Basic Event Model Type Modifications.
    Figure 4.1.8.2.4 is not included in the list of FIGURES in the table of contents or referenced in the document.
    Provide reference to the figure and add the figure to the list of FIGURES in the table of contents.

50. Page 36, section 4.1.8.4 Analysis Capabilities Specific to EE Models.
    Figure 4.1.8.4.1 is not included in the list of FIGURES in the table of contents.
    Please add the figure to the list of FIGURES in the table of contents.

51. Page 37, section 4.1.8.4 Analysis Capabilities Specific to EE Models.
    Figure 4.1.8.4.2 is not included in the list of FIGURES in the table of contents.
    Please add the figure to the list of FIGURES in the table of contents.

52. Page 38, section 4.1.8.4 Analysis Capabilities Specific to EE Models.
    Figure 4.1.8.4.3 is not included in the list of FIGURES in the table of contents.
    Please add the figure to the list of FIGURES in the table of contents.

53. Page 39, section 4.1.8.5 Showing Model Types for User Interaction.
    Figure 4.1.8.5.1 is not included in the list of FIGURES in the table of contents.
    Please add the figure to the list of FIGURES in the table of contents.

54. Page 40, section 4.1.9.2 General Structure of the Help Page.
    This section contains an example of the nominal help page structure.
    IV&V suggest adding a figure caption to this example, providing reference to the figure and adding the figure to the list of FIGURES in the table of contents.

55. Page 42, section 4.3.1 General SAGE-ST Tool Description.
    This section contains a table describing the Sage-ST tool set.
    IV&V suggest adding a table caption to this table, providing reference to the table and adding the table to the list of TABLES in the table of contents.

56. Page 44, section 4.3.2 SAPHIRE 8.0 Database Design.
    This section contains a table listing the tables in the database schema.
    IV&V suggest adding a table caption to this table, providing reference to the table and adding the table to the list of TABLES in the table of contents.

57. Page 45, section 4.4.2 Event Object Design.
    This section contains a table listing the failure model types.
    IV&V suggest adding a table caption to this table, providing reference to the table and adding the table to the list of TABLES in the table of contents.

58. Page 46, section 4.4.2 Event Object Design.
    Provide reference to Figure 4.4.2-1.

59. Page 47, section 4.4.2 Event Object Design.
    Provide reference to Figure 4.4.2-2.

60. Page 47, section 4.4.2 Event Object Design.
    Provide reference to Figure 4.4.2-3.

61. Page 48, section 4.4.2 Event Object Design.
    Figure 4.4.2-4 is not included in the list of FIGURES in the table of contents or referenced in the document.
    Provide reference to the figure and add the figure to the list of FIGURES in the table of contents.

62. Page 52, section 4.4.6 Sequence Object Design.
    Figure 4.4.6-1 is not included in the list of FIGURES in the table of contents.
    Please add the figure to the list of FIGURES in the table of contents.

63. Page 54, section 4.5.2 Importance Measures Analysis Design.
    Provide reference to Figure 4.5.2.

64. Page 55, section 4.5.2.1 Fussell-Vesely Importance (FV).
    Provide reference to Figure 4.2.2.1.

65. Page 56, section 4.5.2.2 Birnbaum Importance (B).
    Provide reference to Figure 4.5.2.2.

66. Page 57, section 4.5.2.3 Risk Reduction Ratio (RRR) and Risk Reduction Interval (RRI) Importance..
    Provide reference to Figure 4.5.2.3-1.

67. Page 58, section 4.5.2.3 Risk Reduction Ratio (RRR) and Risk Reduction Interval (RRI) Importance..
    Provide reference to Figure 4.5.2.3-2.

68. Page 59, section 4.5.2.4 Risk Increase Ratio (RIR) and Risk Increase Interval (RII) Importance.
    Figure 4.5.2.1 is not included in the list of FIGURES in the table of contents or referenced in the document.
    Provide reference to the figure and add the figure to the list of FIGURES in the table of contents.

69. Page 60, section 4.5.2.4 Risk Increase Ratio (RIR) and Risk Increase Interval (RII) Importance.
    Provide reference to Figure 4.5.2.2.

70. Page 62, section 4.5.3 Uncertainty Importance.
    Provide reference to Figure 4.5.3-2.

71. Page 70, section 4.5.9 General Analysis Design.
    Figure 4.5.12-1 is not included in the list of FIGURES in the table of contents.
    Please add the figure to the list of FIGURES in the table of contents.

72. Page 71, section 4.5.9 General Analysis Design.
    Figure 4.5.12-2 is not included in the list of FIGURES in the table of contents.
    Please add the figure to the list of FIGURES in the table of contents.

73. Page 72, section 4.5.9 General Analysis Design.
    Figure 4.5.12-3 is not included in the list of FIGURES in the table of contents.
    Please add the figure to the list of FIGURES in the table of contents.

74. Page 72, section 4.5.9 General Analysis Design.
    Figure 4.5.12-4 is not included in the list of FIGURES in the table of contents.
    Please add the figure to the list of FIGURES in the table of contents.

75. Page 76, section 4.5.11 Rules Editor Design.
    Figure 4.1.14-1 is not included in the list of FIGURES in the table of contents or referenced in the document.
    Provide reference to the figure and add the figure to the list of FIGURES in the table of contents.

76. Page 77, section 4.5.11 Rules Editor Design.
    Figure 4.1.14-2 is not included in the list of FIGURES in the table of contents or referenced in the document.
    Provide reference to the figure and add the figure to the list of FIGURES in the table of contents.

77. Page 79, section 4.6 Embedded Macro Design.
    Figure 4.6.1 is not included in the list of FIGURES in the table of contents.
    Please add the figure to the list of FIGURES in the table of contents.

78. Page 80, section 4.6 Embedded Macro Design.
    Figure 4.6.2 is not included in the list of FIGURES in the table of contents.
    Please add the figure to the list of FIGURES in the table of contents.

79. Page 81, section 4.6 Embedded Macro Design.
    Figure 4.6.3 is not included in the list of FIGURES in the table of contents.
    Please add the figure to the list of FIGURES in the table of contents.

80. Page 81, section 4.6 Embedded Macro Design.
    Figure 4.6.4 is not included in the list of FIGURES in the table of contents.
    Please add the figure to the list of FIGURES in the table of contents.

81. Page 83, section 4.7.1 General Phase Information.
    Figure 4.7.1 is not included in the list of FIGURES in the table of contents.
    Please add the figure to the list of FIGURES in the table of contents.

82. Page 84, section 4.7.1 General Phase Information.
    Provide reference to Figure 4.7.2.

83. Page 95, section 4.8 Common Cause Failure Module Design.
    Figure 2 is not included in the list of FIGURES in the table of contents.
    Please add the figure to the list of FIGURES in the table of contents.

84. Page 97, section 4.8.2 Defining a CCF Object.
    This section contains a table listing the information matrix for a CCF object.
    IV&V suggest adding a table caption to this table, providing reference to the table and adding the table to the list of TABLES in the table of contents.

85. Page 99, section 4.8.2 Defining a CCF Object.
    The figure shown is not included in the list of FIGURES in the table of contents or referenced in the document and does not have a figure caption.
    Provide reference to the figure, add the figure to the list of FIGURES in the table of contents and add a figure caption.

86. Page 109, section 4.8.8 CCF Example.
    The two figures shown are not included in the list of FIGURES in the table of contents or referenced in the document and do not have figure captions.
    Provide reference to the figures, add the figures to the list of FIGURES in the table of contents and add figure captions.

87. Page 115, section 4.8.9 Conditioning CCF Approach.
    Provide reference to Table 2.

88. Page 120, section 4.9.1 General Model Type Information.
    This section contains a table listing the general model type information.

IV&V suggest adding a table caption to this table, providing reference to the table and adding the table to the list of TABLES in the table of contents.

89. Page 122, section 4.9.2 Basic Event Model Type Modifications.
    Figure 4.8.3 is not included in the list of FIGURES in the table of contents or referenced in the document.
    Provide reference to the figure and add the figure to the list of FIGURES in the table of contents.

90. Page 126, section 4.9.4 Analysis Capabilities Specific to EE Models.
    Provide reference to Figure 4.8.6.

91. Page 127, section 4.9.4 Analysis Capabilities Specific to EE Models.
    Provide reference to Figure 4.8.7.

92. Page 128, section 4.9.4 Analysis Capabilities Specific to EE Models.
    Provide reference to Figure 4.8.8.

93. Page 129, section 4.9.6 Adding an EE Accident Matrix.
    The figure shown is not included in the list of FIGURES in the table of contents or referenced in the document and does not have a figure caption.
    Provide reference to the figure, add the figure to the list of FIGURES in the table of contents and add a figure caption.

94. Page 130, section 4.9.6 Adding an EE Accident Matrix.
    The three figures shown are not included in the list of FIGURES in the table of contents or referenced in the document and do not have figure captions.
    Provide reference to the figures, add the figures to the list of FIGURES in the table of contents and add figure captions.

95. Page 131, section 4.9.6 Adding an EE Accident Matrix.
    The two figures shown are not included in the list of FIGURES in the table of contents or referenced in the document and do not have figure captions.
    Provide reference to the figures, add the figures to the list of FIGURES in the table of contents and add figure captions.

96. Page 132, section 4.9.6 Adding an EE Accident Matrix.
    The figure shown is not included in the list of FIGURES in the table of contents or referenced in the document and does not have a figure caption.
    Provide reference to the figure, add the figure to the list of FIGURES in the table of contents and add a figure caption.

97. Page 143, section 4.9.6 Adding an EE Accident Matrix.
    This section contains a table summarizing the keyword changes and lists the new/modified keywords and information related to their use.

IV&V suggest adding a table caption to this table, providing reference to the table and adding the table to the list of TABLES in the table of contents.

98. Page 150, section 4.11.1 Features of a Significance Determination Process Module.
    The figure shown is not included in the list of FIGURES in the table of contents or referenced in the document and does not have a figure caption.
    Provide reference to the figure, add the figure to the list of FIGURES in the table of contents and add a figure caption.

99. Pages 153-157, section 4.11.2 Significance Determination Process Results Reports.
    The example shown is not included in the list of FIGURES in the table of contents or referenced in the document and does not have a figure caption.
    Provide reference to the figure, add the figure to the list of FIGURES in the table of contents and add a figure caption.

100. Page xiv, ACRONYMS.
    The following acronyms are used in the document, but are not listed in the acronym list: ASCII, B, CD, CDP, CPET, DET, ESW, FT, FTR, FTS, FV, HTML, IE, LERP, MGL, PDF, RASP, RII, RIR, RRI, RRR, RTF, SPAR, T&M, XLS.

3.3 SVVP – Volume II Findings

The following provides minor corrections for the Software Verification and Validation Plan – Volume II.

1. Page iii, CONTENTS.
   The Table of Contents currently lists the previous section headings.
   Update the Table of Contents to reflect the current section headings.

2. Page 13, section 6.1 Features to be Tested, last paragraph.
   The sentence "*Section 9.3.2 lists the models used for testing in the current SV&V*" references "*section 9.3.2*". This section is not found.
   Provide corrections as necessary.

3. Pages 14-20, Table 6-1 Tests where specific PRA features are verified.
   The Software Acceptance Test Plan Document ID: INL/EXT-09-16236 for SAPHIRE 8 lists 105 tests.
   Provide updates to Table 6-1 to include all 105 tests.

4. Page 15, Table 6-1 Tests where specific PRA features are verified.
   The second row containing Test IDs Test-03, Test-04 Test-12, Test 22, Test-33 and Test-50.
   IV&V suggests lining up the Test IDs with the Test Names.

5. Page 15, Table 6-1 Tests where specific PRA features are verified.
   The ninth row containing Test IDs Test-02, Test-13, Test-41, Test-42.
   Test-42 is missing the Test Name.

6. Page 18, Table 6-1 Tests where specific PRA features are verified.

The row containing “All tests” in the Test column.
IV&V suggests listing all Test Cases to be used in the Test column.

7. Page 19, Table 6-1 Tests where specific PRA features are verified.
   The rows containing Test IDs Test-03 and Test-04.
   IV&V suggests lining up the Test IDs with the Test Names.

8. Page 19, Table 6-1 Tests where specific PRA features are verified.
   The row containing “Test-58” in the Test column specifies “All SPAR 2Q, 3i models” in the Test Models column.
   IV&V suggests listing all Test Models to be used in the Test Models column.

9. Page 20, Table 6-1 Tests where specific PRA features are verified.
   The second row containing Test-60. The Test Models specifies “TBD”.
   Provide updates to Table 6-1 as necessary.

10. Page 20, Table 6-1 Tests where specific PRA features are verified.
    The row containing Test-64. Test Name specifies “DOES NOT EXIST YET”. Section 7.2.1 Test Descriptions subsection 7.2.1.64 provides Test-64, Calculations on the Common-Cause Plug-in.
    Provide updates to Table 6-1 as necessary.

11. Page 20, Table 6-1 Tests where specific PRA features are verified.
    The second row containing Test-65. The Test Models specifies “TBD”.
    Provide updates to Table 6-1 as necessary.

12. Pages 14-20, Table 6-1 Tests where specific PRA features are verified.
    The Test Models column in some instances specifies “All” and “Multiple”.
    IV&V suggests listing all Test Models to be used in the Test Models column.

13. Pages 22, Section 7.1.1.1 PRA Analysis Levels.
    The first sentence references “*Figure 6-1*”. “*Figure 6-1*” is not found.
    Provide corrections as necessary.

14. Page 45, Section 7.2.1.54 Test-54, Fault Tree Utility Functions: Auto page, Solve, Save Cut Sets to End States, first sentence.
    “*SAPHIRE provides several utilities maintain fault trees.*” Sentence seems to be missing words.
    Provide corrections as necessary.

15. Page 50, Section 7.2.1.88 Test 88, Event Tree, Fault Tree Creation in a new project.
    “*Scenarios builds in the Standard Analysis interface a demonstration sized model with 3 phases and two model types from scratch and save the new project. A software developer will review these results initially. Subsequent tests will compare against verified output.*”
    Paragraph seems to be missing words.
    Provide corrections as necessary.

16. Page 52 following Section 7.2.1.104 Test 104, Event and Condition Analysis uncertainty calculations.
    Test 105, SPAR-H worksheet calculations is missing.
    Provide corrections as necessary.

17. Page 52, Section 7.2.1.103 Test 103 Test 103, Significance Determination Process Interface testing of Figure III-D (Change in delta CDF as a function of duration) point estimate checks.
    The sentence "*Figure III-D Change in delta CDF as a function of duration) is based upon a one hour value expanded to a full year outage*" is missing the opening parentheses.
    Provide corrections as necessary.

18. Page 52, Table of Features Tested by the Automated Test Suite.
    Is "Table of Features Tested by the Automated Test Suite" a section heading?

19. Page 52 and page 53, Table of Features Tested by the Automated Test Suite.
    Reference is made to Table 7.2.1-1 and Table 6-4. These tables are not found.
    Provide corrections as necessary.

20. Page 54, Table 6.2.1-1 Features tested by the automated test suite.
    The Software Acceptance Test Plan Document ID: INL/EXT-09-16236 for SAPHIRE 8 lists 105 tests. All 105 tests are not listed in Table 6.2.1-1.
    Provide updates to Table 6.2.1-1 to include all 105 tests.

21. Page 55, Section 7.4 Test Documents.
    IV&V suggests providing the Job Control Number with reference to "*NRC Form 189, Revision 7*".

22. Page 66, Section 8.3 Sources of Data.
    The first sentence states "*There are 104 different tests…*"
    The Software Acceptance Test Plan Document ID: INL/EXT-09-16236 for SAPHIRE 8 lists 105 tests.
    Make corrections as necessary.

23. Page 66, Section 8.6 Work Products.
    IV&V suggests providing the Job Control Number with reference to "*NRC Form 189, Revision 7*".

24. Page 68, Appendix A Automated Test Scripts.
    Appendix A is not referenced in the document.

25. Page 77, Appendix C Coding Standards.
    Appendix C is not referenced in the document.

26. Page 77, Appendix C Coding Standards.
    Provide updates to Appendix C Coding Standards as necessary.

27. Page 94, Appendix D Requirements Traceability Matrix.
    Appendix D is not referenced in the document.

28. Page 136, Appendix E IEEE Verification and Validation Integrity Level 1 Tasks.
    Appendix E is not referenced in the document.

29. Page 143, Appendix F Database Schema for SAPHIRE 8.
    Appendix F is not referenced in the document.

30. Page 205, Appendix G API Module Unit Summaries and List of External Procedure Calls.
    Appendix G is not referenced in the document.

31. Page 206, Appendix G API Module Unit Summaries and List of External Procedure Calls.
    Under the Module: API_BlockDiagrams.pas, the routine
    "*BlockDiagram_DeleteBlockDiagram*" is listed twice.
    Provide corrections as necessary.

32. Page 215, Appendix G API Module Unit Summaries and List of External Procedure Calls.
    Under the Module: API_RiskErr.pas, the routine no routines are listed.
    Provide corrections as necessary.

33. Page 7, section 5.3 Quality Assurance and Assessment Approach.
    Figure 5-1 is not included in the list of FIGURES in the table of contents.
    Please add the figure to the list of FIGURES in the table of contents.

34. Page 10, section 5.5 Change Design and Testing Procedure.
    Figure 2 is not included in the list of FIGURES in the table of contents.
    Please add the figure to the list of FIGURES in the table of contents.

35. Page 14, section 6.2 User-Interface Testing.
    Table 6-1 is not included in the list of TABLES in the table of contents.
    Please add the table to the list of TABLES in the table of contents.

36. Page 23, section 7.1.1.1 PRA Analysis Levels.
    Provide reference to Figure 6.1.

37. Page 26, section 7.1.1.3 Plant Models Available In SAPHIRE 8.0.
    Table 7.1.1.3-1 is not included in the list of TABLES in the table of contents.
    Please add the table to the list of TABLES in the table of contents.

38. Page 30, section 7.1.1.3 Plant Models Available In SAPHIRE 8.0.
    Table 7.1.1.3-2 is not included in the list of TABLES in the table of contents.
    Please add the table to the list of TABLES in the table of contents.

39. Page 32, section 7.1.1.3 Plant Models Available In SAPHIRE 8.0.

Table 7.1.1.3-3 is not included in the list of TABLES in the table of contents.
Please add the table to the list of TABLES in the table of contents.

40. Page 55, section 7.5 Requirements Validation.
The figure showing an example of the types of summary information contained in the RTM is not included in the list of FIGURES in the table of contents or referenced in the document and does not have a figure caption.
Provide reference to the figure, add the figure to the list of FIGURES in the table of contents and add a figure caption.

41. Page 57, section 8 Test Phases.
The figure showing test phases is not included in the list of FIGURES in the table of contents or referenced in the document and does not have a figure caption.
Provide reference to the figure, add the figure to the list of FIGURES in the table of contents and add a figure caption.

42. Page 65, section 8.2 Participants.
The table showing SAPHIRE 8 participants is not included in the list of TABLES in the table of contents or referenced in the document and does not have a table caption.
Provide reference to the table, add the table to the list of TABLES in the table of contents and add a table caption.

4.0 IV&V Evaluation Checklist

SOFTWARE DESIGN and INTERFACE DESIGN		
Criteria: 1	**Does the Software Design Specification (SDS) present the structure of the software such that it can be translated into code? NUREG/BR-0167 Section 4.4**	
Pass		Comments
Fail	X	Section 4.1.2 Project controls does not contain design information. Section 4.1.5 Project-Wide Search Design specifies "*This functionality is currently in the concept stage of design.*" These two sections need to provide software design information. Section 4.1.8 External Events Design does not contain design information leading into the design information presented within subsections 4.1.8.1 thru 4.1.8.5. Section 4.7 Phase Mission Design does not contain design information leading into the design information presented with subsections 4.7.1 thru 4.7.4.2. Section 4.4.5 End State Object Design specifies "*End state objects are currently under development*", then the paragraph following goes into the End State Object Design. Section 4.5.9 General Analysis Design specifies "*This analysis is currently in the development stage of design*" then goes into the General Analysis Design. The consistency of detail between design components varies. For example refer to section 4.1.1 Access to Top Level Objects Design and section 4.5.8 ECA Analysis Design.
N/A		
Criteria: 2	**Does the SDS provide a description of the major elements/components of the software as related to the requirements in the SRS? NUREG/BR-0167 Section 4.4**	
Pass		Comments
Fail	X	Section 4.1.2 Project controls does not contain design information. Section 4.1.5 Project-Wide Search Design specifies "*This functionality is currently in the concept stage of design.*" These two sections need to provide software design information. The Requirements Traceability Matrix (RTM) as presented in the SAPHIRE Version 8 Software Verification and Validation Plan – Volume II, Appendix D Requirements Traceability Matrix, (INL/EXT-05-00821) is incomplete and currently does not show the traceability between software design components and software requirements. The design components are not uniquely identified. For example: Section 2.4.1 Model Creation and Maintenance specifies "*The limit on SAPHIRE accident sequence objects will be 2,000,000.*" This requirement could be considered a "Function" requirement since it describes a function that the software will perform. The requirement could be uniquely identified as: FR-01 - "*The limit on SAPHIRE accident sequence objects will be 2,000,000.*" Section 2.4.6 Sequence Object specifies "*The total number of sequences available will be up to 2,000,000.*" This requirement could be considered a "Function" requirement since it describes a function that the software will perform.
N/A		

		The requirement could be uniquely identified as: FR-02 - "*The total number of sequences available will be up to 2,000,000.*" Section 4.4.6 Sequence Object Design specifies "*The sequence object contains the declarations, methods (procedures and functions) and properties for specifying a sequence. The items contained within this object are used within the event tree, fault tree and end state objects.*" The design component could be uniquely identified as: Size_1 – "*The sequence object contains the declarations, methods (procedures and functions) and properties for specifying a sequence. The items contained within this object are used within the event tree, fault tree and end state objects.*" The description for test case Test-63 is "*Sequence Stress Testing*". Traceability can now be shown for the example above: Software requirements FR-01, FR-02 map to design component Size_1 which map to test case Test-63.
Criteria: 3	**Does the SDS provide a technical description in terms of the theoretical basis? NUREG/BR-0167 Section 4.4**	
Pass	X	Comments
Fail		Refer to section 1.1 System Description.
N/A		
Criteria: 4	**Does the SDS provide a technical description in terms of the mathematical model? NUREG/BR-0167 Section 4.4**	
Pass	X	Comments
Fail		Refer to sections 4.5 Core Analysis Design, 4.7 Phase Mission Design, 4.8 Common Cause Failure Module Design, 4.10 Level 2 Design.
N/A		
Criteria: 5	**Does the SDS provide a technical description of the data flow(s) and data structure(s)? NUREG/BR-0167 Section 4.4**	
Pass	X	Comments
Fail		Refer to sections 4.1.8.1 General Model Type Information, section 4.3.1 General SAGE-ST Tool Description, section 4.4.6 Sequence Object Design, section 4.6 Embedded Macro Design, section 4.7.1 General Phase Information, section 4.9.1 General Model Type Information, SAPHIRE Version 8 Software Verification and Validation Plan – Volume II, Appendix F Database Schema for SAPHIRE 8, (INL/EXT-05-00821).
N/A		
Criteria: 6	**Does the SDS provide the defined range of input values? NUREG/BR-0167 Section 3.2.4.1 (boundary conditions)**	
Pass	X	Comments
Fail		Various discussions of inputs are found throughout section 4 Design Specification. Refer to section 4.1.6 User Selectable Constants Design, section 4.1.8 External Events Design, section 4.4 Core Modeling Design "*The input screens will be dynamic and display only relevant information based on previous user selection and input.*", section 4.5 Core Analysis Design, 4.7 Phase Mission Design, 4.8 Common Cause Failure Module Design, 4.9 External Events Design, section 4.10 Level 2 Design, section 4.11 SDP Workspace Design, section 4.12 Events and Condition Assessment Workspace Design.
N/A		
Criteria: 7	**Does the SDS provide the defined range of output values? NUREG/BR-0167 Section 3.2.4.1 (boundary conditions)**	
Pass	X	Comments
Fail		Various discussions of outputs are found throughout section 4 Design Specification.
N/A		

		Refer to section 4.1.6 User Selectable Constants Design, section 4.5 Core Analysis Design.
Criteria: 8	**Has the “Test Plan” and “Test Suite” for validating the software (by the development team) been addressed? NUREG/BR-0167 Appendix B**	
Pass	X	Comments
Fail		Refer to section 4.6 Embedded Macro Design. The SAPHIRE Version 8 Software Verification and Validation Plan – Volume II (INL/EXT-05-00821), sections 6 Test Specification, 7 Test Methodologies, 8 Test Phases and 9 Development and Test Environment address these criteria.
N/A		
Criteria: 9	**Has the RTM been updated to map the design components back to the defined requirements and are the design components/requirements mapped to test cases? NUREG/BR-0167 Section 4.3**	
Pass		Comments
Fail	X	The Requirements Traceability Matrix (RTM) as presented in the SAPHIRE Version 8 Software Verification and Validation Plan – Volume II, Appendix D Requirements Traceability Matrix, (INL/EXT-05-00821) is incomplete and currently does not show the traceability between software design components and software requirements. The RTM does not list design components that map to requirements. The test cases as listed in the RTM are incomplete (“NA”, “None”, “To be determined”). Refer to criteria 2.
N/A		
Criteria: 10	**Has the acceptance criteria for specifying how to determine the validity of the software provided, given the results of the test cases? NUREG/BR-0167 Section 2.6**	
Pass	X	Comments
Fail		The following sections presented in the SAPHIRE Version 8 Software Verification and Validation Plan – Volume II (INL/EXT-05-00821) specifies how to determine the validity of the software given the results of the test cases. Section 7.1.1.2 PRA Elements Embodied within SAPHIRE 8.0 specifies “*The success criteria are a specification of the compliment of equipment that must successfully operate to achieve functional success for each branch point or top event. This specification is developed analytically. The success criteria are used to define the boundary conditions for the failure modeling embodied within the corresponding fault tree.*” Section 7.2.1 Test Descriptions provides test results verification criteria. Section 3.4 Test Data specifies “*The test acceptance criteria ranged from a single value (e.g., total core damage frequency) to hundreds of similar values (e.g., core damage frequency from individual accident sequences) to a set of dissimilar values (e.g., different importance measures for fault trees, moments, and percentiles from uncertainty sampling). In all cases, though, knowledgeable PRA personnel or statisticians at INL obtained and verified the results.*” Section 8.3 Sources of Data specifies “*For each test, criteria are developed to determine if SAPHIRE accomplished a task. This generation of acceptance criteria results in a significant amount of information, since a test may use multiple PRA models. For example, the first test (Test-01) is performed using 82 different databases. Also, where applicable, the test evaluated the different mechanisms in SAPHIRE to accomplish the same task. An example of this aspect is the ability to generate end state cut sets using either the predefined end state categories (on the event tree) or using the end state partition rules.*”
N/A		

		Section 8.4 Entrance and Exit Criteria specifies "*The entrance criteria for testing are to obtain the stored test repository and associated project databases from the revision control system. The test scripts will be exercised as noted in the script.* *The exit criteria for testing are to check the suite test output results file for any failed tests. Note that one test has been designed to always fail and is used as a "false positive" results to ensure functionality of the designed comparison against the QA benchmarked results.*"
Criteria: 11	**Are the test case identifiers unique/unambiguous?** **NUREG/BR-0167 Section 6.2, 2.6.2**	
Pass	X	Comments
Fail		Test case identifiers are listed in the SAPHIRE Version 8 Software Verification and Validation Plan – Volume II (INL/EXT-05-00821), section 7.2.1 Test Descriptions.
N/A		
Criteria: 12	**Has a data dictionary been developed?** **Software Engineering Practices**	
Pass	X	Comments
Fail		The Data Dictionary has been developed. The Data Dictionary contains database table names, descriptions of the database tables and data types, data lengths and key information. The Data Dictionary does not contain information that defines items computed in the code, what they are and what they do. Define in the Data Dictionary items computed in the code, what they are and what they do.
N/A		
Criteria: 13	**If the SRS is found to require an update, has the SRS been updated, information represented correctly, completely, and accurately in the SRS?** **NUREG/BR-0167 Section 4.3, Section 6**	
Pass		Comments
Fail	X	Refer to document Independent Verification and Validation Of SAPHIRE 8 Software Requirements Project Number: N6423 U.S. Nuclear Regulatory Commission, Document ID: INL/EXT-09-16789 Revision 1.
N/A		
Criteria: 14	**Have all documents, including revised documents from the Requirements phase, been placed under Configuration Control and were Configuration Control procedures been performed completely and accurately?** **NUREG/BR-0167 Section 6**	
Pass	X	Comments
Fail		SAPHIRE Version 8 Software Verification and Validation Plan Volume I (INL/EXT-05-00821) and SAPHIRE Version 8 Software Verification and Validation Plan Volume II (INL/EXT-05-00821) are baselined using the revision control system (RCS) described in the Software Configuration Management Plan (INL/EXT-09-16696).
N/A		
Criteria: 15	**Have Peer Reviews, Software Requirements Reviews, Preliminary Design Reviews, Critical Design Reviews and Qualification Readiness Reviews been performed, with recorded results (usually via checklist or pre-approved form), and placed under configuration control? NOTE: IV&V activities require attendance at all major life-cycle reviews and audits.** **NUREG/BR-0167 Section 3.1 and 3.2.2, 3.2.3**	
Pass	X	Comments
Fail		Previous reviews, SAPHIRE 8 Build Alpha Preliminary Design Review April 25, 2006, SAPHIRE 8 Design Review from Audit August 9, 2007, Design Review Comments On SDP Interface NRC April 23 2008, SAPHIRE 8.0.3.31 Design Review Modifications to Cut Set Viewer April 24, 2008, Design Review From Audit December 3, 2008, current code reviews using the SAPHIRE Version 8 Software Verification and Validation Plan – Volume II (INL/EXT-05-00821), Appendix C Coding Standards are baselined using the revision control system (RCS) described in the Software Configuration Management Plan (INL/EXT-09-16696).
N/A		