

Handouts for Session 15 and Session 16

Slide 14, SRP Figure 7.0-A-3

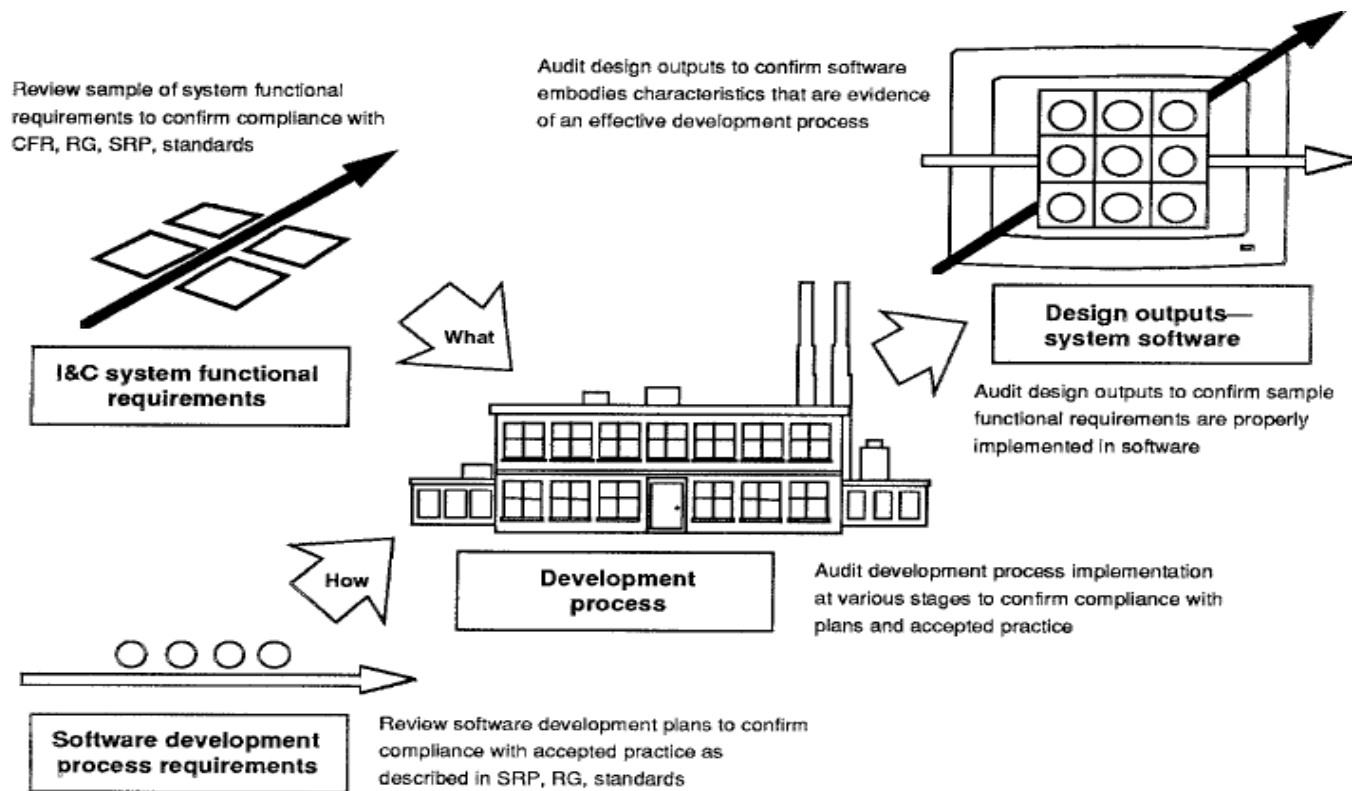


Figure 7.0-A-3. Software review process.

Slide 17, SRP 7, Appendix A

Life Cycle Activity Groups	Planning Activities	Requirements Activities	Design Activities	Implementation Activities	Integration Activities	Validation Activities	Installation Activities	Operation & Maintenance Activities
Software Management Plan	Requirements Specification	Design Specification	Code Listings	System Build Documents			Operations Manuals	
Software Development Plan							Installation Configuration Tables	
Software QA Plan								
Integration Plan								
Installation Plan								
Maintenance Plan								
Training Plan								
Operations Plan								
Software Safety Plan	Requirements Safety Analysis	Design Safety Analysis	Code Safety Analysis	Integration Safety Analysis	Validation Safety Analysis	Installation Safety Analysis		Design outputs
Software V&V Plan	V&V Requirements Analysis Report	V&V Design Analysis Report	V&V Implementation Analysis & Test Report	V&V Integration Analysis & Test Report	V&V Validation Analysis & Test Report	V&V Installation Analysis & Test Report		Process implementation
Software CM Plan	CM Requirements Report	CM Design Report	CM Implementation Report	CM Integration Report	CM Validation Report	CM Installation Report		Change Safety Analysis
								V&V Change Report
								CM Change Report

Process planning

Note: A separate document is not required for each topic identified; however, project docu-

Slide 25/26, IEEE Std 7-4.3.2

Table A.1— Mapping of IEEE Std 603-1998 to IEEE Std 7-4.3.2-2003

IEEE Std 603-1998 criteria	IEEE Std 7-4.3.2-2003 additional requirements	Annex for guidance
4. Safety system design basis	Safety system design basis	Annex B
5. Safety system criteria	None	Annex B
5.1 Single-failure criterion	None	—
5.2 Completion of protective action	None	—
5.3 Quality	Software development (see 5.3.1) Software tools (see 5.3.2) Verification and validation (see 5.3.3) Independent V&V (IV&V) requirements (see 5.3.4) Software configuration management (see 5.3.5) Software project risk management (see 5.3.6)	Annex D and Annex F
5.4 Equipment qualification	Testing software and diagnostics (see 5.4.1) Qualification of existing commercial computers (see 5.4.2)	Annex C
5.5 System integrity	Design for computer integrity (see 5.5.1) Design for test and calibration (see 5.5.2) Fault detection and self-diagnostics (see 5.5.3)	Annex B and Annex C
5.6 Independence	Independence (see 5.6)	Annex E
5.7 Capability for test and calibration	None	—
5.8 Information displays	None	—
5.9 Control of access	None	—
5.10 Repair	None	—
5.11 Identification	Identification (see 5.11)	—
5.12 Auxiliary features	None	—

Table A.1—Mapping of IEEE Std 603-1998 to IEEE Std 7-4.3.2-2003 *(continued)*

IEEE Std 603-1998 criteria	IEEE Std 7-4.3.2-2003 additional requirements	Annex for guidance
5.13 Multi-unit stations	None	—
5.14 Human factor considerations	None	—
5.15 Reliability	Reliability (see 5.15)	Annex F
6. Sense and command feature—Functional design requirements	None	—
7. Execute feature—Functional design requirements	None	—
8. Power source requirements	None	—

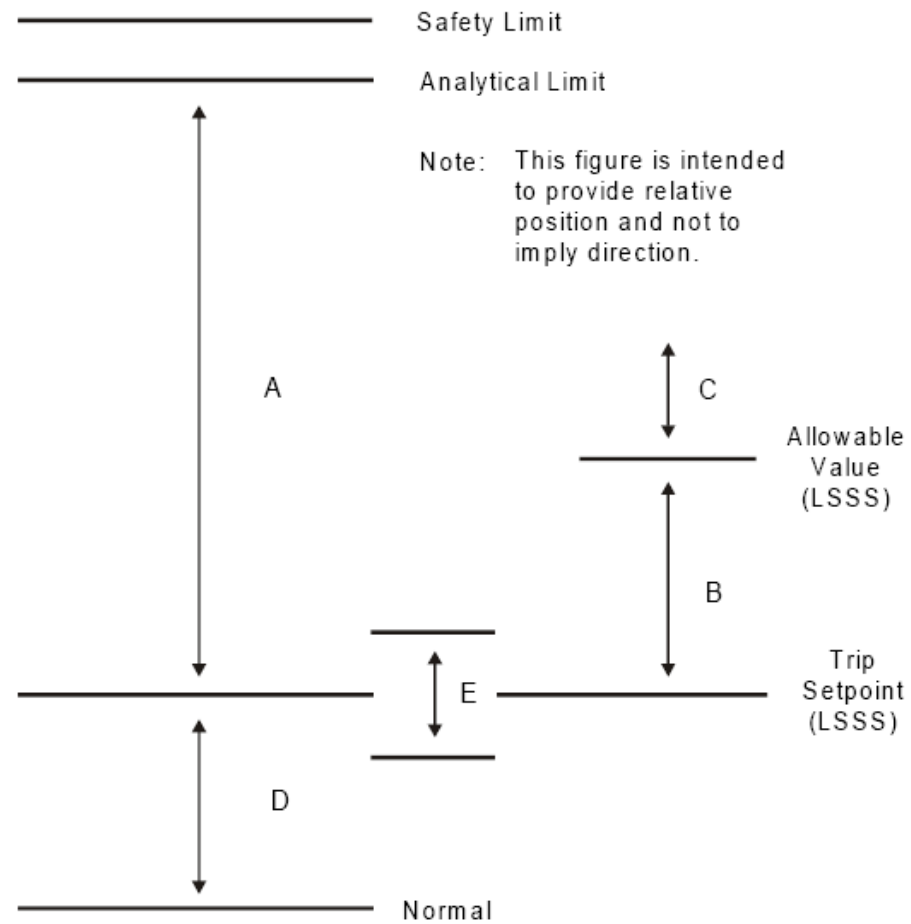
Table 1—SCM classes of information

Class of information	Description	IEEE Std 828-2005 reference	Plan reference
Introduction	Describes the Plan's purpose, scope of application, key terms, and references	3.1	1
SCM management	(Who?) Identifies the responsibilities and authorities for managing and accomplishing the planned SCM activities	3.2	2
SCM activities	(What?) Identifies all activities to be performed in applying to the project	3.3	3
SCM schedules	(When?) Identifies the required coordination of SCM activities with the other activities in the project	3.4	4
SCM resources	(How?) Identifies tools and physical and human resources required for execution of the Plan	3.5	5
SCM plan maintenance	Identifies how the Plan will be kept current while in effect	3.6	6

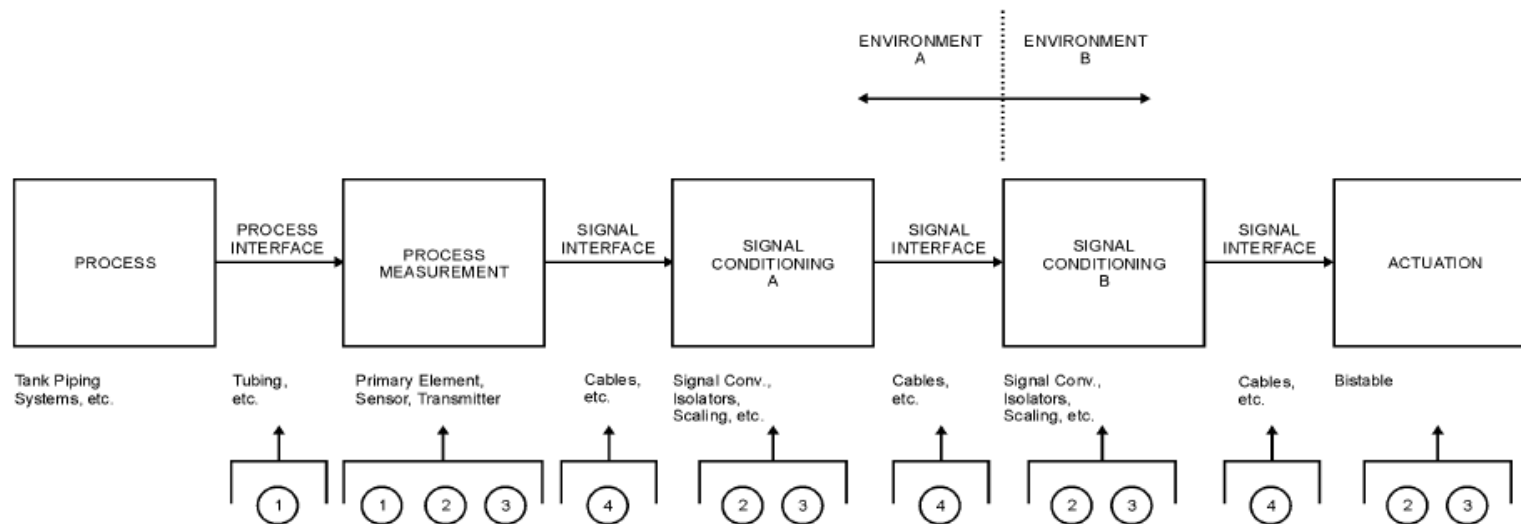
Table B.1—Assignment of software integrity levels

Software integrity level	Description
4	An error to a function or system feature that causes: —catastrophic consequences to the system with reasonable, probable, or occasional likelihood of occurrence of an operating state that contributes to the error; or —critical consequences with reasonable or probable likelihood of occurrence of an operating state that contributes to the error.
3	An error to a function or system feature that causes: —catastrophic consequences with occasional or infrequent likelihood of occurrence of an operating state that contributes to the error; or —critical consequences with probable or occasional likelihood of occurrence of an operating state that contributes to the error; or —marginal consequences with reasonable or probable likelihood of occurrence of an operating state that contributes to the error.
2	An error to a function or system feature that causes: —critical consequences with infrequent likelihood of occurrence of an operating state that contributes to the error; or —marginal consequences with probable or occasional likelihood of occurrence of an operating state that contributes to the error; or —negligible consequences with reasonable or probable likelihood of occurrence of an operating state that contributes to the error.
1	An error to a function or system feature that causes: —critical consequences with infrequent likelihood of occurrence of an operating state that contributes to the error; or —marginal consequences with occasional or infrequent occurrence of an operating state that contributes to the error; or —negligible consequences with probable, occasional, or infrequent likelihood of occurrence of an operating state that contributes to the error.

Slide 67, Setpoints



Slide 72, ISA 67.04.02



UNCERTAINTY ALLOWANCES

- ① Process Measurement Effects
- ② Instrument Uncertainty
- ③ Calibration Uncertainty
- ④ Other Uncertainties (IR, Leadwire Effects, etc.)