

1 2.1 **Evaluation of Defense-in-Depth Attributes and Safety Margins**

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

18 2.1.1 ***Defense-in-Depth***

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

26 This section provides some background on the defense-in-depth philosophy, ~~beginning~~  
27 ~~with including a discussion on the high-level objective for defense-in-depth.~~ Next is a discussion of ~~seven~~  
28 ~~key factors~~ ~~five considerations~~ that may be used to evaluate the impact of a proposed change on defense-  
29 in-depth. One or more examples are provided to help illustrate what is meant by each ~~factor~~ ~~consideration~~.  
30 Finally, this section provides guidance on a process for evaluating ~~any changes to defense-in-depth~~ ~~the~~  
31 ~~seven key factors~~, including an integrated example.

## 32 2.1.1.1 Background

33 Defense-in-depth is an element of the NRC's safety philosophy that employs successive  
34 compensatory measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally  
35 caused event occurs at a nuclear facility<sup>1</sup>. The defense-in-depth philosophy has traditionally been applied  
36 in reactor design and operation to provide multiple means to accomplish safety functions and prevent the  
37 release of radioactive material. It has been and continues to be an effective way to account for  
38 uncertainties in equipment and human performance and, in particular, to account for the potential for  
39 unknown and unforeseen failure mechanisms or phenomena, which (because they are unknown or  
40 unforeseen) are not reflected in either the PRA or traditional engineering analyses.

---

<sup>1</sup> 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)

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

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

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

57 2.1.1.2 High Level Consideration

58 Since the focus of this Regulatory Guide is on applications using a risk-informed argument to  
59 propose changes to the licensing basis, it is based on the presumption that the as-built, as-  
60 operated plant, prior to the change, is consistent with the defense-in-depth philosophy, in that:

61 A reasonable balance between the levels of protection has been established.

62 Effectiveness of the barriers is ensured by conformance with design standards and regulations.

63 Administrative procedures and controls are in place to preserve the defenses.

64 Preserve a reasonable balance among the layers of defense.

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

Formatted: Indent: Left: 0", Hanging: 0.5", No bullets or numbering

Formatted: No bullets or numbering

77 ~~The evaluation of any change to defense in depth should be based on the presumption that the as-~~  
 78 ~~built, as-operated plant, prior to the change, is consistent with the defense in depth philosophy, in~~  
 79 ~~that:~~

80 ~~A reasonable balance between the levels of protection has been established.~~

81 ~~Effectiveness of the barriers is ensured by conformance with design standards and regulations.~~

82 ~~Administrative procedures and controls are in place to preserve the defenses.~~

83 Formatted: bullet2, Indent: Left: 0.5"

84 2.1.1.32 ~~Considerations~~Factors for Evaluating the Impact of LB Changes on Defense-in-Depth

85 Any one or more of the layers of defense discussed above may be ~~adversely~~ impacted by a  
 86 proposed change to a plant's licensing basis. The NRC has identified ~~seven factors~~five considerations that  
 87 should be used to assess the impact of the change on defense-in-depth. These are discussed in detail  
 88 below. Guidance on how to apply these factors is discussed in more detail in section 2.1.1.43.

89 The NRC finds it acceptable for a licensee to use the following ~~seven factors~~five considerations  
 90 to evaluate ~~whether-how~~ a proposed change to the LB ~~maintains the impacts~~ philosophy of defense-in-  
 91 depth. ~~The considerations should be assessed in an integrated manner. A "failure" of any one~~  
 92 ~~consideration is not a reason to reject a risk-informed change.~~

93 ~~1. Preserve a reasonable balance among the layers of defense.~~

94 ~~A reasonable balance of the layers of defense—minimizing challenges to the plant, preventing~~  
 95 ~~any events from progressing to core damage, containing the radioactive source term, and~~  
 96 ~~emergency preparedness—helps to ensure an apportionment of the plant's capabilities between~~  
 97 ~~limiting disturbances to the plant and mitigating their consequences. The term reasonable~~  
 98 ~~balance is not meant to imply an equal apportionment of capabilities. A reasonable balance is~~  
 99 ~~preserved if the proposed plant change does not significantly reduce the effectiveness of a layer~~  
 100 ~~that exists in the plant design and operation before the proposed change. The NRC recognizes~~  
 101 ~~that there may be aspects of a plant's design or operation that may cause one or more of the layers~~  
 102 ~~to be adversely affected. For these situations, the balance between the other layers becomes~~  
 103 ~~especially important when evaluating the impact of a proposed change to the LB and its impact~~  
 104 ~~on defense in depth.~~

105 ~~2.~~ 1. Preserve adequate capability of design features without an overreliance on  
 106 programmatic activities as compensatory measures. Formatted: Indent: Left: 0.5", No bullets or numbering

107 Some proposed changes to the LB may involve or require compensatory measures; that is,  
 108 measures taken to compensate for some reduced functionality, availability, reliability,  
 109 redundancy, or other feature of the plant's design. Such compensatory measures are often  
 110 associated with temporary plant configurations. Compensatory measures may include hardware  
 111 (e.g., skid-mounted temporary power supplies), human actions (e.g., manual system actuation), or  
 112 some combination of these measures. The preferred approach for accomplishing *safety functions*  
 113 is through engineered systems. Therefore, when a proposed change necessitates reliance on  
 114 *programmatic activities* as compensatory measures, the licensee should justify that this reliance is  
 115 not excessive.

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

124 ~~3.~~ 2. Preserve system redundancy, independence, and diversity commensurate with the  
 125 expected frequency, consequences of challenges to the system, and uncertainties.

Formatted: Indent: Left: 0.5", No bullets or numbering

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

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

142 ~~4.~~ 3. Preserve adequate defense against potential common-cause failures (CCF).

Formatted: Indent: Left: 0.5", No bullets or numbering

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

149 ~~5.~~ 4. Maintain multiple fission product barriers.

Formatted: Indent: Left: 0.5", No bullets or numbering

150 Physical fission product barriers (e.g., the fuel cladding, reactor coolant system pressure  
 151 boundary, and containment) includes the physical barriers themselves and any equipment relied  
 152 upon to protect the barriers (e.g., containment spray). In general, these barriers are designed to  
 153 perform independently so that a complete failure of one barrier does not disable the next  
 154 subsequent barrier. For example, one barrier, the containment, is designed to withstand a double-  
 155 ended guillotine break of the largest pipe in the reactor coolant system, another barrier.

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

159 ~~6.~~ 5. Preserve sufficient defense against human errors.

Formatted: Indent: Left: 0.5", No bullets or numbering

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

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

Formatted: Indent: Left: 0", Hanging: 0.5"

168  
169 ~~7.~~ ~~Continue to meet the intent of the plant's design criteria<sup>2</sup>.~~

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

177 ~~For plant's licensed under 10 CFR Part 52, this factor should also address those design features~~  
178 ~~for the prevention and mitigation of severe accidents that are described and analyzed in~~  
179 ~~accordance with 10 CFR 52.47(a)(23) for DC applications and 10 CFR 52.79(a)(38) for COL~~  
180 ~~applications. For this factor, the potential impacts on these severe accident design features should~~  
181 ~~also be evaluated to ensure the intent of the design features continue to be met.<sup>3</sup>~~

182 2.1.1.4~~3~~Evaluating the Impact of the LB Change on Defense-in-Depth

183 The ~~five considerations seven factors~~ described above are an acceptable way for a licensee to  
184 evaluate the impact of a proposed change to the LB on defense-in-depth. ~~While such an evaluation of a~~  
185 ~~change against the seven factors is qualitative, the licensee should be able to conclude that the change~~

<sup>2</sup> 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.

<sup>3</sup> 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.

186 maintains consistency of the plant design with the defense in depth philosophy by showing that the intent  
187 of each factor still is met following the proposed change.

188 ~~The seven factors could be arranged in a hierarchical manner. For example, the first factor is an~~  
189 ~~over-arching, high level description of how defense-in-depth is achieved. Factors two through six may~~  
190 ~~apply at any of the layers of defense to aid the analyst in justifying that the proposed change maintains~~  
191 ~~suitable balance among the layers. Finally, factor seven helps ensure completeness of the assessment of~~  
192 ~~how the proposed change could affect defense in depth. Nevertheless, in the interest of simplicity, the~~  
193 ~~seven factors should each be addressed for any proposed risk-informed change to the licensing basis. If a~~  
194 ~~proposed change has no impact on a given factor, that should be stated with a brief justification as~~  
195 ~~appropriate. Licensees are encouraged to structure their discussion of how a proposed change maintains~~  
196 ~~the impacts defense-in-depth philosophy by addressing the seven factors considerations as relevant to the~~  
197 ~~decision being sought; such an approach should facilitate the licensee's analysis as well as make for a~~  
198 ~~more efficient review by the NRC staff. The licensee should demonstrate/justify that there has not been a~~  
199 ~~significant impact to LB for each of the factors.~~

200 Note that the focus here is on the effect of the change on defense-in-depth. When a nuclear  
201 power plant is licensed, NRC regulations result in some amount of protection or defense at each of the  
202 layers of defense. The ~~seven factors~~five considerations presented above are not intended to define how  
203 defense-in-depth is implemented in a plant's design, but to help licensees assess the impact of the  
204 proposed change. To demonstrate that defense in depth has been preserved, the LAR should demonstrate  
205 that the proposed change maintains appropriate safety within the defense in depth philosophy by showing  
206 that:

207 The licensee should consider the impact of the proposed change on each of the layers of defense-  
208 in-depth in the following way:

- 209 • Robust plant design to survive hazards and minimize challenges that could result in an  
210 event occurring – the change should not significantly increase the likelihood of initiating  
211 events or create new significant initiating events;
- 212 • Prevention of a severe accident (core damage) should an event occur – the change should  
213 not significantly impact the availability and reliability of SSCs that provide the safety  
214 functions that prevent plant challenges from progressing to core damage;
- 215 • Containment of the source term should a severe accident occur – the change should not  
216 significantly impact the containment function or SSCs that support that function, such as  
217 containment fan coolers and sprays; and,
- 218 • Protection of the public from any releases of radioactive material – the change should not  
219 significantly reduce the effectiveness of the EP program, including the ability to detect  
220 and measure releases of radioactivity, to notify offsite as necessary.

221 In addition, the licensee should demonstrate that the proposal does not introduce new or additional failure  
222 dependencies among barriers that significantly increase the likelihood of failure compared to the  
223 existing conditions.

224  
225 The change does not result in significant increase in the existing challenges to the integrity of the  
226 barriers

Formatted: Indent: Left: 0", Hanging: 0.5"

DRAFT

DRAFT

DRAFT

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

227 ~~The proposal does not significantly change the failure probability of any individual barrier~~  
228 ~~The proposal does not introduce new or additional failure dependencies among barriers that~~  
229 ~~significantly increase the likelihood of failure compared to the existing conditions.~~  
230 ~~The NRC finds it acceptable for a licensee to use the following seven key factors to evaluate~~  
231 ~~whether a proposed change to the LB maintains the philosophy of defense in depth.~~  
232 ~~Evaluating Factor I High Level Consideration: Preserve a reasonable balance among the layers of~~  
233 ~~defense.~~  
234 ~~A propose change should not significantly reduce the effectiveness of a layer of defense that exists in the~~  
235 ~~plant design before the proposed change.~~  
236  
237 ~~The evaluation of the proposed change should consider insights based on traditional engineering~~  
238 ~~approaches; insights from risk assessments may be used to support engineering insights, but should not be~~  
239 ~~the only justification for meeting this factor.~~  
240 ~~To demonstrate that this factor is met, the licensee should address each of the layers in turn.~~  
241 If a comprehensive risk analysis is done, it can provide insights into whether the balance among the layers  
242 of defense remains appropriate to ensure protection of public health and safety. Such a risk analysis  
243 would not only include the likelihood of challenges to the plant (i.e., initiating event frequencies) from  
244 various hazards, but would include estimates of core damage frequency, containment response, and dose  
245 estimates to the public. It would include implementation of the emergency plan and estimate the  
246 effectiveness of actions such as sheltering in place or evacuation.  
247 Note that the risk acceptance guidelines in this RG are based on the surrogates for the Commission's  
248 quantitative health objectives, CDF and LERF. These risk metrics, developed as part of the risk  
249 assessment, can help inform the licensee's assessment of the relative balance between the second and  
250 third layers of defense. In addition, qualitative and quantitative insights from the PRA may help justify  
251 the balance across all the layers.  
252 The NRC also recognizes that compensatory measures are sometimes associated with temporary  
253 conditions. A licensee may request a risk-informed change to the plant's licensing basis to permit  
254 occasional entry into conditions requiring measures that rely on plant programs to compensate for reduced  
255 capability of engineered systems, or for one-time to allow completion of corrective action to restore  
256 engineered systems to match the design and licensing basis. For such situations, the licensee should  
257 demonstrate that the plant condition requiring such compensatory measures would occur at a sufficiently  
258 low frequency or that the time frame to effect corrective action is commensurate with the significance of  
259 the non-conforming condition.  
260  
261 However, to address the unknown and unforeseen failure mechanisms or phenomena, the licensee's  
262 evaluation of this factor of defense-in-depth should also address insights based on traditional engineering  
263 approaches. Results and insights of the risk assessment may be used to support the conclusion but should  
264 not be the only justification for meeting this factor. ~~The licensee should consider the impact of the~~  
265 ~~proposed change on each of the layers of defense.~~

DRAFT

DRAFT

DRAFT

266 • ~~Robust plant design to survive hazards and minimize challenges that could result in an event~~  
267 ~~occurring—the change should not significantly increase the likelihood of initiating events or create new~~  
268 ~~significant initiating events;~~

269 • ~~Prevention of a severe accident (core damage) should an event occur—the change should not~~  
270 ~~significantly impact the availability and reliability of SSCs that provide the safety functions that prevent~~  
271 ~~plant challenges from progressing to core damage;~~

272 • ~~Containment of the source term should a severe accident occur—the change should not~~  
273 ~~significantly impact the containment function or SSCs that support that function, such as containment fan~~  
274 ~~coolers and sprays; and,~~

275 • ~~Protection of the public from any releases of radioactive material—the change should not~~  
276 ~~significantly reduce the effectiveness of the EP program, including the ability to detect and measure~~  
277 ~~releases of radioactivity, to notify offsite agencies and the public, to shelter or evacuate the public as~~  
278 ~~necessary~~

279 Evaluating ~~Consideration 1~~Factor 2: Preserve adequate capability of design features without an  
280 overreliance on programmatic activities as compensatory measures.

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

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

286 To ~~demonstrate that this factor is met~~evaluate this consideration, the licensee should first determine  
287 whether the proposed change necessitates compensatory measures. If not, this should be stated as the  
288 reason this ~~factor-consideration~~ is met. If compensatory measures are needed to support the proposed  
289 change, the licensee should determine the extent to which programmatic activities, as compared to design  
290 features, are being relied upon. The intent of this factor is not to preclude the use of programs as  
291 compensatory measures, but to ensure that this use is not excessive.

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

302 ~~The NRC also recognizes that compensatory measures are sometimes associated with temporary~~  
303 ~~conditions. A licensee may request a risk informed change to the plant's licensing basis to permit~~  
304 ~~occasional entry into conditions requiring measures that rely on plant programs to compensate for reduced~~  
305 ~~capability of engineered systems, or for one-time to allow completion of corrective action to restore~~  
306 ~~engineered systems to match the design and licensing basis. For such situations, the licensee should~~  
307 ~~demonstrate that the plant condition requiring such compensatory measures would occur at a sufficiently~~

Formatted: bullet2, No bullets or numbering

DRAFT

DRAFT

DRAFT

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

308 ~~low frequency or that the time frame to effect corrective action is commensurate with the significance of~~  
309 ~~the non-conforming condition.~~

310 Evaluating Consideration 2~~Factor 3~~: Preserve system redundancy, independence, and diversity  
311 commensurate with the expected frequency, consequences of challenges to the system, and uncertainties.

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

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

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

326 Some proposed changes are temporary<sup>4</sup> in nature and result in the plant being in an operational condition  
327 where certain design features are not available to perform their intended functions. For example, a single  
328 train of a multi-train system may be out of service. It is not the intent of this factor of defense-in-depth to  
329 preclude such temporary plant configurations. In general, a proposed change would meet the intent of  
330 this factor provided no permanent change to the plant's design or change in operation that affects the  
331 redundancy, independence or diversity of the design was being contemplated. There are other controls on  
332 temporary plant configurations, such as the Technical Specifications, that limit the exposure to risk during  
333 such periods.

334 Evaluating Consideration 3~~Factor 4~~: Preserve adequate defense against potential common-cause failures  
335 (CCF).

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

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

341 To understand a defense strategy against a CCF event, it is necessary to understand that defending against  
342 a CCF event is no different than defending against an independent failure that has a single root cause,  
343 except that more than one failure has occurred and the failures are related through a coupling mechanism.  
344 The defense mechanisms for the CCF system include functional barrier, physical barrier, monitoring and  
345 awareness, maintenance staffing and scheduling, component identification, and diversity. These defenses  
346 are constructed primarily based on defending against the CCF coupling factors. A coupling factor is the  
347 condition or mechanism through which multiple components could be affected (or coupled) by the same

<sup>4</sup> Temporary is not meant to imply excessive periods of time.

DRAFT

DRAFT

DRAFT

DRAFT

DRAFT

DRAFT

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

348 cause. Coupling factors can be based on attributes, such as hardware quality (manufacturing, installation),  
349 design (component part, system configuration), maintenance (schedule, procedure, staff), operation  
350 (procedure, staff), and environment (external, internal).

351 There are three methods of defense against a CCF: (1) defend against the failure cause, (2) defend against  
352 the CCF coupling factor, or (3) defend against both items 1 and 2. A defense strategy against causes  
353 typically includes design control, use of qualified equipment, testing and preventive maintenance  
354 programs, procedure review, personnel training, quality control, redundancy, diversity, and barriers. For  
355 coupling factors, a defense strategy typically includes diversity (functional, equipment, and staff),  
356 barriers, and staggered testing and maintenance. A defense strategy addressing both the cause and  
357 coupling factor is the most comprehensive.<sup>5</sup>

358 To ~~evaluate this consideration~~~~demonstrate that this factor is met~~, the licensee should evaluate the  
359 proposed change to determine whether it increases the potential for events or causes that would be a CCF.  
360 The licensee should also evaluate the proposed change to determine whether new CCF mechanisms could  
361 be introduced.

362 Evaluating ~~Factor 5~~Consideration 4: Maintain multiple fission product barriers.

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

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

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

369 To ~~demonstrate that this factor is met~~~~evaluate this consideration~~, the licensee should demonstrate that the  
370 change does not create a significant increase in the likelihood or consequence of an event that  
371 simultaneously challenges multiple barriers. To do this, the licensee should consider the following  
372 objectives to ensure that the proposed change maintains appropriate safety within the defense-in-depth  
373 philosophy:

- 374 • The change does not result in a significant increase in the existing challenges to the integrity of  
375 the barriers.
- 376 • The proposal does not significantly increase the failure probability of any individual barrier.
- 377 • The proposal does not introduce new or additional failure dependencies among barriers that  
378 significantly increase the likelihood of failure compared to the existing conditions.
- 379 • The overall redundancy and diversity among the barriers is sufficient to ensure compatibility with  
380 the risk acceptance guidelines.

---

<sup>5</sup> 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.

DRAFT

DRAFT

DRAFT

381 Evaluating ~~Factor 6~~Consideration 5: Preserve sufficient defense against human errors.

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

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

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

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

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

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

396 *~~The evaluation of the proposed change should demonstrate that the change does not significantly~~*  
397 *~~compromise meeting the plant's design criteria thereby significantly reducing the effectiveness of one or~~*  
398 *~~more defense in depth layers.~~*

399 ~~This factor of defense in depth should consider the current licensing basis of the plant and how the~~  
400 ~~proposed change would continue to meet the intent of the plant's design criteria and, for Part 52 plants,~~  
401 ~~continue to meet the intent of the severe accident design features. It is recognized that, in general, the~~  
402 ~~consideration of applicable regulations under the first principle of risk informed regulation would be~~  
403 ~~expected to address this factor of defense in depth. Also, it is not the intent of this factor that changes to~~  
404 ~~the plant's design criteria or severe accident design features cannot be requested. However, the licensee~~  
405 ~~should fully understand any impacts that the proposed change may have on the design criteria or severe~~  
406 ~~accident design features of the plant.~~

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

411

412 ~~It is proposed that consideration of defense-in-depth would be most relevant when:~~

413 ~~The proposed change affects a method of achieving a required safety function when the level of~~  
414 ~~redundancy or diversity is limited or where significant uncertainty exists.~~

415 ~~The proposed license amendment affects defense-in-depth by introducing cross-cutting changes (e.g.,~~  
416 ~~administrative changes, maintenance practices) that affect multiple safety functions or cut across levels of~~  
417 ~~protection.~~

DRAFT

DRAFT

DRAFT

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

418 Changes whose effects cannot be addressed directly by the PRA, e.g., impacts the likelihood or modes of  
419 late containment failures.

420 2.1.2 ***Safety Margin***

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

- 427 • Codes and standards or their alternatives approved for use by the NRC are met.
- 428 • Safety analysis acceptance criteria in the LB (e.g., FSAR, supporting analyses) are met or  
429 proposed revisions provide sufficient margin to account for analysis and data uncertainty.

430 The NRC has developed application-specific guidelines reflecting this general guidance which  
431 may be found in the application-specific regulatory guides (Refs. 5–9).

DRAFT

DRAFT

DRAFT

DRAFT