Appendix A. Software System Hazard Analysis and Mitigation (Guidance)

Appendix A provides guidance on analyzing software to help ensure the necessary safety functions are met.

A. For ML-1 through ML-3 software, consider conducting and documenting a **software** hazard analysis at the system and component level to identify software risks and develop mitigating approaches for controlling them. Potential failures should be identified and evaluated for their consequences of failure and probability of occurrence. Some potential problems may include (1) complex or faulty algorithm, (2) lack of proper handling of incorrect data or error conditions, (3) buffer overflow, and (4) incorrect sequence of operations due to either logic or timing faults.

B. Ensure the software hazard analysis is consistent with the system safety documentation for the associated facility. See SBP111-1, *Facility Hazard Categorization and Documentation* for associated facility safety documentation.

C. For ML-1 and ML-2 software, perform and document the hazard analysis based on recognized consensus standards. See ESM Chapter 8, *Instrument & Controls* for application of hazard analysis/mitigation with respect to the following standards for SSC software:

- ANSI/Instrumentation, Systems, and Automation Society (ISA) S84.00.01, *Functional Safety: Safety Instrumented Systems for the Process industry Sector*; and,
- ANSI/IEEE Std 7-4.3.2, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations).

D. *For ML-3 software, standard-based methods or less formal methods should be used using a graded approach (e.g., failure modes and effects analysis, fault-tree modeling, event-tree modeling, cause-consequence diagrams, hazard and operability analysis, and interface analysis).*

E. For ML-4 software, a hazard analysis is not required but may be performed.

F. *Multiple/common-cause failures should be evaluated in the hazard analysis.*

Note: Failure mode and effect analysis (FMEA) approaches, when used alone, do not address multiple failures/common-cause failures. (ANSI/ISA 84.00-01-2004-Part 1 and IEEE STD-7-4.3.2-2003 provide guidance.)

G. The hazard analysis and design must include analysis and possible problems with the computer program's operating environment (including security environment) and external and internal abnormal conditions and events that can affect the computer program.

H. In the software design documentation (SWDD), as part of the SWHA, or in a separate deliverable, provide documentation that shows how the consequences of hazards/problems are mitigated. *Mitigation strategies should be included for:*

1. Software standard hazards (i.e., the basic hazards associated with the software or process);
2. Software system failures (i.e., the functionality written into the software itself to protect from failure); and
3. Software system overrides (i.e., the functionality written into the software to keep a user or other system from bypassing the safety features within the software item.)

If a standalone SWHA is desired, the document number may be assigned here.