

2.1 Evaluation of Defense-in-Depth Attributes and Safety Margins

One aspect of the engineering evaluation is to show that the proposed change does not compromise the fundamental safety principles on which the plant design was based. Design-basis accidents (DBAs) play a central role in the design of nuclear power plants. DBAs are a combination of postulated challenges and failure events against which plants are designed to ensure adequate and safe plant response. During the design process, plant response and associated safety margins are evaluated using assumptions of physical properties and operating characteristics that are intended to be conservative. National standards and other considerations such as defense-in-depth attributes and the single-failure criterion constitute additional engineering considerations that also influence plant design and operation. The licensee's proposed LB change may affect margins and defenses incorporated into the current plant design and operation; therefore, the licensee should reevaluate the safety margins and layers of defense to support a requested LB change. As part of this evaluation, the impact of the proposed LB change on the functional capability, reliability, and availability of affected equipment should be determined. The plant's LB identified in the FSAR is the reference point for judging whether a proposed change adversely affects safety margins or defense-in-depth. Sections 2.1.1 and 2.1.2 below provide guidance on assessing whether implementation of the proposed change maintains adequate safety margins and consistency with the defense-in-depth philosophy.

2.1.1 *Defense-in-Depth*

The engineering evaluation should evaluate whether the impact of the proposed LB change is consistent with the defense-in-depth philosophy. In this regard, the intent of this key principle of risk-informed decision-making is to ensure that any impact of the proposed LB change on defense-in-depth is fully understood and addressed and that the philosophy of defense-in-depth is maintained; not to prevent changes in the way defense-in-depth is achieved. The licensee must fully understand how the change will impact the design, operation and maintenance of the plant, both from risk and traditional engineering perspectives.

This section provides some background on the defense-in-depth philosophy. Next is discussion of seven key factors that may be used to evaluate the impact of a proposed change on defense-in-depth. One or more examples are provided to help illustrate what is meant by each factor. Finally, this section provides guidance on a process for evaluating the seven key factors, including an integrated example.

2.1.1.1 Background

Defense-in-depth is an element of the NRC's safety philosophy that employs successive compensatory measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs at a nuclear facility¹. The defense-in-depth philosophy has traditionally been applied in reactor design and operation to provide multiple means to accomplish safety functions and prevent the release of radioactive material. It has been and continues to be an effective way to account for uncertainties in equipment and human performance and, in particular, to account for the potential for unknown and unforeseen failure mechanisms or phenomena, which (because they are unknown or unforeseen) are not reflected in either the PRA or traditional engineering analyses.

In addition, there is some flexibility that can be gained in the operations and maintenance of the nuclear plant that leverages the implementation of the defense-in-depth philosophy in the design of the

¹ Staff Requirements Memorandum (SRM) - SECY-98-0144, "White Paper on Risk-Informed and Performance-Based Regulation," March 1, 1999, (Agencywide Document Access and Management System (ADAMS) accession number ML003753601)

Revised Draft of Section 2.1 from DG-1285 [7-27-16]

41 plant. For example, testing and maintenance of SSCs or corrective action to restore an engineered safety
42 system may be allowed for short periods while remaining at power, consistent with established Technical
43 Specifications. The NRC recognizes and allows these temporary configurations within these established
44 programs. If a licensee requests a risk-informed change to the plant's licensing basis to permit new or
45 extended entry into temporary conditions, the licensee should demonstrate that the plant condition is
46 justified and consistent with the defense-in-depth philosophy as described in this section.

47 For the purposes of this RG, nuclear power plant defense-in-depth is taken to consist of layers of
48 defense and successive measures to protect the public:

- 49 • Robust plant design to survive hazards and minimize challenges that could result in an event
50 occurring;
- 51 • Prevention of a severe accident (core damage) should an event occur;
- 52 • Containment of the source term should a severe accident occur; and,
- 53 • Protection of the public from any releases of radioactive material (through, e.g., siting in low
54 population areas and the ability to shelter or evacuate people if necessary).

55 2.1.1.2 Factors for Evaluating the Impact of LB Changes on Defense-in-Depth

56 Any one or more of the layers of defense discussed above may be adversely impacted by a
57 proposed change to a plant's licensing basis. The NRC has identified seven factors that should be used to
58 assess the impact of the change on defense-in-depth. These are discussed in detail below. Guidance on
59 how to apply these factors is discussed in more detail in section 2.1.1.3.

60 The NRC finds it acceptable for a licensee to use the following seven factors to evaluate whether
61 a proposed change to the LB maintains the philosophy of defense-in-depth.

- 62 1. Preserve a reasonable balance among the layers of defense.

63 A reasonable balance of the layers of defense—minimizing challenges to the plant, preventing
64 any events from progressing to core damage, containing the radioactive source term, and
65 emergency preparedness—helps to ensure an apportionment of the plant's capabilities between
66 limiting disturbances to the plant and mitigating their consequences. The term *reasonable*
67 *balance* is not meant to imply an equal apportionment of capabilities. A reasonable balance is
68 preserved if the proposed plant change does not significantly reduce the effectiveness of a layer
69 that exists in the plant design and operation before the proposed change. The NRC recognizes
70 that there may be aspects of a plant's design or operation that may cause one or more of the layers
71 to be adversely affected. For these situations, the balance between the other layers becomes
72 especially important when evaluating the impact of a proposed change to the LB and its impact
73 on defense-in-depth.

- 74 2. Preserve adequate capability of design features without an overreliance on programmatic
75 activities as compensatory measures.

76 Some proposed changes to the LB may involve or require compensatory measures; that is,
77 measures taken to compensate for some reduced functionality, availability, reliability,
78 redundancy, or other feature of the plant's design. Such compensatory measures are often
79 associated with temporary plant configurations. Compensatory measures may include hardware

Revised Draft of Section 2.1 from DG-1285 [7-27-16]

80 (e.g., skid-mounted temporary power supplies), human actions (e.g., manual system actuation), or
81 some combination of these measures. The preferred approach for accomplishing *safety functions*
82 is through engineered systems. Therefore, when a proposed change necessitates reliance on
83 *programmatic activities* as compensatory measures, the licensee should justify that this reliance is
84 not excessive.

85 Nuclear power plant licensees implement a number of programs, including, for example,
86 programs for quality assurance, testing and inspection, maintenance, control of transient
87 combustible material, foreign material exclusion, containment cleanliness, training, and so forth.
88 In some cases, activities taken as part of these programs are used to ensure safety functions; for
89 example, reactor vessel inspections that provide assurance that reactor vessel failure is unlikely.
90 The intent of this factor is not to preclude the use of such programs as compensatory measures,
91 but to ensure that the use of such measures does not significantly compromise the capability of
92 the design features (e.g., hardware).

93 3. Preserve system redundancy, independence, and diversity commensurate with the expected
94 frequency, consequences of challenges to the system, and uncertainties.

95 A substantial reduction in the ability to accomplish system safety functions is not consistent with
96 the defense-in-depth philosophy. The importance of system redundancy, independence and
97 diversity is to ensure that the system safety function can be achieved. As stated in Section 2.1.1
98 above, the defense-in-depth philosophy has traditionally been applied in reactor design and
99 operation to provide multiple means to accomplish safety functions. System redundancy,
100 independence, and diversity not only result in high availability and reliability of SSCs, but also
101 help ensure that system safety functions are not reliant on any single feature of the design.

102 A proposed risk-informed change should consider both safety-related and nonsafety-related SSCs
103 that are important to core damage or large early release. Redundancy provides for duplicate
104 equipment that enables the failure or unavailability of at least one set of equipment to be tolerated
105 without loss of function. Independence among equipment implies that the redundant equipment
106 are separate such that they do not rely on the same supports to function. It can sometimes be
107 achieved by the use of physical separation or physical protection. Diversity is accomplished by
108 having equipment that perform the same function rely on different attributes, such as different
109 principles of operation, different physical variables, different conditions of operation, or
110 production by different manufacturers.

111 4. Preserve adequate defense against potential common-cause failures (CCF).

112 An important aspect of ensuring defense-in-depth is to guard against CCF. Failure of several
113 devices or components to function may occur as a result of a single specific event or cause. Such
114 failures may simultaneously affect several different items important to risk. The event or cause
115 may be a design deficiency, a manufacturing deficiency, an operating or maintenance error, a
116 natural phenomenon, a human-induced event, or an unintended cascading effect from any other
117 operation or failure within the plant.

118 5. Maintain multiple fission product barriers.

119 Physical fission product barriers (e.g., the fuel cladding, reactor coolant system pressure
120 boundary, and containment) includes the physical barriers themselves and any equipment relied
121 upon to protect the barriers (e.g., containment spray). In general, these barriers are designed to
122 perform independently so that a complete failure of one barrier does not disable the next

Revised Draft of Section 2.1 from DG-1285 [7-27-16]

123 subsequent barrier. For example, one barrier, the containment, is designed to withstand a double-
124 ended guillotine break of the largest pipe in the reactor coolant system, another barrier.

125 A plant's licensing basis may contain events that, by their very nature, challenge multiple barriers
126 simultaneously. Examples include interfacing-system LOCA and SGTR. Therefore, complete
127 independence of barriers, while a goal, may not be achievable for all possible scenarios.

128 6. Preserve sufficient defense against human errors.

129 Human errors include the failure of operators to perform the actions necessary to operate the plant
130 or respond to off-normal conditions and accidents; errors committed during test and maintenance;
131 and other plant staff performing an incorrect action. Human errors can result in the degradation
132 or failure of a system to perform its function, thereby significantly reducing the effectiveness of
133 one of the defense-in-depth layers or one of the fission product barriers.

134 The plant design and operation includes defenses to prevent the occurrence of such errors and
135 events. These defenses generally involve the use of procedures, training, and human engineering;
136 however, other considerations, e.g., communication protocols, may also be important.

137 7. Continue to meet the intent of the plant's design criteria².

138 For plants licensed under 10 CFR Part 50 or Part 52, the plant's design criteria are set forth in the
139 current licensing basis of the plant, which is documented in the plant's FSAR, as updated. The
140 plant's design criteria define minimum requirements that achieve aspects of the defense-in-depth
141 philosophy; as a consequence, a compromise to those design criteria can directly result in a
142 significant reduction in the effectiveness of one or more of the defense-in-depth layers. When
143 evaluating the effect of the proposed change, the licensee should demonstrate that the intent of the
144 plant's design criteria continue to be met.

145 For plant's licensed under 10 CFR Part 52, this factor should also address those design features
146 for the prevention and mitigation of severe accidents that are described and analyzed in
147 accordance with 10 CFR 52.47(a)(23) for DC applications and 10 CFR 52.79(a)(38) for COL
148 applications. For this factor, the potential impacts on these severe accident design features should
149 also be evaluated to ensure the intent of the design features continue to be met.³

² The General Design Criteria of Appendix A to 10 CFR 50 form the basis for the design criteria for newer plants licensed under 10 CFR Part 50 or Part 52. In some cases, exemptions to specific GDC may have been granted. Older plants may have been licensed to other criteria, such as the AEC draft design criteria. A given plant's design criteria are summarized in its FSAR, as updated. This factor of defense-in-depth should consider the current licensing basis of the plant and how the proposed change would continue to meet the intent of the plant's design criteria.

³ Section C.I.19.8 of Regulatory Guide 1.206, "Combined License Applications for Nuclear Power plants (LWR Edition)," issued June 2007, provides guidance on implementing these requirements and ties the requirements to the issues and performance goals identified in SECY-90-016, "Evolutionary Light-Water Reactor (LWR) Certification Issues and Their Relationship to Current Regulatory Requirements," dated January 12, 1990 and SECY-93-087, "Policy, Technical, and Licensing issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," dated April 2, 1993, which the Commission approved in staff requirements memoranda (SRMs) dated June 26, 1990, and July 21, 1993, respectively. In addition, Regulatory Guide 1.216, Containment Structural Integrity Evaluation for Internal Pressure Loadings above Design-Basis Pressure," dated August 2010, provides acceptable methods for an analysis that specifically addresses the issues and performance goals identified in SECY-90-016 and SECY-93-087 and related SRMs for containment structures in nuclear power plants under severe accident conditions.

150 2.1.1.3 Evaluating the Impact of the LB Change on Defense-in-Depth

151 The seven factors described above are an acceptable way for a licensee to evaluate the impact of a
152 proposed change to the LB on defense-in-depth. While such an evaluation of a change against the seven
153 factors is qualitative, the licensee should be able to conclude that the change maintains consistency of the
154 plant design with the defense-in-depth philosophy by showing that the intent of each factor still is met
155 following the proposed change.

156 The seven factors could be arranged in a hierarchical manner. For example, the first factor is an
157 over-arching, high level description of how defense-in-depth is achieved. Factors two through six may
158 apply at any of the layers of defense to aid the analyst in justifying that the proposed change maintains
159 suitable balance among the layers. Finally, factor seven helps ensure completeness of the assessment of
160 how the proposed change could affect defense-in-depth. Nevertheless, in the interest of simplicity, the
161 seven factors should each be addressed for any proposed risk-informed change to the licensing basis. If a
162 proposed change has no impact on a given factor, that should be stated with a brief justification as
163 appropriate. Licensees are encouraged to structure their discussion of how a proposed change maintains
164 the defense-in-depth philosophy by addressing the seven factors; such an approach should facilitate the
165 licensee's analysis as well as make for a more efficient review by the NRC staff. The licensee should
166 demonstrate/justify that there has not been a significant impact to LB for each of the factors.

167 Note that the focus here is on the effect of the change on defense-in-depth. When a nuclear
168 power plant is licensed, NRC regulations result in some amount of protection or defense at each of the
169 layers of defense. The seven factors presented above are not intended to define how defense-in-depth is
170 implemented in a plant's design, but to help licensees assess the impact of the proposed change.

171 The NRC finds it acceptable for a licensee to use the following seven key factors to evaluate
172 whether a proposed change to the LB maintains the philosophy of defense-in-depth.

173 Evaluating Factor 1: Preserve a reasonable balance among the layers of defense.

174 *A propose change should not significantly reduce the effectiveness of a layer of defense that exists in the*
175 *plant design before the proposed change.*

176
177 *The evaluation of the proposed change should consider insights based on traditional engineering*
178 *approaches; insights from risk assessments may be used to support engineering insights, but should not be*
179 *the only justification for meeting this factor.*

180 To demonstrate that this factor is met, the licensee should address each of the layers in turn.

181 If a comprehensive risk analysis is done, it can provide insights into whether the balance among the layers
182 of defense remains appropriate to ensure protection of public health and safety. Such a risk analysis
183 would not only include the likelihood of challenges to the plant (i.e., initiating event frequencies) from
184 various hazards, but would include estimates of core damage frequency, containment response, and dose
185 estimates to the public. It would include implementation of the emergency plan and estimate the
186 effectiveness of actions such as sheltering in place or evacuation.

187 Note that the risk acceptance guidelines in this RG are based on the surrogates for the Commission's
188 quantitative health objectives, CDF and LERF. These risk metrics, developed as part of the risk
189 assessment, can help inform the licensee's assessment of the relative balance between the second and
190 third layers of defense. In addition, qualitative and quantitative insights from the PRA may help justify
191 the balance across all the layers.

192 However, to address the unknown and unforeseen failure mechanisms or phenomena, the licensee's
 193 evaluation of this factor of defense-in-depth should also address insights based on traditional engineering
 194 approaches. Results and insights of the risk assessment may be used to support the conclusion but should
 195 not be the only justification for meeting this factor. The licensee should consider the impact of the
 196 proposed change on each of the layers of defense:

- 197 • Robust plant design to survive hazards and minimize challenges that could result in an event
 198 occurring - the change should not significantly increase the likelihood of initiating events or
 199 create new significant initiating events;
- 200 • Prevention of a severe accident (core damage) should an event occur - the change should not
 201 significantly impact the availability and reliability of SSCs that provide the safety functions that
 202 prevent plant challenges from progressing to core damage;
- 203 • Containment of the source term should a severe accident occur - the change should not
 204 significantly impact the containment function or SSCs that support that function, such as
 205 containment fan coolers and sprays; and,
- 206 • Protection of the public from any releases of radioactive material - the change should not
 207 significantly reduce the effectiveness of the EP program, including the ability to detect and
 208 measure releases of radioactivity, to notify offsite agencies and the public, to shelter or evacuate
 209 the public as necessary

210 Evaluating Factor 2: Preserve adequate capability of design features without an overreliance on
 211 programmatic activities as compensatory measures.

212 *A proposed change should not* significantly reduce the reliability and availability of design features to
 213 perform their safety functions.

214 *The evaluation of the proposed change should demonstrate that the change does not* result in the
 215 overreliance of programmatic activities to compensate for an intended reduction in the capability of
 216 engineered safety features is not excessive

217 To demonstrate that this factor is met, the licensee should first determine whether the proposed change
 218 necessitates compensatory measures. If not, this should be stated as the reason this factor is met. If
 219 compensatory measures are needed to support the proposed change, the licensee should determine the
 220 extent to which programmatic activities, as compared to design features, are being relied upon. The intent
 221 of this factor is not to preclude the use of programs as compensatory measures, but to ensure that this use
 222 is not excessive.

223 A proposed change that does not affect how safety functions are performed or reduce the reliability or
 224 availability of the SSCs that perform those functions would meet this defense-in-depth factor. However,
 225 a licensee could contemplate a change where a reduction in the capability of those SSCs is compensated
 226 in some manner by reliance on plant programs. In such a case, the licensee should assess whether the
 227 proposed change would increase the need for programmatic activities to compensate for the lack of
 228 engineered features. If the change requires new or additional reliance on such programs, the licensee
 229 should justify that reliance on these measures is not excessive. Use of compensatory measures may be
 230 considered overreliance when a program is substituted for an engineered means of performing a safety
 231 function, or failure of the programmatic activity could prevent an engineered safety feature from
 232 performing its intended function.

233 The NRC also recognizes that compensatory measures are sometimes associated with temporary
234 conditions. A licensee may request a risk-informed change to the plant's licensing basis to permit
235 occasional entry into conditions requiring measures that rely on plant programs to compensate for reduced
236 capability of engineered systems, or for one-time to allow completion of corrective action to restore
237 engineered systems to match the design and licensing basis. For such situations, the licensee should
238 demonstrate that the plant condition requiring such compensatory measures would occur at a sufficiently
239 low frequency or that the time frame to effect corrective action is commensurate with the significance of
240 the non-conforming condition.

241 Evaluating Factor 3: Preserve system redundancy, independence, and diversity commensurate with the
242 expected frequency, consequences of challenges to the system, and uncertainties.

243 *A proposed change should not significantly impact the ability for the system function to be performed.*

244 *The evaluation of the proposed change should demonstrate that the change does not result in a substantial*
245 *reduction in the availability or reliability of the associated SSCs and does not introduce a new single*
246 *failure.*

247 To demonstrate that this factor is met, the licensee should ensure that there is not a substantial reduction
248 in the ability to accomplish a safety function. A safety function may be compromised if one of the plant
249 features that provides for either system redundancy, independence, or diversity is defeated. This adverse
250 impact could occur by the introduction of a new dependency that could potentially defeat the redundancy,
251 independence or diversity of the affected equipment. Plant changes that introduce new dependencies
252 among systems or functions, or that introduce new common cause failures (addressed under factor 4),
253 should not result in a disproportionate increase in risk. That is, system redundancy, independence and
254 diversity can be assumed to be preserved if, given the proposed licensing change, the affected system
255 safety function can be accomplished assuming a new single failure has not been introduced.

256 Some proposed changes are temporary⁴ in nature and result in the plant being in an operational condition
257 where certain design features are not available to perform their intended functions. For example, a single
258 train of a multi-train system may be out of service. It is not the intent of this factor of defense-in-depth to
259 preclude such temporary plant configurations. In general, a proposed change would meet the intent of
260 this factor provided no permanent change to the plant's design or change in operation that affects the
261 redundancy, independence or diversity of the design was being contemplated. There are other controls on
262 temporary plant configurations, such as the Technical Specifications, that limit the exposure to risk during
263 such periods.

264 Evaluating Factor 4: Preserve adequate defense against potential common-cause failures (CCF).

265 *A proposed change should not significantly reduce defenses against CCFs that could defeat the*
266 *redundancy, independence, and/or diversity of DID layers, fission product barriers, and design or*
267 *operation plant features.*

268 *The evaluation of the proposed change should demonstrate that the change does not result in a significant*
269 *reduction of existing CCF defenses or introduce new CCF dependencies.*

270 To understand a defense strategy against a CCF event, it is necessary to understand that defending against
271 a CCF event is no different than defending against an independent failure that has a single root cause,
272 except that more than one failure has occurred and the failures are related through a coupling mechanism.

⁴ Temporary is not meant to imply excessive periods of time.

273 The defense mechanisms for the CCF system include functional barrier, physical barrier, monitoring and
274 awareness, maintenance staffing and scheduling, component identification, and diversity. These defenses
275 are constructed primarily based on defending against the CCF coupling factors. A coupling factor is the
276 condition or mechanism through which multiple components could be affected (or coupled) by the same
277 cause. Coupling factors can be based on attributes, such as hardware quality (manufacturing, installation),
278 design (component part, system configuration), maintenance (schedule, procedure, staff), operation
279 (procedure, staff), and environment (external, internal).

280 There are three methods of defense against a CCF: (1) defend against the failure cause, (2) defend against
281 the CCF coupling factor, or (3) defend against both items 1 and 2. A defense strategy against causes
282 typically includes design control, use of qualified equipment, testing and preventive maintenance
283 programs, procedure review, personnel training, quality control, redundancy, diversity, and barriers. For
284 coupling factors, a defense strategy typically includes diversity (functional, equipment, and staff),
285 barriers, and staggered testing and maintenance. A defense strategy addressing both the cause and
286 coupling factor is the most comprehensive.⁵

287 To demonstrate that this factor is met, the licensee should evaluate the proposed change to determine
288 whether it increases the potential for events or causes that would be a CCF. The licensee should also
289 evaluate the proposed change to determine whether new CCF mechanisms could be introduced.

290 Evaluating Factor 5: Maintain multiple fission product barriers.

291 *A proposed change should not significantly reduce the effectiveness of the multiple fission product*
292 *barriers.*

293 *The evaluation of the proposed change should demonstrate that the change does not:*

- 294 • Create a significant increase in the likelihood or consequence of an event that simultaneously
295 challenges multiple barriers.
- 296 • Introduce the possibility of a new event that would simultaneously impact multiple barriers.

297 To demonstrate that this factor is met, the licensee should demonstrate that the change does not create a
298 significant increase in the likelihood or consequence of an event that simultaneously challenges multiple
299 barriers. To do this, the licensee should consider the following objectives to ensure that the proposed
300 change maintains appropriate safety within the defense-in-depth philosophy:

- 301 • The change does not result in a significant increase in the existing challenges to the integrity of
302 the barriers.
- 303 • The proposal does not significantly increase the failure probability of any individual barrier.
- 304 • The proposal does not introduce new or additional failure dependencies among barriers that
305 significantly increase the likelihood of failure compared to the existing conditions.

⁵ Refer to NUREG/CR-6268, Revision 1, Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding, for further discussions on major failure cause categories, coupling factor categories, and defense mechanisms.

- 306 • The overall redundancy and diversity among the barriers is sufficient to ensure compatibility with
307 the risk acceptance guidelines.

308 Evaluating Factor 6: Preserve sufficient defense against human errors.

309 *A proposed change should not significantly increase the potential for or create new human errors that may*
310 *adversely affect one or more layers of defense.*

311 *The evaluation of the proposed change should demonstrate that the change does not*

- 312 • Create new human failure events that have a significant adverse impact on risk;
313 • Significantly increase the burden on the plant staff responding to events; or,
314 • Significantly increase the human error probability of existing human actions.

315 In determining whether these defenses are preserved, the licensee should assess whether the proposed
316 change would create new human actions that significantly impact the change in risk, place a greater
317 mental/physical demand in responding to events, or increase the probability of existing human errors.
318 The licensee should consider whether the change creates new situations that are likely to cause errors, not
319 only for operators, but for maintenance personnel and other plant staff.

320 Evaluating Factor 7: Continue to meet the intent of the plant's design criteria.

321 *A proposed change should not affect meeting the intent of the plant's design criteria referenced in the*
322 *licensing basis.*

323 *The evaluation of the proposed change should demonstrate that the change does not significantly*
324 *compromise meeting the plant's design criteria thereby significantly reducing the effectiveness of one or*
325 *more defense-in-depth layers.*

326 This factor of defense-in-depth should consider the current licensing basis of the plant and how the
327 proposed change would continue to meet the intent of the plant's design criteria and, for Part 52 plants,
328 continue to meet the intent of the severe accident design features. It is recognized that, in general, the
329 consideration of *applicable regulations* under the first principle of risk-informed regulation would be
330 expected to address this factor of defense-in-depth. Also, it is not the intent of this factor that changes to
331 the plant's design criteria or severe accident design features cannot be requested. However, the licensee
332 should fully understand any impacts that the proposed change may have on the design criteria or severe
333 accident design features of the plant.

334 For example, for some hazards and for some licensees, defense-in-depth may be defined in the plants LB.
335 For example, the fire protection program for licensed nuclear power plants requires that fire protection
336 defense-in-depth, which is scenario-based, be maintained. Any proposed plant change must be evaluated
337 against any plant-specific LB defense-in-depth requirements in addition to the guidance presented herein.

338 2.1.2 **Safety Margin**

339 The engineering evaluation should assess whether the impact of the proposed LB change is
340 consistent with the principle that sufficient safety margins are maintained. Here also, the licensee is
341 expected to choose the method of engineering analysis appropriate for evaluating whether sufficient
342 safety margins would be maintained if the proposed LB change were to be implemented. An acceptable
343 set of guidelines for making that assessment is summarized below. Other equivalent acceptance
344 guidelines may also be used. With sufficient safety margins, the following are true:

- 345 • Codes and standards or their alternatives approved for use by the NRC are met.
 - 346 • Safety analysis acceptance criteria in the LB (e.g., FSAR, supporting analyses) are met or
 - 347 proposed revisions provide sufficient margin to account for analysis and data uncertainty.
- 348 The NRC has developed application-specific guidelines reflecting this general guidance which
- 349 may be found in the application-specific regulatory guides (Refs. 5–9).

DRAFT