TABLE OF CONTENTS

This mandatory functional series document is available online at http://engstandards.lanl.gov.

It derives from P342, Engineering Standards, which is issued under the authority of the Conduct of Engineering program at the Laboratory.

RECORD OF REVISIONS

Rev	Date	Description	POC	OIC
0	11/17/03	Initial issue.	Tobin Oruch, FWO-DO	Gurinder Grewal, FWO-DO
1	10/27/06	Administrative changes only including org and contract reference updates from LANS transition; document number changes, etc.	Mel Burnett, FME-PSE	Kirk Christensen, CENG
1 Chg1	1/10/07	Added 5.1.H on common-cause failure of site systems.	Mel Burnett, FME-PSE	Kirk Christensen, CENG
2	2/23/11	Eliminated App A etc. in lieu of APs; update for 1189; was F1030.3	Tobin Oruch, CENG	Larry Goen, CENG

Please contact the ESM Nuclear POC for interpretation, variance, and upkeep issues.

F1030.70 NUCLEAR

1.0 APPLICATION OF CHAPTER

A. This chapter contains requirements that shall be followed in the design and construction of Hazard Category 1, 2, and 3 nuclear facilities -- both new construction and modifications (see Section 2.0 Acronyms and Definitions for definition of modification)[1]

Note: The use of the term facility in this section follows the definition of nuclear facility in 10 CFR 830 and includes process (programmatic) systems and activities.[2]

1. Activities associated with end-of-life (e.g., D&D) may be exempted from certain DOE O 420.1 requirements if adequately justified by approved safety analysis; seek variance per Chapter 1 Section Z10.
2. For projects that are Hazard Category 1, 2, and 3 nuclear facilities or include major modifications thereto (as defined in 10 CFR Part 830 [see Definitions at end of Z10]), the requirements in DOE-STD-1189, as amended, shall be fully implemented.
    1. The following documents must be submitted: Safety Design Strategy (CD-1), Conceptual Safety Design Report (CD-1), Preliminary Safety Design Report (CD-2), Preliminary Documented Safety Analysis (CD-3), and Documented Safety Analysis with Technical Safety Requirements (CD-4). For major modifications, the Conceptual Safety Design Report (CSDR) and the Preliminary Safety Design Report (PSDR) may either be separate documents or be subsumed within the Preliminary Documented Safety Analysis. The need to maintain the CSDR and PSDR as separate documents shall be based on the design development phases. Projects with conceptual and/or preliminary design phases shall develop the corresponding safety documentation.[3]

B. *This chapter helps ensure that nuclear activities and facilities are designed and constructed to prevent accidents and mitigate consequences; yet are efficient, convenient, and adequate for good service; minimize the generation of radioactive and mixed wastes; and are maintainable, standardized, and adequate for future expansion.*

C. *This chapter, along with other chapters of the Engineering Standards Manual, comprehensively implement design requirements and guidance in DOE O 420.1B, Facility Safety, and its two guides, (1) DOE G 420.1-1, Nonreactor Nuclear Safety Design Criteria and Explosive Safety Criteria Guide for use with DOE O 420.1 Facility Safety and (2) DOE G 420.1-2, Guide for the Mitigation of Natural Phenomena Hazards for DOE Nuclear Facilities and Non-Nuclear Facilities, along with containing additional requirements.*

D. Follow additional requirements specific to nuclear design elsewhere in the ESM (*primarily Chapter 4—Structural, Ch 5—Mechanical, Ch 7—Electrical, and Ch 10-Hazardous*).

WARNING: Failure to comply with the DOE O 420.1-based requirements in this chapter could result in civil and criminal enforcement under the Price-Anderson Amendments Act because 10CFR830 invokes 420.1B. LANL cannot wavier 420.1 requirements without formal NNSA concurrence.

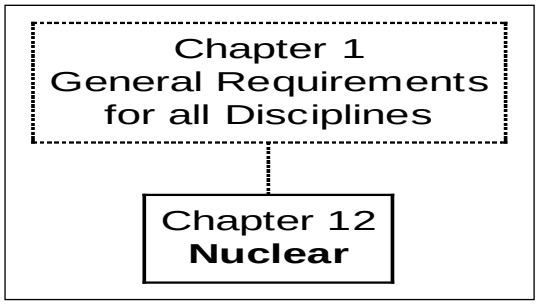
[1] DOE O 420.1B, Ch I
[2] 10 CFR 830 Sec. 803: *Nuclear facility* means a reactor or a nonreactor nuclear facility where an activity is conducted for or on behalf of DOE and includes any related area, structure, facility, or activity to the extent necessary to ensure proper implementation of the requirements established by this Part
[3] DOE O 413.3B CRD (Att 1), Item 13

Note: Guidance statements are in *italics* or are otherwise clearly indicated

E. All new **facility**-related design, material, equipment, and installations shall comply with the requirements in this chapter and Chapter 1 of the ESM. **This entire chapter is also applicable to programmatic structures, systems, and components (SSC) unless specifically noted otherwise.**

F. Issuance of this chapter does not require the modification of existing SSCs and projects to conform (see ESM Chapter 1 Section Z10 on Code of Record).

G. The hierarchy and the organization of the ESM for this chapter is depicted below:



2.0 ACRONYMS AND DEFINITIONS

CDR	conceptual design report
Design Agency	The organization performing the detailed design and analysis of a project or modification
Design Authority	The person responsible for the final acceptability of and changes to the design of a system or component and its technical baseline (typically the manager of engineering or his designee)
DBA	design basis accident
DC	design criteria
DSA	Documented safety analysis means a documented analysis of the extent to which a nuclear facility can be operated safely with respect to workers, the public, and the environment, including a description of the conditions, safe boundaries, and hazard controls that provide the basis for ensuring safety [10 CFR 830.3]. **Note**: DSAs may take the form of safety analysis report (SAR), basis for interim operation (BIO), or health and safety plan (HASP). The process involves production of a hazards inventory (HI), preliminary hazards analysis (PHA) and HA, and – for Haz Cat 2s and 3s – an accident analysis (AA).
ESM	Engineering Standards Manual
Facility	Normally at LANL, facility is a synonym for "real property and installed equipment." RP&IE is the land, improvements on the land such as buildings, roads, fences, bridges, and utility systems and the equipment installed as part of the basic building construction that is essential to normal functioning of a building space, such as plumbing, electrical and mechanical systems. This property/equipment is also referred to as institutional or plant and was formerly known as Class A. [from DOE Order 4330.4B]

	In the context of this chapter, however, facility refers to the definition of nuclear facility in 10 CFR 830 that includes process (programmatic) systems and activities.
FDD	facility design description
Hazard Category	The DOE-STD-1027 category as governed by SBP 111-1, *Facility Hazard Categorization and Documentation*
ITS	Important to safety (here, those defense in depth SSCs that are not SC or SS).
ML	management level, defined by AP-341-502, Management Level Determination.
modification	When used generically, this is any change to the form, fit, or function of an SSC, or the addition or removal of an SSC to a facility or activity. For this chapter only, all modifications shall follow DOE O 420.1B and its Guides as implemented by this ESM chapter and others unless, during the design process, the design authority determines and the design agency documents that the modification will not trigger one or more of the following: • Mission change or introduce a technology that is new to the facility • Positive USQ • Technical safety requirement (TSR) change • Significantly increased probability or consequence of a nuclear accident • Changes that go beyond those necessary for day-to-day operations • Changes that management has predetermined to submit to DOE for safety review and approval
NPH	Natural phenomena hazards include seismic (earthquake), wind, volcanic eruption and ash fall, lightning strikes, range fires, snow loads, and extreme temperatures.
non-reactor nuclear facility	Means "those facilities, activities or operations that involve, or will involve, radioactive and/or fissionable materials in such form and quantity that a nuclear or a nuclear explosive hazard potentially exists to workers, the public, or the environment, but does not include accelerators and their operations and does not include activities involving only incidental use and generation of radioactive materials or radiation such as check and calibration sources, use of radioactive sources in research and experimental and analytical laboratory activities, electron microscopes, and X-ray machines." (10 CFR 830.3)
PDSA	preliminary documented safety analysis
priority drawings	Priority drawings include the small set of "upper-tier" design drawings that are necessary to support the safe performance of facility operations, maintenance, and design activities within the facility's approved safety envelope. These drawings typically include piping & instrumentation diagrams, emergency evacuation maps (e.g., floor plans), and electrical one-lines. [AP-341-405, *Identification and Control of Technical Baseline in Operating Facilities.]*
Programmatic/ PP&PE	A synonym for Personal Property and Programmatic Equipment. PP&PE is equipment used purely for programmatic purposes, such as reactors, accelerator machinery, chemical processing lines, lasers, computers, machine tools, etc., and the support equipment dedicated to the programmatic purpose. This property/equipment is also referred to as organizational, research, production, operating or process and was formerly known as Class B. [DOE Order 4330.4B]

Safety Class (SC) SSC	*Safety class structures, systems, and components* means the structures, systems, or components, including portions of process systems, whose preventive or mitigative function is necessary to limit radioactive hazardous material exposure to the public, as determined from safety analyses. [10 CFR 830: § 830.3 Definitions.]
Safety SSC	A term meaning safety class, safety significant, and safety-impacting ML-1 and ML-2 SSCs; any of these could potentially impact worker or public safety or the environment if they failed.
Safety Significant (SS)	Structures, systems, and components which are not designated as safety-class SSCs but whose preventive or mitigative function is a major contributor to defense in depth and/or worker safety as determined from safety analyses. [10 CFR 830] As a general rule of thumb, safety-significant SSC designations based on worker safety are limited to those systems, structures, or components whose failure is estimated to result in a prompt worker fatality or serious injuries or significant radiological or chemical exposures to workers. The term, serious injuries, as used in this definition, refers to medical treatment for immediately life-threatening or permanently disabling injuries (e.g., loss of eye, loss of limb). The general rule of thumb cited above is neither an evaluation guideline nor a quantitative criterion. It represents a lower threshold of concern for which safety-significant SSC designation may be warranted. Estimates of worker consequences for the purpose of safety-significant SSC designation are not intended to require detailed analytical modeling. Considerations should be based on engineering judgment of possible effects and the potential added value of safety-significant SSC designation. [DOE G 420.1-1]
SDD	System design description. Required format in DOE-STD-3024, DOE Standard Content of System Design Descriptions
SSC	structures, systems, and components
USQ	*Unreviewed safety question (USQ)* means a situation where: (1) The probability of the occurrence or the consequences of an accident or the malfunction of equipment important to safety previously evaluated in the documented safety analysis could be increased; (2) The possibility of an accident or malfunction of a different type than any evaluated previously in the documented safety analysis could be created; (3) A margin of safety could be reduced; or (4) The documented safety analysis may not be bounding or may be otherwise inadequate. *Unreviewed safety question process* means the mechanism for keeping a safety basis current by reviewing potential unreviewed safety questions, reporting unreviewed safety questions to DOE, and obtaining approval from DOE prior to taking any action that involves an unreviewed safety question [10 CFR 830: § 830.3 Definitions]

3.0 ESTABLISHING TECHNICAL REQUIREMENTS AND DESIGN CRITERIA

A. Design personnel shall work to produce designs to best meet the technical requirements of the design criteria and functional and operational requirements, and not begin until these requirements are properly documented. Conversely, design elements over and above or not required by the DC and F&OR documents shall not be included without an approved baseline change authorization.[4]

B. Tailoring: Where this chapter allows tailoring of national or DOE standards (i.e., determining which parts of a standard apply to a project or how their intent is satisfied), document the thought processes followed during the tailoring and, for facility projects, submit for Building Official review along with each design review submittal (*e.g., CDR, 30%, 60%, 90%)* per ESM Chapter 16.

Guidance: As the design progresses the design criteria should be further refined and made specific to the SSCs if not already so. For instance, safety and non-safety SSCs will have different standards applied.

4.0 MAINTAINING TECHNICAL REQUIREMENTS DOCUMENTS AND DESIGN CRITERIA DURING DESIGN

A. The project management and/or design team shall employ a design and construction phase configuration management program to maintain consistency between the technical baseline (including system requirements and performance criteria), the design documentation, and the as-built conditions.[5]

B. *Project documentation should be validated against the actual physical configuration and manufacturer's documentation of facility and process SSCs during design and again during construction.*[6]

C. When required by ESM Chapter 1 Section Z10, originating personnel, project management personnel, and/or design personnel shall develop and maintain appropriately detailed FDD, SDDs, priority drawings and other critical drawings and documentation during the design and construction process. The FDD and SDDs shall be started during conceptual phase; *it is recommended they be started at pre-conceptual phase. Further guidance: The FDD and SDDs should adequately reflect the requirements contained in the draft safety analysis (which is still changing). SDDs are a good way to start documenting system purpose, functional requirements, applicable codes and standards, system interfaces etc. as the Process Flow Diagrams and design development is started. This information is very important for reviewers. Usually it is beneficial to the design agency to put at least functional requirements, applicable codes and standards under change control prior to start of the preliminary design in order to minimize late changes to system requirements by the customer. This activity should directly support facility safety basis development and documentation.*

D. *For projects with over $200k design cost, the design requirements should be incorporated into an equipment database that correlates each SSC with the SSC grade, the design requirements, technical topics involved, and associated documentation.*[7]

---

[4] To produce an effective design efficiently, the requestor must establish the most basic criteria at the outset of the process since these have a major effect on how design is performed. Failing to do so can result in costly rework or a tendency for schedule-driven design compromises.

[5] DOE O 420.1B Ch V 3(c)

[6] DOE O 420.1B Ch V 3(c)

E. *System and Process Boundaries: The boundaries for each system and process should be established in such a manner as to contain the components necessary to satisfy the design requirements for that system or process. See ESM Chapter 1 Sections 210 and 220.*[8]

F. *Specific Equipment List: On the basis of the equipment scope criteria and the assignment of SSC grades, the specific SSCs included in the CM program should be identified. Ref*: AP-341-404, *Master Equipment List.*[9]

G. Establishment of Design Basis: The basis for design decisions, whether inclusions or exclusions, shall be formally established and documented, and correlated with the design and/or the function and other design requirements (e.g., RCD, F&OR).[10]

1. *A technical management review should be performed to determine the adequacy of the design basis. If the design basis is not fully documented, not accurate, or not complete, it should be reconstituted to the extent identified by the design reconstitution adjunct program.*
2. *The design basis for new or modified design requirements should be established and documented as these requirements are developed.*

5.0 NUCLEAR SAFETY DESIGN

5.1 General

A. Defense-in-depth concepts shall be used for the design of nuclear facilities to provide multiple layers to protect against the uncontrolled release of radioactive materials. Defense in depth shall include, as applicable: [11]

1. Site selection[12]
2. Minimizing hazardous material at risk [13]
3. Use of conservative design margins and quality assurance
4. Use of successive physical barriers for protection against the release of radioactivity
5. Provision of multiple means to ensure critical safety functions (those basic safety functions needed to control the processes, maintain them in a safe state, and to confine and mitigate radioactivity associated with the potential for accidents with significant public radiological impact)
6. Use of equipment and administrative controls that restrict deviations from normal operations and provide for recovery from accidents to achieve a safe condition[14]
7. Ability to monitor and record radiological releases to the environment and to initiate an emergency response (coordinate with ER-Emergency Management & Response Group)

---

[7] DOE O 420.1B Ch V 3(c).and DOE-STD-1073-93, 2.2.1, 2nd paragraph.
http://www.hss.doe.gov/nuclearsafety/ns/techstds/standard/std1073/doe-std-1073-2003.pdf
[8] DOE-STD-1073-93 1.3.2
[9] DOE-STD-1073-93-1.3.2
[10] DOE-STD-1073-93 1.3.2
[11] DOE O 420.1B, Ch I Section 3.b
[12] Details on siting covered in the Guide, section 3.2. This is going into LIR 210-01-01 in 2003
[13] This is both a design (such as for a process system) and an operational tool
[14] Shows that ACs are considered along with engineered features when deciding upon an appropriate controls set

B. Locate (site) and design facilities to give adequate protection for the health and safety of the public and for workers, including those at adjacent facilities, from the effects of potential facility accidents involving the release of radioactive materials.[15]

C. Confine uncontained radioactive materials. Provide material handling equipment and containment structures or gloveboxes to allow for the safe handling of radioactive materials not contained within appropriate storage containers if required by project or programmatic needs. Additional requirements are contained in ESM Chapter 6, Mechanical, especially Subsection E1020. [16]

D. Design the safety SSCs identified by the safety analysis so that they can perform their safety functions when called upon to operate.[17]

E. Provide input to the PDSA/DSA effort to select safety SSCs using the following criteria to the extent possible. [18]

1. Minimization of hazardous materials at risk (minimization of the amount of material to be processed at one time and the total quantity to be stored) is the first priority.
2. Safety SSCs are preferred over administrative controls.
3. Passive SSCs are preferred over active SSCs.
4. Preventative controls are preferred over mitigative controls.
5. Facility safety SSCs are preferred over personal protective equipment.
6. Select controls closest to the hazard that will provide best protection to both workers and the public.
7. Controls that are effective for multiple hazards can be resource effective.

F. *Design consideration should be given to the interaction of more than one event, particularly those more likely to occur simultaneously. For example, heavy rains usually accompany tornadoes or high winds; excessive roof loads may result from rain and accumulated volcanic ash; and upstream dams may fail due to seismic events.*[19]

G. *Common Cause: The design and evaluation process should consider potential damage and failure of SSCs due to both direct natural phenomena effects, including common cause, and indirect natural phenomena effects, including interaction with other SSCs (discussed above). Regarding common cause, the occurrence of a natural phenomena event, especially an earthquake, affects many or all SSCs in a facility or across an entire site. Common cause effects are failures due to a single event that might otherwise be assumed to be independent. Hence, it is possible to have multiple natural phenomena-induced ("non-ambient environmental stress induced") failures of SSCs. These common cause effects must be considered in design or evaluation. For example, an earthquake could simultaneously initiate a fire in a facility and cause failure of the water supply for the fire suppression system. A recent study has shown that LANL's fire water supply may not be reliable for fire suppression during a significant earthquake; therefore, the design and DSA must document alternative methods for assuring fire suppression if required under these circumstances. Other sitewide*

[15] DOE O 420.1B, Ch I Section 3.b adds the requirement that workers in adjacent facilities be specifically considered. This is not specified in a nuclear safety analysis (3009 for example). Limited to radioactive material releases
[16] DOE O 420.1B, Ch I Section 3.b . Confinement requirement (additional details in same section of 420.1)
[17] DOE O 420. 1B, Ch I Section 3.b
[18] DOE G 420.1-1, Section 2.1.1, Functional Classification of Safety Systems. Note this also echoes the requirements in DOE-STD-3009, Attachment A
[19] DOE G 420.1-1, Section 3.3.3 – Consideration of interaction of NPH events beyond general guidelines in DOE O 420.1 and its NPH guide

services that must also be evaluated (and possibly augmented) if they are to be relied upon during the specific scenarios are electrical power and communications.[20]

H. *Preventative Features: Preventive features should be considered in the design to prevent abnormal facility and process activity conditions from progressing to accidents. This consideration includes design features providing a return to normal operation or return to a safe condition. It may also include automatic system response to such events or may be monitors that alert operators to the necessity of taking manual action.*[21]

I. Mitigating Features: Provide safety SSCs to mitigate consequences of accidents that may still occur despite the application of the preceding conventions. Ensure these safety SSCs are identified through the PDSA and DSA.[22]

J. Consider the guidance in applicable DOE Standards including DOE-STD-1132, Design Considerations. *Also reference DOE EH Office of Nuclear & Facility Safety Policy and Safety Design Page*

5.2 Reliability

A. Design, fabricate, erect, and test safety SSCs and their associated support systems to standards and quality requirements commensurate with their importance to safety. *An acceptable level of assurance that the safety SSCs will perform their intended safety functions can be achieved by meeting the requirements contained within the following paragraphs.*[23]

B. Assurance of Safety Function: Design safety SSCs to reliably perform their safety functions under those conditions and events for which their safety functions are intended as indicated in the safety analysis. [24]*Further design guidance can be found in IEEE 603, Standard Criteria for Safety Systems for Nuclear Power Generating Stations.*

C. Conservative Design: Design safety SSCs to withstand all design basis loadings with an appropriate margin of safety.

1. *The design should incorporate, commensurate with the importance of the safety function, multiple levels of protection against normal, anticipated, and accident conditions.*[25]
2. *Design margins that account for deviations from normal process parameters. The facility and process activity design also should accommodate means such as monitors and automatic and manual controls to restrict deviations from normal operations and to assist recovery during the early stages of an accident sequence.*[26]
3. Design safety-class SSCs to the suitably conservative criteria contained in applicable DOE orders and standards addressing safety functions (e.g., natural phenomena design mitigation[27]). *Guidance: These criteria are largely captured by the ESM in this and other chapters*.).

[20] DOE G 420.1-2 Sect. 6.2.1; DOE-STD-3009-94, Change Notice 2, April 2002, "Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analysis" Sections 4.3.X.3 and 4.4.X.3; "Issue 03-011, Number 75 -- Perform Sitewide Water System Fragility Study," Mertz, Salmon, and Cardon.
[21] DOE G 420.1-1, Section 3.1.3.
[22] DOE G 420.1-1, Section 3.1.4.
[23] DOE G 420.1-1, Section 5.1.
[24] DOE G 420.1-1, Section 5.1.1.
[25] DOE G 420.1-1, Section 5.1.1.1 – Conservative design features.
[26] DOE G 420.1-1, Section 3.1.2.
[27] DOE G 420.1-1, Section 5.1.1.1 – Conservative design features.

D. Design against single-point failure: Design SSCs to perform all safety functions with the reliability indicated by the PDSA.[28] *Guidance: The PDSA does not generally supply reliability requirements directly, but describes the frequency and severity of accidents that are prevented/mitigated by the safety SSCs. From this information, a quantitative reliability is determined for the design of safety class SSC. For safety significant design, best industry practice as required by the ESM is generally sufficient and no quantitative reliability analysis is required (the exception is I&C design in which industry practice – i.e., ISA 84.01 -- does result in quantitative understanding of the probability of failure on demand).*

1. Apply the single-point failure criterion, requirements, and design analysis identified in IEEE 379, *Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems*, during the design process as the primary method of achieving this reliability.[29]

E. Environmental Qualification: Design SC SSCs to perform all safety functions, as determined by the DSA, with no failure mechanism that could lead to common cause failures under postulated service conditions. The requirements from IEEE 323, Standard for qualifying Class 1E equipment for nuclear power generating stations**,** for mild environmental qualification shall be used unless the environments in which the SSC is located changes significantly as a result of the DBAs. Additional seismic qualification requirements are addressed in ESM Chapter 5, Structural. *Guidance*: *In general, qualification for mild environments should consist of two elements:*[30]

1. *Ensuring that all equipment is selected for application to the specific service conditions based on sound engineering practices and manufacturers' recommendations.*
2. *Ensuring that the system documentation includes controls that will preserve the relationship between equipment application and service conditions.*

F. The design shall provide reliable safe conditions and sufficient confinement of nuclear and hazardous material during and after all DBAs. At both the facility and SSC level, the design shall ensure that more probable modes of failure (e.g., fail to open versus fail to close) will increase the likelihood of a safe condition. [31]

G. Within the flexibility allowed by the ESM, tailor selections of codes and standards for each specific application based on the required safety function.[32]

H. *The safety analysis conducted per DOE-STD-3009 (or other approved DSA format) that results in a particular safety classification is also the same analysis used to identify and define design criteria.*[33]

I. *The national codes and standards listed in the ESM discipline chapters define the minimum aggregation of codes, standards, and standard practices that should be considered in identifying the design criteria and other considerations for each specific SSC commensurate with its function. Additional design criteria may be applied as necessary to perform the safety function.*[34]

---

[28] DOE G 420.1-1, Section 5.1.1.2 – Single point failure criterion.
[29] DOE G 420.1-1, Section 5.1.1.2 – Single point failure criterion.
[30] DOE G 420.1-1, Section 5.1.1.3 – Environmental qualification.
[31] DOE G 420.1-1, Section 5.1.1.4 – Safe failure modes.
[32] DOE G 420.1-1, Section 5.2 – Tailoring of codes and standards for safety functions.
[33] DOE G 420.1-1, Section 5.2 – Safety analysis design criteria relationship. Note that the safety analysis can be summarized and referenced in the PDSA or DSA.
[34] DOE G 420.1-1, Section 5.2 – this paragraph tailored to the LANL engineering standard. Assumes all the referenced codes

J. *A Reliability, Availability, and Maintainability (RAM) program should be established per best available guidance and graded as to the complexity and hazards of the facility. Some useful resources:*[35]

- http://www.sre.org—Society of Reliability Engineers.
- MIL-HDBK-470A, Designing and Developing Maintainable Products and Systems
- DOD-HDBK-791, Maintainability Design Techniques
- IEEE 352, IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems
- *Introduction to Reliability Engineering*, Lewis (at LANL Research Library)
- Eberling, Charles E. *An Introduction to Reliability and Maintainability Engineering*, McGraw-Hill, 1997.

5.3 Interfaces

A. *In some cases, safety SSCs rely upon supporting SSCs to perform the intended safety function. These support SSCs are classified the same as the SSCs they support. Refer to the PDSA/DSA to obtain the classification.*[36]

B. Minimize interfaces between SC, SS, and other SSCs.[37]

C. Evaluate interfaces to identify SSC failures that would prevent the safety SSCs from performing their intended safety function. *Guidance: For these SSC failures, isolation devices, interface barriers, or design class upgrades should be provided to ensure safety SSC protection and reliability.* [38]

D. *System interface evaluations should clearly define boundaries. In all instances, a case-by-case evaluation should be performed.*[39] *See ESM Chapter 1 Section 220, System Boundaries.*

5.4 Quality Assurance

A. *Design safety SSCs* under a quality assurance program that satisfies 10 CFR 830 Subpart A.[40]

B. Develop the QA requirements for the design, fabrication, construction, and modification of safety SSCs.[41]

1. *At the earliest stages of the design, the safety documents, which identify the functional requirements of safety SSCs, should be used as a basis for determining appropriate QA requirements.*[42]

---

and standards that follow in sections 5.2.X of the guide.
[35] DOE G 420.1-1, Section 3.5.
[36] DOE G 420.1-1, Section 5.1.2.1 – Support system safety classification
[37] DOE G 420.1-1, Section 5.1.2.2 – Interface design
[38] DOE G 420.1-1, Section 5.1.2.2 – Interface design
[39] DOE G 420.1-1, Section 5.1.2.2 – Interface design
[40] DOE O 420.1, Section 4.1.1.2, Safety SSC (safety class and safety significant) general design requirement
[41] DOE G 420.1-1, Section 5.1.3 – Quality assurance
[42] DOE G 420.1-1, Section 5.1.3 – Quality assurance

C. Procurement: Follow the requirements of 10 CFR 830 Subpart A in the procurement of all safety SSCs.

1. Document supplier quality and receipt inspection requirements. *These should state what will be inspected, how this will be performed, and who will perform.*
2. Ensure the supplier is qualified to provide the specific SSC (*LANL's QA-IQ Institutional Quality Group maintains an approved supplier list*). Alternatively, develop a commercial grade dedication for the SSC.
3. *In most cases, components used in DOE nonreactor nuclear facilities will be commercial grade (off the shelf); that is, they will not be from NQA-1 qualified suppliers. Therefore, safety SSC quality standards can either be design based or achieved through testing, vendor control, and inspection.*[43]
4. *See references in ESM Chapter 1 Section Z10 (Z1020).*

6.0 DESIGN/SAFETY ANALYSIS INTEGRATION FOR PROJECTS (GUIDANCE)

A. This section (6.0) supplements DOE-STD-1189 regarding how the design and safety analysis processes interface for nuclear facility projects. The discussion is for a new facility or modification using the DOE O 413.3 Critical Decisions. Most modification projects to existing facilities will follow a slightly different process and must also consider:

1. The existing SSCs that might be impacted,
2. The existing safety basis that will need to be kept current, the transitional states that may be achieved during construction if the facility is to remain fully or partially operational during the modification, and
3. The unplanned operational or construction upsets that might have an adverse affect on workers or the public.

B. LANL Project Management Directorate documents address many of the deliverables discussed in this section and should be used where required or applicable. Guidance on design steps at various project phases, including integration of design and safety, is also contained in DOE O 413.3, Project Management for the Acquisition of Capital Assets – and DOE O 430.1, Real Property Asset Management.

[43] DOE G 420.1-1, Section 5.1.3 – Quality assurance – Commercial off the shelf